



A.M. REDDY

Memorial College of Engineering and Technology
Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada
SPONSORED BY
ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution

Web : www.amreddyengineering.ac.in
E-mail: principal.amreddyengineering@gmail.com
VINUKONDA ROAD, MASTAN REDDY HAGAR, PETLURIVARIPALEM,
NARASARAOPET PALHADU (DIST) - 522601,
CONTACT : 08647-247190.

II B.TECH II SEM ECE TIME TABLE (2022-2023)

W.E.From 30.01.2023

PERIOD	1	2	11:10 TO 11:20	3	4	1:00 TO 1:50	5	6	3:30 TO 3:40	7		
DURATION	9:30 TO 10:20	10:20 TO 11:10		11:20 TO 12:10	12:10 TO 1:00		1:50 TO 2:40	2:40 TO 3:30		3:40 TO 4:20		
MON	SOFT SKILLS LAB		B R E A K	SS LAB	ECA	L U N C H	DICD	LCS	B R E A K	MOB		
TUE	ECA	AC		DICD	LIBRARY		MOB	MOB		SPORTS		
WED	MOB	AC		DICD	LCS		AC	ECA		COI		
THU	LCS	AC LAB		AC LAB			MOB	AC		COI		
FRI	COI	DICD LAB		DICD LAB			AC	LCS		ECA		
SAT	ECA	DICD		DICD	LCS		ECA LAB					

ECA Electronic Circuit Analysis

DICD Digital IC Design

AC Analog Communications

LCS Linear control Systems

DICD LAB Digital IC Design Lab

AC LAB Analog Communications Lab

MOB Management & Organizational Behavior

SS Soft Skills

ECA LAB Electronic Circuit Analysis Lab

COI Constitution of India

Mr P GANESH KUMAR

Mr. N RAMESH BABU

Mr. K SANJEEVA RAO

Mrs.K SILPA

Mr. N RAMESH BABU

Mr. K SANJEEV RAO

Mrs.G.SRAVANI

Mrs .K GOWRI

Mr.G.ANIL KUMAR

Mr.RAVI SANKAR

Ganesh
HOD

Ganesh
Principal

Ganesh
PRINCIPAL

HEAD OF THE DEPARTMENT
ELECTRONICS AND COMMUNICATION ENGINEERING
A.M. REDDY MEMORIAL COLLEGE OF ENGG & TECH
PETLURIVARIPALEM

Narasaraopet (M.D.) Guntur (DL)

A.M. REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PAL

Narasaraopet (M.D.) Guntur (DL)

Principal
A.M. REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

II Year-II Semester		L	T	P	C
	ANALOG COMMUNICATIONS	3	0	0	3

Course Objectives:

Students undergoing this course are expected to

- Familiarize with the fundamentals of analog communication systems.
- Familiarize with various techniques for analog modulation and demodulation of signals.
- Distinguish the figure of merits of various analog modulation methods.
- Develop the ability to classify and understand various functional blocks of radio transmitters and receivers.
- Familiarize with basic techniques for generating and demodulating various pulse modulated signals.

UNIT I

AMPLITUDE MODULATION : Introduction to communication system, Need for modulation, Frequency Division Multiplexing , Amplitude Modulation, Definition, Time domain and frequency domain description, single tone modulation, power relations in AM waves, Generation of AM waves, square law Modulator, Switching modulator, Detection of AM Waves; Square law detector, Envelope detector.

UNIT II

DSB & SSB MODULATION: Double side band suppressed carrier modulators, time domain and frequency domain description, Generation of DSBSC Waves, Balanced Modulators, Ring Modulator, Coherent detection of DSB-SC Modulated waves, COSTAS Loop. Frequency domain description, Frequency discrimination method for generation of AM SSB Modulated Wave, Time domain description, Phase discrimination method for generating AMSSB Modulated waves. Demodulation of SSB Waves, Vestigial side band modulation: Frequency description, Generation of VSB Modulated wave, Time domain description, Envelope detection of a VSB Wave pulse Carrier, Comparison of AM Techniques, Applications of different AM Systems, FDM.

UNIT III

ANGLE MODULATION: Basic concepts, Frequency Modulation: Single tone frequency modulation, Spectrum Analysis of Sinusoidal FM Wave, Narrowband FM, Wideband FM, Constant Average Power, Transmission bandwidth of FM Wave- Generation of FM Waves, Detection of FM Waves: Balanced Frequency discriminator, Zero crossing detector, Phase locked loop. Comparison of FM & AM.

UNIT IV

TRANSMITTERS & RECEIVERS: Radio Transmitter - Classification of Transmitter, AM Transmitter, Effect of feedback on performance of AM Transmitter, FM Transmitter –Variable reactance type and phase modulated FM Transmitter, frequency stability in FM Transmitter. **Radio Receiver** - Receiver Types - Tuned radio frequency receiver, Super heterodyne receiver, RF section and Characteristics - Frequency changing and tracking, Intermediate frequency, AGC, FM Receiver, Comparison with AM Receiver, Amplitude limiting. Communication Receivers, extensions of super heterodyne principle and additional circuits.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT V

NOISE: Review of noise and noise sources, noise figure, Noise in Analog communication Systems, Noise in DSB & SSB System, Noise in AM System, Noise in Angle Modulation Systems, Threshold effect in Angle Modulation System, Pre-emphasis & de-emphasis **PULSE MODULATION:** Types of Pulse modulation, PAM (Single polarity, double polarity) PWM: Generation & demodulation of PWM, PPM, Generation and demodulation of PPM, Time Division Multiplexing, TDM Vs FDM

TEXTBOOKS:

1. Principles of Communication Systems–HTaub&D.Schilling, GautamSahe, TMH, 3rd Edition, 2007.
2. Principles of Communication Systems-Simon Haykin, John Wiley, 2nd Edition, 2007.
3. Modern Digital and Analog Communication Systems –B.P.Lathi, Zhi Ding, Hari Mohan Gupta, Oxford University Press, 4th Edition, 2017

REFERENCES:

1. Electronics & Communication System– George Kennedyand Bernard Davis, TMH 2004.
2. Communication Systems–R.P.Singh, SP Sapre, Second Edition TMH, 2007.
3. Electronic Communication systems–Tomasi, Pearson, fourth Edition, 2007.

Course Outcomes:

After undergoing the course, students will be able to

- Differentiate various Analog modulation and demodulation schemes and their spectral characteristics
- Analyze noise characteristics of various analog modulation methods
- Analyze various functional blocks of radiotransmitters and receivers
- Design simple analog systems for various modulation techniques

[Signature]
Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
KAKINADA

[Signature]
Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
KAKINADA


 <p>A.M. REDDY Memorial College of Engineering and Technology Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada SPONSORED BY ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003</p>	<p>An ISO 9001:2015 Certified Institution Web : www.amreddyengineering.ac.in E-mail: principal.amreddyengineering@gmail.com VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM, NARASARAOPET PALNADU (DIST) - 522601, CONTACT : 08647-247190.</p>
--	---


Department of ECE

III B.TECH/I-SEM

S.NO	REGD.NO	STUDENT NAME
1	20HM1A0401	ANIMELA SUMA LATHA
2	20HM1A0402	BADIGE MANOJ KUMAR
3	20HM1A0403	BANDI VINOD KUMAR
4	20HM1A0404	BANDI VISWA NARAYANA
5	20HM1A0405	BANDLA PALLI VIJAYA KUMAR REDDY
6	20HM1A0406	BELDAR SHAMEER
7	20HM1A0407	BODAGALA VENUGOPAL
8	20HM1A0408	BUSAGANI BALAPPA
9	20HM1A0410	CHINNA GOWNI THARUN KUMAR
10	20HM1A0411	CHIPPAGIRI MANOJU NATH REDDY
11	20HM1A0412	DEVANA SAI SANDEEP REDDY
12	20HM1A0413	EEDIGA PRADEEP GOWD
13	20HM1A0415	GANDAM SANDEEPKUMAR
14	20HM1A0417	GULURU GOPAL REDDY
15	20HM1A0421	KASUKURTHI AKHILA
16	20HM1A0422	KAVUJULA THIRUPATHAMMA
17	20HM1A0423	KOSURU NAGA JOSHNA
18	20HM1A0424	LOKEPALLI RAKESH REDDY
19	20HM1A0425	MADINENI MAHESH
20	20HM1A0426	MANGALI YASWANTH
21	20HM1A0427	MULLAPUDI SUZEEL
22	20HM1A0428	MYLAVARAM JAGAN MOHAN REDDY
23	20HM1A0429	PALAPARTHI SUMANTH
24	20HM1A0430	PALETI PRABHUDHINAKAR
25	20HM1A0431	POBBATHI SAI TEJA
26	20HM1A0433	SAKE PRAVEEN
27	20HM1A0434	TUMMALAGUNTA ASMITHA
28	20HM1A0435	UPPARA ANITHA
29	20HM1A0436	VEERLA SRILAKSHMI
30	21HM5A0401	VAJRALA VEERA GOPAL REDDY


 Principal
 A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Mdl), Guntur, Dr.


 Principal
 A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Mdl), Guntur, Dr.

 <p>A.M. REDDY Memorial College of Engineering and Technology Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada SPONSORED BY ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003</p>	<p>An ISO 9001:2015 Certified Institution Web : www.amreddyengineering.ac.in E.mail: principal.amreddyengineering@gmail.com VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM, NARASARAOPET PALNADU (DIST) - 522601, CONTACT : 08647-247190.</p>
--	--

SCHEME OF EVALUATION: Set 1

1-Mid Examination

1.(a) Definition 1mark

Explanation 1.5 mark

(b) circuit diagram 1.5 mark

Explanation 1 mark

2. (a) definition 1 mark

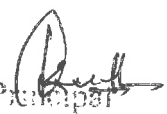
(b) circuit diagram 3 marks

Explanation 1 mark

3.(a) circuit diagram 3 marks

(b) Explanation 2 marks


Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Md), Guntur Dist.


Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Md), Guntur

SEHEME OF EVALUATION :

2-MID EXAMINATION

1 (a) definition 1 mark

Block diagram 2 marks

Explanation 2marks

2. (a) Block diagram 3 marks

Explanation 1 mark

Advantages 1 mark

3. Block diagram 3 marks

Explanation 2 marks

PROGRAM OUTCOMES (POs): Common to all branches of Engineering

Engineering Graduates will be able to:

PO1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
PO2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO3	Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
PO4	Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO5	Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
PO6	The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
PO7	Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
PO8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
PO10	Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
PO11	Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
PO12	Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Programme Outcome (PO's) of M.Tech Transportation Engineering:


PO1	Demonstrate skill for planning, design, construction and maintenance of transportation projects.
PO2	Assessment of environmental and its allied issues to the construction of the transportation projects.
PO3	Demonstrate skills to use modern engineering tools, software and equipments to analyze problems and evolve solutions
PO4	To enhance communication skills and successfully apply research aptitude among students to R &D activities and consultancy works.

Programme Outcome (PO's) of M.Tech Structural Design:

PO1	Demonstrate the thorough knowledge of profession and implement it for enrichment of quality of life in the society.
PO2	Demonstrate design skills by using software and technical support.
PO3	Demonstrate the ability to undertake the research projects in various fields of civil engineering using software and experimental techniques.
PO4	Demonstrate ability for team work and lifelong learning.

Bloom's Taxonomy Level for Assessment Design

- Bloom's Taxonomy provides an important framework to not only design curriculum and teaching methodologies but also to design appropriate examination questions belonging to various cognitive levels.
- Bloom's Taxonomy of Educational Objectives developed in 1956 by Benjamin Bloom was widely accepted by educators for curriculum design and assessment.
- In 2001, Anderson and Krathwohl modified Bloom's taxonomy to make it relevant to the present-day requirements.
- It attempts to divide learning into three types of domains (cognitive, affective, and behavioural) and then defines the level of performance for each domain.
- Conscious efforts to map the curriculum and assessment to these levels can help the programsto aim for higher-level abilities which go beyond remembering or understanding, and require application, analysis, evaluation and creation.

	<h1 style="margin: 0;">A.M. REDDY</h1> <p style="margin: 0;">Memorial College of Engineering and Technology</p> <p style="margin: 0;">Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada</p> <p style="margin: 0;">SPONSORED BY</p> <p style="margin: 0;">ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003</p>	<p style="margin: 0;">An ISO 9001:2015 Certified Institution</p> <p style="margin: 0;">Web : www.amreddyengineering.ac.in</p> <p style="margin: 0;">E.mail: principal.amreddyengineering@gmail.com</p> <p style="margin: 0;">VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARI PALEM, NARASARAOPET PALNADU (DIST) - 522601, CONTACT : 08647-247190.</p>
---	--	--

QUIZ-II EXAMINATIONS

Roll No. :

SUBJECT: ANALOG COMMUNICATIONS (SET-I)

DATE:

TIME: 20 MINUTES

1.	2.	3.	4.	5.
6.	7.	8.	9.	10.

1. The sampling technique having the minimum noise interference is

- a. Instantaneous sampling
- b. Natural sampling
- c. Flat top sampling
- d. All of the above

2. Types of analog pulse modulation systems are

- a. Pulse amplitude modulation
- b. Pulse time modulation
- c. Frequency modulation
- d. Both a and b

3. In pulse amplitude modulation,

- a. Amplitude of the pulse train is varied
- b. Width of the pulse train is varied
- c. Frequency of the pulse train is varied
- d. None of the above

*** Pulse time modulation (PTM) includes**

- a. Pulse width modulation
- b. Pulse position modulation
- c. Pulse amplitude modulation
- d. Both a and b

5. Drawback of using PAM method is

- a. Bandwidth is very large as compared to modulating signal
- b. Varying amplitude of carrier varies the peak power required for transmission
- c. Due to varying amplitude of carrier, it is difficult to remove noise at receiver
- d. All of the above

6. In different types of Pulse Width Modulation,

- a. Leading edge of the pulse is kept constant
- b. Tail edge of the pulse is kept constant
- c. Centre of the pulse is kept constant
- d. All of the above

7. In pulse width modulation,

- a. Synchronization is not required between transmitter and receiver
- b. Amplitude of the carrier pulse is varied
- c. Instantaneous power at the transmitter is constant
- d. None of the above

8. In PWM signal reception, the Schmitt trigger circuit is used

- a. To remove noise
- b. To produce ramp signal
- c. For synchronization
- d. None of the above

9. In Pulse Position Modulation, the drawbacks are

- a. Synchronization is required between transmitter and receiver


 A.M. REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Mdl), Guntur Dt.


 Principal

A.M. REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Mdl), Guntur Dt.

- b. Large bandwidth is required as compared to PAM
- c. None of the above
- d. Both a and b

10. Why a helical antenna is used for satellite tracking?

- a) because of its circular polarization
- b) because of its broad bandwidth
- c) because of its low bandwidth
- d) because of rectangular polarization

11.	12.	13.	14.	15.
16.	17.	18.	19.	20.

11. Which one of the following noise becomes of great importance at high frequencies?

- a) flicker noise
- b) shot noise
- c) impulse noise
- d) transit-time noise

12. Which one of the following statement is false?

- a) High Frequency mixers are generally noisier
- b) Voltage of impulse noise is independent of bandwidth
- c) Thermal noise is not dependent on frequency
- d) Flicker noise occurs at low frequency

13. Which of broad classifications of noise are most difficult to treat?

- a) noise generated in the receiver
- b) noise generated in the transmitter
- c) external noise
- d) internal noise

14. What points must be important to remember, when we deal with random noise calculations?

- a) all calculations are based on peak to peak values
- b) calculations are based on quantised values
- c) calculations are based on average values
- d) calculations are based on RMS values

15. Which of the following statement is true?

- a) Random noise power is inversely proportional to bandwidth
- b) Flicker noise occurs at high frequency
- c) Noise mixers are caused by inadequate image frequency rejection
- d) A random voltage across a resistance cannot be calculated

16. For a periodic function, the spectral density and auto-correlation functions are _____

- a) Laplace transform pair
- b) Fourier transform pair
- c) Gauss transform pair
- d) Z-transform pair

17. Spectral density express _____

- a) Average voltage
- b) Average power in a waveform as a function of frequency
- c) Average noise voltage
- d) Average channel capacity

18. For a Gaussian process, auto correlation also implies _____

- a) Statistical dependence
- b) Statistical independence
- c) Statistical distribution
- d) Ergodic process

19. What will be the value of modulation if we want maximum undistorted transmitted power?

- a) 0
- b) 1
- c) 0.2
- d) 0.5

d. None of the above

19. In Pulse Position Modulation, the drawbacks are

- a. Synchronization is required between transmitter and receiver
- b. Large bandwidth is required as compared to PAM
- c. None of the above
- d. Both a and b

20. Why a helical antenna is used for satellite tracking?

- a) because of its circular polarization
- b) because of its broad bandwidth
- c) because of its low bandwidth
- d) because of rectangular polarization


Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, D.


Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, D.

9. What will be the value of modulation if we want maximum undistorted transmitted power?

- a) 0
- b) 1
- c) 0.2
- d) 0.5

10. For providing two or more voice circuits on the same carrier, we can use _____

- a) SSB
- b) ISB systems
- c) DSB-SC
- d) VSB

11.	12.	13.	14.	15.
16.	17.	18.	19.	20.

11. The sampling technique having the minimum noise interference is

- a. Instantaneous sampling
- b. Natural sampling
- c. Flat top sampling
- d. All of the above

12. Types of analog pulse modulation systems are

- a. Pulse amplitude modulation
- b. Pulse time modulation
- c. Frequency modulation
- d. Both a and b

13. In pulse amplitude modulation,

- a. Amplitude of the pulse train is varied
- b. Width of the pulse train is varied
- c. Frequency of the pulse train is varied
- d. None of the above

14. Pulse time modulation (PTM) includes

- a. Pulse width modulation
- b. Pulse position modulation
- c. Pulse amplitude modulation
- d. Both a and b

15. Drawback of using PAM method is

- a. Bandwidth is very large as compared to modulating signal
- b. Varying amplitude of carrier varies the peak power required for transmission
- c. Due to varying amplitude of carrier, it is difficult to remove noise at receiver
- d. All of the above

16. In different types of Pulse Width Modulation,

- a. Leading edge of the pulse is kept constant
- b. Tail edge of the pulse is kept constant
- c. Centre of the pulse is kept constant
- d. All of the above

17. In pulse width modulation,

- a. Synchronization is not required between transmitter and receiver
- b. Amplitude of the carrier pulse is varied
- c. Instantaneous power at the transmitter is constant
- d. None of the above

18. In PWM signal reception, the Schmitt trigger circuit is used

- a. To remove noise
- b. To produce ramp signal
- c. For synchronization

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dt.

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dt.



A.M. REDDY

Memorial College of Engineering and Technology
Approved by AICTE, New Delhi. Affiliated to JNTUK-Kakinada
SPONSORED BY
ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution

Web : www.amreddyengineering.ac.in
E.mail: principal.amreddyengineering@gmail.com
VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM,
NARASARAOPET PALNADU (DIST) - 522601,
CONTACT : 08647-247190.

QUIZ-II EXAMINATIONS

Roll No. :

DATE:

SUBJECT: ANALOG COMMUNICATIONS (SET-2)

TIME: 20 MINUTES

1.	2.	3.	4.	5.
6.	7.	8.	9.	10.

- Which one of the following noise becomes of great importance at high frequencies?
 - flicker noise
 - shot noise
 - impulse noise
 - transit-time noise
- Which one of the following statement is false?
 - High Frequency mixers are generally noisier
 - Voltage of impulse noise is independent of bandwidth
 - Thermal noise is not dependent on frequency
 - Flicker noise occurs at low frequency
- Which of broad classifications of noise are most difficult to treat?
 - noise generated in the receiver
 - noise generated in the transmitter
 - external noise
 - internal noise
- What points must be important to remember, when we deal with random noise calculations?
 - all calculations are based on peak to peak values
 - calculations are based on quantised values
 - calculations are based on average values
 - calculations are based on RMS values
- Which of the following statement is true?
 - Random noise power is inversely proportional to bandwidth
 - Flicker noise occurs at high frequency
 - Noise mixers are caused by inadequate image frequency rejection
 - A random voltage across a resistance cannot be calculated
- For a periodic function, the spectral density and auto-correlation functions are _____
 - Laplace transform pair
 - Fourier transform pair
 - Gauss transform pair
 - Z-transform pair
- Spectral density express _____
 - Average voltage
 - Average power in a waveform as a function of frequency
 - Average noise voltage
 - Average channel capacity
- For a Gaussian process, auto correction also implies _____
 - Statistical dependance
 - Statistical independence
 - Statistical distribution
 - Ergodic process

Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur D.

Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur D.

Code No:R2022043

R20

SET - 1

II B. Tech II Semester Regular Examinations, June/July - 2022
ANALOG COMMUNICATIONS
(Common to ECE &ECT)

Time: 3 hours

Max. Marks:

70

Answer any FIVE Questions each Question from each unit
All Questions carry Equal Marks

UNIT-I

- 1 a) With neat sketch explain Frequency Division Multiplexing. [7M]
b) Calculate the percentage power saving when the carrier and one of the sidebands are suppressed in an AM wave modulated to a depth of 100% and 50%. [7M]
Or
2 a) Develop the equation of a single tone modulation of AM system and explain the power relations. [7M]
b) With the help of waveforms and spectrum, describe the concept of Amplitude modulation both in time domain and frequency domain. [7M]

UNIT-II

- 3 a) List out the methods for generation of SSB-SC signal and explain any one of the method in detail. [7M]
b) Find the various frequency components and their amplitudes in the voltage given by $v(t) = 50(1 + 0.7 \cos 5000t - 0.3 \cos 1000t) \sin 5 \times 10^6 t$. Draw the single sided spectrum. Also evaluate the modulated and sideband power. [7M]
Or
4 a) Explain the generation of DSB-SC signal using balanced modulator. Derive the expression for DSB-SC signal. [7M]
b) A carrier signal $c(t) = 10 \cos(2\pi \cdot 10^6 t)$ is modulated by a message signal $m(t) = 2 \cos(8\pi \cdot 10^3 t)$ to generate a DSB-SC signal. Sketch the spectrum, calculate the B.W and power. [7M]

UNIT-III

- 5 a) Explain Armstrong method of generation of FM signal. [7M]
b) Distinguish between FM and PM by giving its mathematical analysis. [7M]
Or
6 a) Describe the frequency analysis of Angle modulated waves. Explain their Bandwidth requirements. [7M]
b) Compare AM and FM Systems noise performances. [7M]

UNIT-IV

- 7 Explain the following (i) AGC (ii) RF sections. [14M]
Or
8 a) Discuss about frequency stability in FM Transmitter. [7M]
b) List out the advantages and disadvantages of TRF receiver. [7M]

UNIT-V

- 9 a) Explain, how a PPM signal can be generated from PWM signal. [7M]
b) Explain demodulation of PPM. [7M]
Or
10 Write short notes on i) Single polarity and Double polarity PAM ii) Generation and Demodulation of PWM [14M]

|||||

Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur, Dt.

Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur, Dt.

Code No:R2022043

R20

SET - 3

II B. Tech II Semester Regular Examinations, June/July - 2022

ANALOG COMMUNICATIONS

(Common to ECE & ECT)

Time: 3 hours

Max. Marks: 70

Answer any **FIVE** Questions each Question from each unit
All Questions carry **Equal** Marks

UNIT-I

- 1 a) With suitable diagram explain the square-law diode modulation method for AM generation. [7M]
b) An amplitude modulated voltage is given by $V = 50 (1 + 0.2 \cos 100 t + 0.001 \cos 3500t) \cos 10^6 t$. State all frequency components present in the voltage, and find modulation index for each modulating voltage term. What is the effective modulation index of V? [7M]

Or

- 2 a) Describe an expression for AM wave and sketch its frequency spectrum. [7M]
b) Explain the square law detection of AM signals. [7M]

UNIT-II

- 3 a) Explain the Frequency discrimination method for generating SSB signal. [7M]
b) With neat sketch explain COSTAS Loop? [7M]

Or

- 4 a) Explain the phase discrimination method for generating SSB. [7M]
b) Explain the principle of coherent detection of DSB-SC with neat block diagram. [7M]

UNIT-III

- 5 a) With the help of waveforms and spectrum, describe the concept of FM. [7M]
b) With neat circuit diagram explain the working of a Balanced Frequency discriminator. [7M]

Or

- 6 a) Draw the block diagram of FM transmitter using indirect method and explain its working. [7M]
b) Describe the working of a varactor diode modulator of FM [7M]

UNIT-IV

- 7 a) Mention the advantages of superhetrodyne receiver over TRF receiver [4M]
b) Distinguish between simple AGC and delayed AGC [5M]
c) Draw the block Schematic for FM broad cast receiver and explain the function of each unit [5M]

Or

- 8 a) Explain the effect of feedback on performance of AM transmitter. [7M]
b) Write a short notes on amplitude limiting. [7M]

UNIT-V

- 9 Write short notes on i) Single polarity PAM ii) Generation of PWM [14M]

Or

- 10 a) What is Noise figure? Find the Average Noise Figure of cascaded networks [7M]
b) Discuss threshold effect in angle modulation systems [7M]

1 of 1





A.M. REDDY

Memorial College of Engineering and Technology

Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada

SPONSORED BY

ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution

Web : www.amreddyengineering.ac.in

E.mail: principal.amreddyengineering@gmail.com

VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM,

NARASARAOPET PALNADU (DIST) - 522601,

CONTACT : 08647-247190.

II-Assignment Question Paper, June- 2023

Year/Sem: II/I

Programme: B.Tech-ECE

Course Code:

R2022043

Regulation :R20

Course Name: ANALOG
COMMUNICATION

Total Marks :5

Q.No	Answer All Questions	Marks	Levels of Bloom's taxonomy	CO
1	Draw the block diagram of TRF receiver		Knowledge	4
2	Draw and explain the FM Demodulator using PLL	2	Explanation	3
3	Explain the Process of generation of PWM with neat diagram	2	Enhancement	3

Princy
Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, Dt

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, Dt



A.M. REDDY

Memorial College of Engineering and Technology
Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada
SPONSORED BY
ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution

Web : www.amreddyengineering.ac.in
E.mail: principal.amreddyengineering@gmail.com
VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM,
NARASARAOPET PALNADU (DIST) - 522601,
CONTACT : 08647-247190,

ACADEMIC CALENDAR 2022-23

B. Tech./B.Pharm. 11 YEAR 1 & 11 SEMESTER

SEM-I

	Description	Duration	
		From	
1	Commencement of I Semester classwork		28.11.2022
2	1 st Spell of Instructions	28.11,2022	21.012023 8 Weeks
3	First Mid Term Examinations	23.012023	30.01.2023 1 Week
4	Submission of First Mid Term Exam Marks to the Universit on or before		04.02.2023
5	2 nd Spell of Instructions	31.01.2023	29.032023 8 Weeks
6	Second Mid Term Examinations	31.03.2023	08.04.2023 1 Week
7	Preparation Holidays and Practical Examinations	10.04.2023	15.04.2023 (1 week)
8	Submission of Second Mid Term Exam Marks to the Universit on or before		15.04.2023
9	End Semester Examinations	17.042023	29.04.2023 2 Weeks

Note: No. of Working / Instructional Days: 93

11 SEM

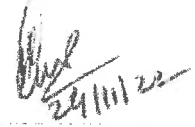
	Description	Duration	
		From	
	Commencement of II Semester classwork		01.05.2023
2	1 st Spell of Instructions (including Summer Vacation	01.05.2023	08.07.2023 (10 Weeks)
3	Summer Vacation	15.052023	2105.2023 2 Weeks
4	First Mid Term Examinations	10.07.2023	15.07.2023 Week
5	Submission of First Mid Term Exam Marks to the Universit on or before		22.07.2023
6	2 nd Spell of Instructions	18.07.2023	11.09.2023 8 Weeks
7	Second Mid Term Examinations	12.09.2023	16.09.2023 1 Week
8	Preparation Holidays and Practical Examinations	19.09.2023	23.09.2023 (1 week)
9	Submission of Second Mid Term Exam Marks to the Universit on or before		23.09.2023

Principal

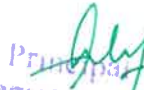
A.M. REDDY MEMORIAL COLLEGE OF ENGINEERING & TECHNOLOGY
PETLURIVARIPALEM
NARASARAOPET (MID), GUNTUR, A.P.

10	End Semester Examinations	25.09.2023	07010.2023 2 Weeks
----	---------------------------	------------	--------------------

Note: No. of Working / Instructional Days: 92



REGISTRAR



Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, Or

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur

**A.M. REDDY**

Memorial College of Engineering and Technology
 Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada
 SPONSORED BY
 ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution

Web : www.amreddyengineering.ac.in
 E-mail: principal.amreddyengineering@gmail.com
 VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM,
 NARASARAOPET PALYADU (Dist) - 522601,
 CONTACT : 08647-242190.

II B.tech II SEM(R-20)-MID Examinations Marks-Academic Year-2022-2023

SUBJECT:AC

SUBJECT CODE:

branch:

S.NO	Roll No	MID-1				MID-2			
		Des 15M	Online 10M	Assi 5M	Sum-1	Des 15M	Online 10M	Assi 5M	Sum-2
1	20HM1A0401	10	9	5	17	9	6	5	20
2	20HM1A0402	12	3	5	20	8	2	5	15
3	20HM1A0403	12	2	5	19	12	4	5	21
4	20HM1A0404	14	4	5	23	13	1	5	19
5	20HM1A0405	15	2	5	22	14	2	5	21
6	20HM1A0406	13	2	5	20	13	3	5	21
7	20HM1A0407	12	1	5	18	12	4	5	21
8	20HM1A0408	10	6	5	21	10	5	5	20
9	20HM1A0410	9	7	5	21	8	2	5	15
10	20HM1A0411	12	3	5	20	11	2	5	18
11	20HM1A0412	12	2	5	19	19	1	5	18
12	20HM1A0413	11	3	5	19	11	6	5	22
13	20HM1A0415	10	4	5	19	12	4	5	21
14	20HM1A0417	12	2	5	19	13	4	5	17
15	20HM1A0421	13	2	5	20	10	3	5	18
16	20HM1A0422	9	6	5	20	12	3	5	20
17	20HM1A0423	7	5	5	17	8	2	5	15
18	20HM1A0424	13	4	5	22	9	1	5	15
19	20HM1A0425	AB	AB	AB	A	10	1	5	16
20	20HM1A0426	12	6	5	23	11	2	5	18
21	20HM1A0427	13	2	5	20	14	2	5	21
22	20HM1A0428	10	4	5	19	12	1	5	18
23	20HM1A0429	12	3	5	20	13	1	5	19
24	20HM1A0430	15	2	5	22	15	3	5	23
25	20HM1A0431	12	2	5	19	15	2	5	22
26	20HM1A0433	15	3	5	23	13	2	5	20
27	20HM1A0434	14	2	5	21	12	4	5	21
28	20HM1A0435	10	2	5	17	10	6	5	21
29	20HM1A0436	11	1	5	17	11	4	5	20
30	21HM5A0401	12	4	5	21	12	3	5	20

A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (M.D), Guntur Dist.

A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (M.D), Guntur Dist.



A.M. REDDY

Memorial College of Engineering and Technology
Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada
SPONSORED BY
ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution

Web : www.amreddyengineering.ac.in
E.mail: principal.amreddyengineering@gmail.com
VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARI PALEM,
NARASARAOPET PALNADU (DIST) - 522601,
CONTACT : 08647-247190.

II-Mid Examination Question Paper, NOVEMBER- 2023

SET-2

Year/Sem: IV/I	Programme: B.Tech- ECE	Course Code: R42043	Regulation :R20	
Course Name: SATELLITE COMMUNICATION	Duration: 90Min.	Total Marks : 15	Min Passing Mark: 8	
Q.No	Answer All Questions	Marks	Levels of Bloom's taxonomy	CO
1	Draw the block diagram of earth station technology and explain.	5	Knowledge	1
2	a) Explain On board processing of TDMA. b) Explain Satellite Switched TDMA.	5	Explanation	2
3	Explain Transmitters, Receivers, and Antennas.	5	Enhancement	3

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Midi), Guntur Dist.

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Midi), Guntur Dist.



A.M. REDDY

Memorial College of Engineering and Technology

Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada

SPONSORED BY

ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution

Web : www.amreddyengineering.ac.in

E.mail: principal.amreddyengineering@gmail.com

VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM,

NARASARAOPET PALMADU (DIST) - 522601,

CONTACT : 08647-247190.

II-Mid Examination Question Paper, NOVEMBER- 2023

SET-2

Year/Sem: IV/I	Programme: B.Tech- ECE	Course Code: R42043	Regulation :R20	
Course Name: SATELLITE COMMUNICATION	Duration: 90Min.	Total Marks : 15	Min Passing Mark: 8	
Q.No	Answer All Questions	Marks	Levels of Bloom's taxonomy	CO
1	Draw the block diagram of earth station technology and explain.	5	Knowledge	1
2	a) Explain On board processing of TDMA. b) Explain Satellite Switched TDMA.	5	Explanation	2
3	Explain Transmitters, Receivers, and Antennas.	5	Enhancement	3

Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur-0.

Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM



A.M. REDDY

Memorial College of Engineering and Technology
Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada
SPONSORED BY
ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution
Web : www.amreddyengineering.ac.in
E.mail: principal.amreddyengineering@gmail.com
VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM,
NARASARAOPET PALNADU (DIST) - 522601,
CONTACT : 08647-247190.

COURSE PLAN

Academic Year: 2022-2023

Subject: Analog Communications

Class & Sem: II B.TECH-II SEM

Faculty Name: K.SANJEEVARAO

Branch: ECE (R20)

Department: ECE

S.NO		TOPIC COVERED	No. of Hours
1	UNIT-I	Introduction to communication system	1
2		Need for modulation	1
3		Frequency Division Multiplexing	1
4	First week	Modulation and Amplitude Modulation	1
5		AM Time domain and frequency domain description	2
6		Single tone modulation, power relations in AM waves	2
7		Generation of AM waves and square law Modulator	2
8		Switching modulator	1
9		Detection of AM Waves; Square law detector, Envelope detector.	2
10	UNIT-II	introduction of DSB & SSB modulation	1
11		Double side band suppressed carrier modulators time domain and frequency domain description	2
12		Generation of DSBSC Waves, Balanced Modulators, Ring Modulator	2
13	2nd week	Coherent detection of DSB-SC Modulated waves	1
14		COSTAS Loop. Frequency domain description	2
15		Frequency discrimination method for generation of AM SSB Modulated Wave	2
16		Phase discrimination method for generating AM SSB Modulated waves. Demodulation of SSB Waves,	2
17		Vestigial side band modulation: Frequency description	2

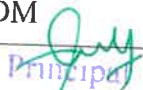
Sanjeevarao
Principal

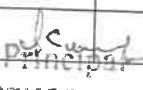
K. Sanjeevarao
Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, Dt

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECH
PETLURIVARI PALEM
Narasaraopet

18		Generation of VSB Modulated wave, Time domain description, Envelope detection of a VSB Wave pulse Carrier,	2
19		Comparison of AM Techniques, Applications of different AM Systems.	1
20	UNIT-III	Basic Concepts Of Angle Modulation	1
21		Frequency Modulation: Single tone frequency modulation, Spectrum Analysis of Sinusoidal FM Wave	2
22		Narrow band FM, Wide band FM, Constant Average Power	2
23		Transmission bandwidth of FM Wave	1
24		Generation of FM Waves, Direct FM, Detection of FM Waves	2
25		Balanced Frequency discriminator, Zero crossing detector Phase locked loop, Comparison of FM & AM.	3
26	UNIT-IV	introduction of transmitters, classification of transmitters	1
27		AM Transmitter, Effect of feedback on performance of AM Transmitter	2
28		FM Transmitter – Variable reactance type and phase modulated FM Transmitter, frequency stability in FM Transmitter	2
29		introduction of Radio Receiver, Receiver Types	1
30		Tuned radio frequency receiver, Superhetrodyne receiver	2
31		RF section and Characteristics, Frequency changing and tracking, Intermediate frequency	2
32		AGC, FM Receiver, Comparison with AM Receivers	2
33		Amplitude limiting. Communication Receivers, Extensions of super heterodyne principle and additional circuits.	2
34	UNIT-V	Review of noise and noise sources, noise figure	2
35		Noise in Analog communication Systems, Noise in DSB& SSB System, Noise in AM System, Noise in Angle Modulation Systems	3
36		Threshold effect in Angle Modulation System, Pre-emphasis & de-emphasis	2
37	UNIT-VI	Introduction Of Pulse Modulation, Time Division Multiplexing,	2
38		Types of Pulse modulation, PAM (Single polarity, double polarity)	2
39		Generation & demodulation of PWM	2
40		PPM, Generation and demodulation of PPM	2
41		FDM ,TDM Vs FDM	2


 Principal
**A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasareopet (Mdi), Guntur Dt.**


 Principal
**A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasareopet (Mdi), Guntur Dt.**



A.M. REDDY

Memorial College of Engineering and Technology
Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada
SPONSORED BY
ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution
Web : www.amreddyengineering.ac.in
E.mail: principal.amreddyengineering@gmail.com
VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM,
NARASARAOPET PALNADU (DIST) - 522601,
CONTACT : 08647-247190.

LESSION PLAN

S.NO	Date & Day of the week	Time		Topic(s) Covered	E.T Gadgets used.if any(LCD/OHP/Charts/Models)
		From	To		
1	4-8-22	10:20	11:10	element of Commun	C/B
2	5-8-22	10:20	11:10	Communication Syste	C/B
3	6-8-22	10:20	11:10	need for modulation	C/B
4	18-8-22	10:20	11:10	FDm	C/B
5	20-8-22	11:20	12:10	Am,	C/B
6	22-8-22	10:20	11:10	Time domain descrip	C/B
7	29-8-22	10:20	11:10	Frequency domain	C/B
8	07-9-22	10:20	11:10	single tone modulatio	C/B
9	26-8-22	10:20	11:10	Power relations in Am	C/B
10	22-8-22	11:20	12:10	Generation of Am wave	C/B
11	29-8-22	10:20	11:10	square law modulator	C/B
12	04-9-22	10:20	11:10	Switched modulator	C/B
13	21-9-22	10:20	11:10	Detection of Am wave	C/B
14	28-9-22	10:20	11:10	square law detector	C/B
15	27-9-22	11:20	12:10	Envelope detector	C/B
16	29-9-22	10:20	11:10	Double side band	C/B
17	30-9-22	10:20	11:10	Time domain	C/B
18	31-9-22	10:20	11:10	Frequency domain	C/B
19	1-10-22	11:10	12:10	DSSC Waves	C/B
20	9-10-22	10:20	11:10	Balanced modulator	C/B
21	10-10-22	10:20	11:10	Ring modulator	C/B
22	15-10-22	10:20	11:10	Coherent detection DSB	C/B
23	18-10-22	10:20	11:10	Colpitts loop	C/B
24	22-10-22	11:10	12:10	Frequency domain	C/B
25	25-10-22	10:20	11:10	Phase discrimination	C/B
26	29-10-22	10:20	11:10	AMSSB	C/B
27	2-11-22	10:20	11:10	Generation of VSB	C/B
28	9-11-22	10:20	11:10	Time domain modulat	C/B
29	16-11-22	10:20	11:10	Envelope detection	C/B
30	23-11-22	10:20	11:10	Amplitude Error	C/B
31	30-11-22	10:20	11:10	Frequency modulatio	C/B
32	2-12-22	11:10	12:10	single tone freq	C/B
33	8-12-22	10:20	11:10	Analy sis of FM wave	C/B
34	12-12-22	10:20	11:10	Narrow band FM	C/B
35	16-12-22	10:20	11:10	wide band FM	C/B
36	20-12-22	10:20	11:10	Average Power	C/B
37	24-12-22	10:20	11:10	Transmission bandw	C/B
38	28-12-22	10:20	11:10	Generation & En wave	C/B
39	4-1-23	11:20	12:10	detection of FM wave	C/B

Principal
A.M. REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dist

Principal
A.M. REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dist



A.M. REDDY

Memorial College of Engineering and Technology
Approved by AICTE, New Delhi. Affiliated to JNTUK-Kakinada
SPONSORED BY
ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution

Web : www.amreddyengineering.ac.in
E-mail: principal.amreddyengineering@gmail.com
VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM,
NARASARAOPET PALNADU (DIST) - 522601,
CONTACT : 08647-247190.

LESSION PLAN

S.NO	Date & Day of the week	Time		Topic(s) Covered	E.T Gadgets used if any(LCD/OHP/Charts/Models)
		From	To		
40	6-1-23	10:20	11:10	Classification of Transmitters	C/B
41	11-1-23	10:20	11:10	Am Transmitter	C/B
42	13-1-23	11:10	11:10	Effect of feedback	C/B
43	18-1-23	10:20	11:10	AM Transmitter	C/B
44	20-1-23	10:20	11:10	Variable resistance feedback	C/B
45	24-1-23	10:20	11:10	Phase modulation Em	C/D
46	30-1-23	10:20	11:10	Frequency Modulation in PM	C/B
47	2-2-23	10:20	11:10	RC Coupled TWT	PPT
48	7-2-23	11:10	12:10	Tuned radio frequency	C/B
49	10-2-23	10:20	11:10	Super heterodyne receiver	C/B
50	14-2-23	10:20	11:10	AE Section Character	C/B
51	20-2-23	10:20	11:10	Frequency Enhanced	C/B
52	23-2-23	10:20	11:10	Intermediate Frequency	C/B
53	27-2-23	10:20	11:10	AGC	C/B
54	3-3-23	11:20	12:10	EM Receiver	C/B
55	6-3-23	10:20	11:10	Comparison with AM Receiver	C/B
56	10-3-23	10:20	11:10	Amplitude limiter	C/B
57	13-3-23	10:20	11:10	Communication Receiver	PPT
58	17-3-23	10:20	11:10	Pre-amplifier	C/B
59	20-3-23	10:20	11:10	Name and noise in	C/B
60	23-3-23	11:10	12:10	Noise figure	C/B
61	25-3-23	10:20	11:10	Noise in Analog Com	C/B
62	27-3-23	10:20	11:10	Noise in DSB	C/B
63	31-3-23	10:20	11:10	Noise in QSB	C/B
64	3-4-23	10:20	11:10	Noise in AM SSB	C/B
65	6-4-23	10:20	11:10	Noise in AM Mod	C/B
66	10-4-23	10:20	11:10	Threshold effect	C/B
67	12-4-23	10:20	11:10	Pre-emphasis	C/B
68	15-4-23	10:20	11:10	de-emphasis	PPT
69	16-4-23	10:20	11:10	Pulse modulation	C/B
70	17-4-23	10:20	11:10	Types of modulator	C/B
71	20-4-23	10:20	11:10	PAM	C/B
72	20-4-23	10:20	11:10	Polarity	C/B
73	21-4-23	10:20	11:10	double Polarity	C/B
74	21-4-23	10:20	11:10	PWM	C/B
75	24-4-23	10:20	11:10	Pulse PPM	C/B
76	21-4-23	10:20	11:10	Generation of PPM	C/B
77	26-4-23	10:20	11:10	Time division mul	C/B
78	28-4-23	10:20	11:10	TDM	C/B

Principal

Principal

A.M. REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dt

A.M. REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dt



A.M. REDDY
Memorial College of Engineering and Technology
Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada
SPONSORED BY
ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution
Web : www.amreddyengineering.ac.in
E.mail: principal.amreddyengineering@gmail.com
VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM,
NARASARAOPET PALNADU (DIST) - 522601,
CONTACT : 08647-247190.

Department of Electrical & Electronics Engineering
Lesson Plan

Year / Branch / Sem:	2022/ECE/II-II	Academic Year:	2022 – 23
Course Name & Code:	Analog Communication		K. Sanjeev Rao

S.No	Hours taken	Unit No	Topic Description	Reference	Teaching Aids	Remarks
1	1	1	Introduction to communication system	T1/R1	GB	
2	1	1	Need of modulation	T1/R2	GB	
3	1	1	Frequency Division Multiplexing	T1/R3	GB	
4	2	1	Modulation and Amplitude Modulation, Time domain and frequency domain description	T1/R2	GB	
5		1	Single tone Modulation, power relation in AM waves	T1/R1	GB	
6	2	1	Generation of AM waves and square law modulation	T1/T2	GB	
7	1	1	Switching modulator	T1	GB	
8	2	1	Detection of AM waves, square law, Envelop detector	T1/R2	GB	
9	1	2	Introduction of DSB & SSB Modulation	T1/T2	GB	
10	1	2	DSBSC Modulators time domain and frequency domain description	T1/T2	GB	
11	2	2	Generation of DSBSC Waves, Balanced Modulators, ring Modulators	T1/T2	GB	
12	3	2	Coherent detection of DSB-SC Modulated wave , COSTAS Loop frequency domain description	T1/R1/T2	GB	
13	2	2	Frequency discrimination method for generation of AM-SSB Modulated wave	T1/R1/T2	GB	
14	2	2	Phase discrimination method for generating AM SSB Modulated waves	T1/R2	GB	
15	1	2	Demodulation of SSB Waves	T1/T2	GB	
16	1	2	VSB Modulation , Frequency description	T1/R1/R2	GB	
17	2	2	Generation of VSB Modulated wave, Time domain description	T1/R1	GB	
18	1	2	Envelope detection of a VSB wave pulse carrier	T1/R2	GB	
19	1	2	Comparison of AM Techniques, Applications of different AM systems	T1/R2	GB	
20	1	3	Basics Concepts of Angle Modulation	T1/R1	GB	
21	2	3	FM single tone frequency modulation, spectrum analysis of sinusoidal FM wave	T1/R2	GB	
22	2	3	NBFM, WBFM ,Constant Average Power	T1/R1	GB	
23	1	3	Transmission bandwidth of FM wave	T1/R1	GB	
24	2	3	Generation of FM Waves	T1/R2/R3	GB	
25	1	3	Detection of FM Waves	T1/R2/R3	GB	

Principal
A.M. REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (M.D.)

Principal
A.M. REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (M.D.)

26	1	3	Phased locked loop	T1/R2	GB	
27	1	3	Comparison of FM & AM	T1/R2	GB	
28	2	3	Introduction to Transmitter classification of transmitters	T1/R1	GB	
29	2	3	AM transmitters, Effect of feedback on performance of AM transmitter	T1/R2	GB	
30	2	3	FM Transmitter-Variable reactance type and phase modulated FM Transmitter	T1/R1	GB	
31	1	3	Frequency stability in FM Transmitter	T1/R1	GB	
32	1	4	Introduction of Radio receiver, Receiver Types	T1/R1	GB	
33	1	4	TRF Receiver	T1/R2	GB	
34	1	4	Superhetrodyne receiver	T1/R1	GB	
35	2	4	RF section and characteristics, Frequency changing and tracking, Intermediate frequency	T1/R2	GB	
36	2	4	AGC,FM Receiver ,Comparison with AM Receivers	T1/R1	GB	
37	2	4	Amplitude limiting, Communication Receiver	T1/R1	GB	
38	1	4	Extensions of super heterodyne principle and additional circuits	T1/R1/T2	GB	
39	1	5	Review of noise sources ,noise figure	T1/R2/T2	GB	
40	3	5	Noise in Analog communication systems, noise in DSB &SSB Systems ,noise in AM systems, noise in angle modulation systems	T1/R1/T2	GB	
41	1	5	Threshold effect in angle Modulation Systems	T1/R2	GB	
42	2	5	Pre-emphasis & De-emphasis	T1/R1	GB	
43	2	5	Introduction of pulse modulation	T1/R3	GB	
44	1	5	Time division Multiplexing	T1/R1	GB	
45	2	5	Types of Pulse Modulation	T1/R1	GB	
46	1	5	PAM (Single polarity, double polarity)	T1/R1	GB	
47	1	5	Generation of PWM	T1/R3	GB	
48	1	5	Demodulation of PWM	T1/R1	GB	
49	1	5	PPM Generation	T1/R1	GB	
50	1	5	Demodulation of PPM	T1/R1	GB	
51	1	5	Frequency division multiplexing	T1/R3	GB	
52	1	5	TDM Vs FDM	T1/R1	GB	
53	2		Revision of Unit 1&2&3	T1/R1	GB	
54	2		Revision of Unit 4&5	T1/R3	GB	
55	73		NO. OF HOURS			

Note: -Teaching aids: - GB = Green board, PPT = Power point presentation

Text Books: -

T1. Principles of Communication Systems -H Taub & schilling, Gautamsahe, TMH ,3rd Edition.

T2. Principles of Communication Systems - SimonHaykin , John wily,2nd Edition,2007.

K. R. Reddy
Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Md),Guntur

K. R. Reddy
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Md),Guntur

Reference Books: -

R1. Electronics & Communication system- Georgy Kennedy and Bernard Davis, TMH 2004


R2. Communication Systems-R. P Singh, SP Sapre, Second Edition TMH, 2007.

R3. Electronic Communication systems -Tomasi,Pearson Edition,2007

Provide any URL links for any of the topic:

- YouTube links
- NPTEL / SWAYAM links
- Gate material link or any animation links etc


Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl),Guntur, S


Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl),Guntur, S

Assignment - 1

5

Name :- P. Devika

Year :- 2nd year

Branch :- 21HM1A0422

Rollno :- ECE

Subject :- Analog Communications


Submitted by
P. Devika

Submitted to
K. Sanjeev Rao Sir

Assignment 1 Received


Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALAYAM
Narasaraopet (Mdi), Gunur


Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALAYAM
Narasaraopet (Mdi), Gunur

Modulation and Demodulation

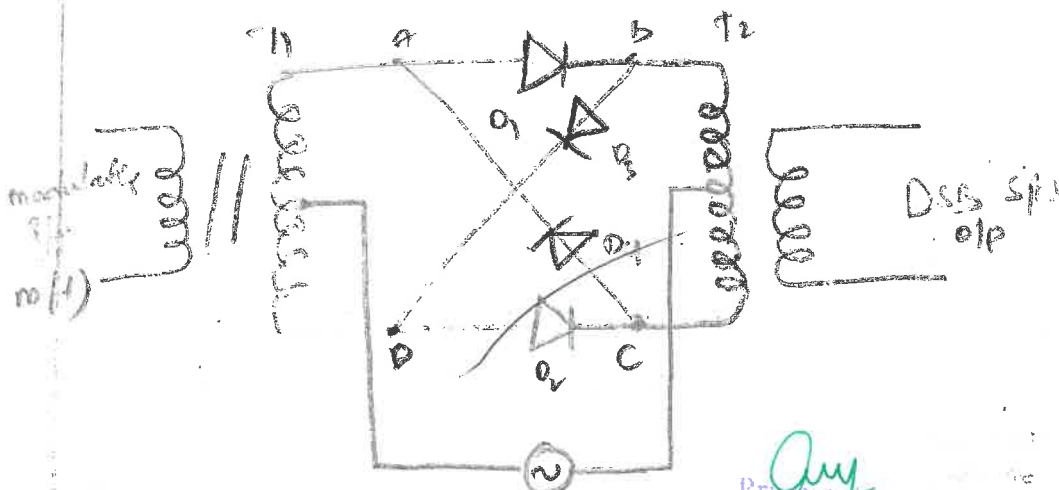
modulation :- modulation is defined as process in which some characteristics parameters of a high frequency carrier signal is varied linearly in accordance with the instantaneous amplitude of the msg signals.

Demodulation :- The process of recovering of original signal from the modulated signal is called demodulation.

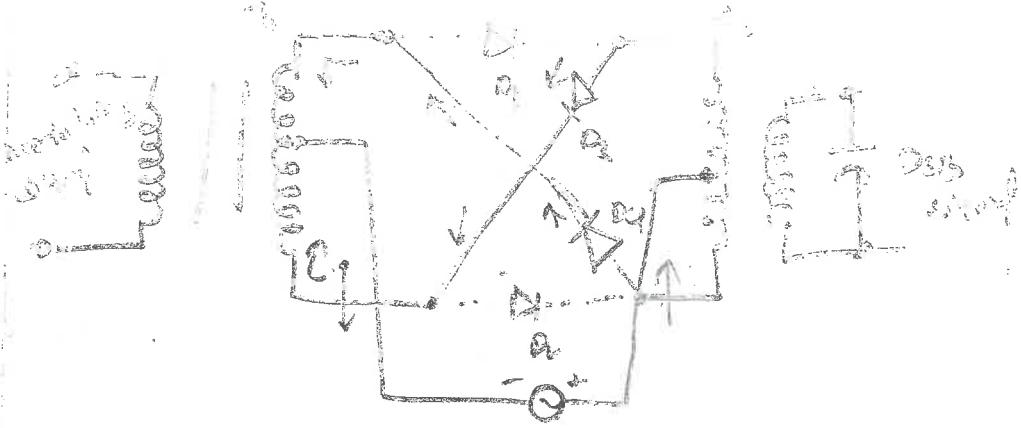
② Balanced ring modulator with wave forms

Initially, we will see the most popular and widely used balanced modulator, diode ring or lattice modulator

It consists of an i/p transformer, T_1 , an output transformer T_2 , and four diodes connected in a bridge circuit.



Princip
A.M REDDY MEMORIAL COLLEGE OF ENGINEERING & TECHNOLOGY
LURIVARI PALEM
Narasaraopet (Mdl), Guntur, A.P.
carrier oscillator
lattice type balanced modulator



Negative half cycle of carrier

with modulating signal

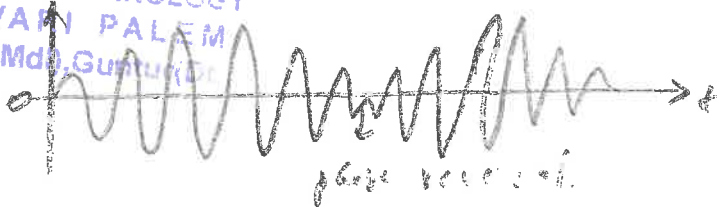
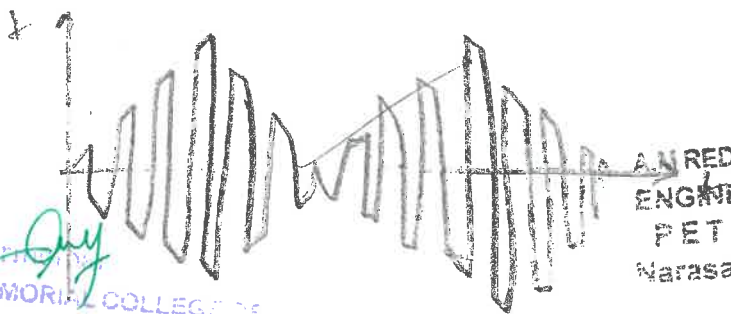
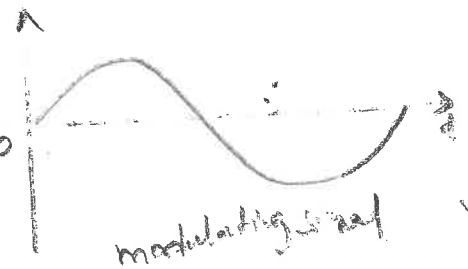
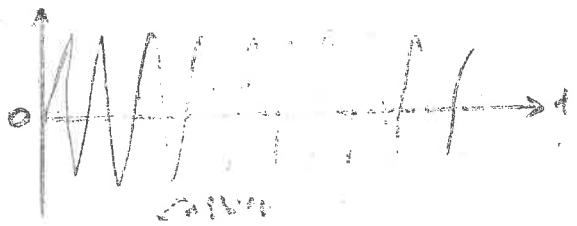
The ring modulator is more ideal when carrier is a square wave. In case of square wave carrier $c(t)$ is represented by

$$c(t) = \frac{4}{\pi} \sum_{n=1,3,5,\dots}^{\infty} \frac{(-1)^{(n-1)/2}}{2n-1} \cos [2\pi f_c t (2n-1)]$$

We know DSBSC

$$s(t) = c(t) m(t)$$

$$s(t) = \frac{4}{\pi} \sum_{n=1,3,5,\dots}^{\infty} \frac{(-1)^{(n-1)/2}}{2n-1} \cos [2\pi f_c t (2n-1)] m(t)$$



Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Md), Guntur (Dt)

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Md), Guntur (Dt)

Assignment - II

5

Name : D. Ajay Kumar

Branch : E.C.E

Rollno : 21HM0A0405

Subject :- Analog Communication

Submitted by :-
D. Ajay Kumar.

Submitted to :-
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur

Ajay
Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur, Dr

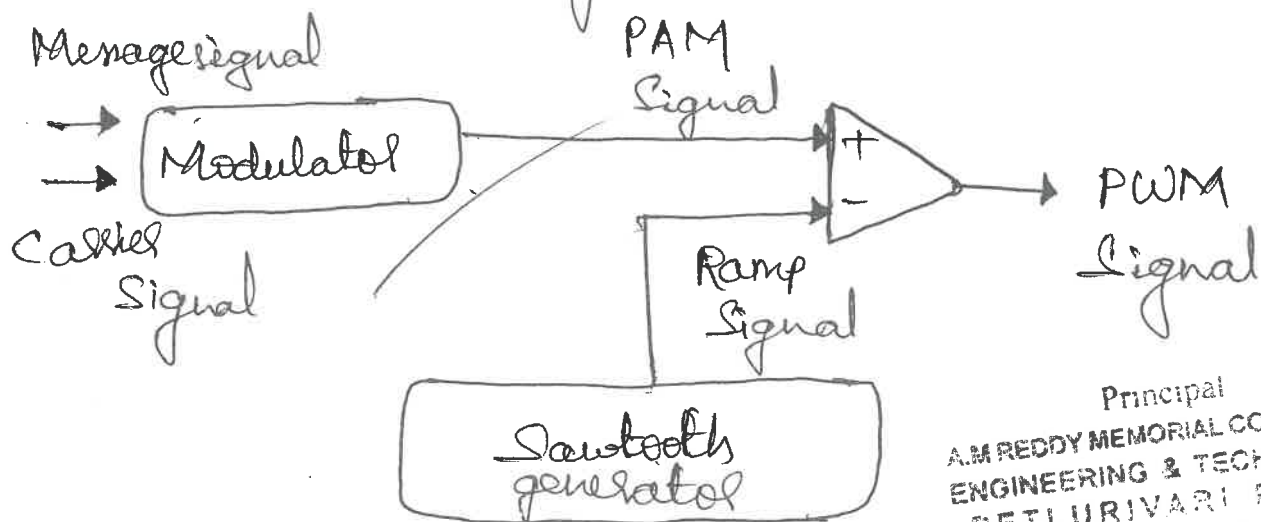
Assignment Received *glo*

②.

PWM Signal Generator

PWM signal can be generated using a comparator. One input of the comparator is connected to a modulating signal and the other input is fed with a non-sinusoidal wave of saw-tooth wave. The comparator compares the two i/p signals and generates a PWM signal.

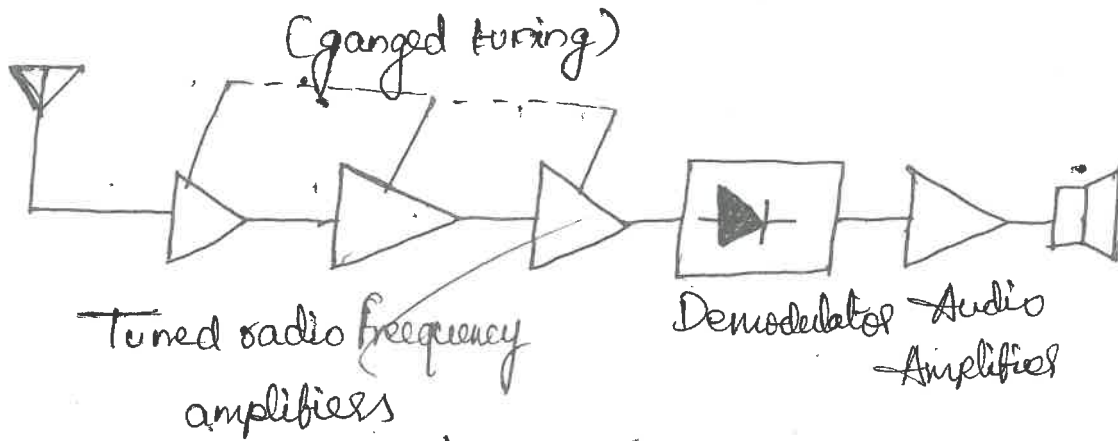
Circuit diagram of PWM Signal Generator



Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Midl), Guntur (Dt.)

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Midl), Guntur (Dt.)

Q1. Block diagram of TRF-Receiver



→ A tuned radio frequency receiver is a type of radio receiver that is composed of one or more tuned radio frequency amplifier stages followed by a detector circuit to extract the audio signal and usually an audio frequency amplifier.

It provides FINRA members with a mechanism for the reporting of transactions effected other-wise than on an exchange.

Assignment - 11

Name :- G. Saroja

Branch :- ECE

Year :- 2nd year

Roll no :- 204M1A0416

subject :- Analog Communications

Submitted by
G. Saroja

Submitted to
K. Sanjeev Rao Sir.

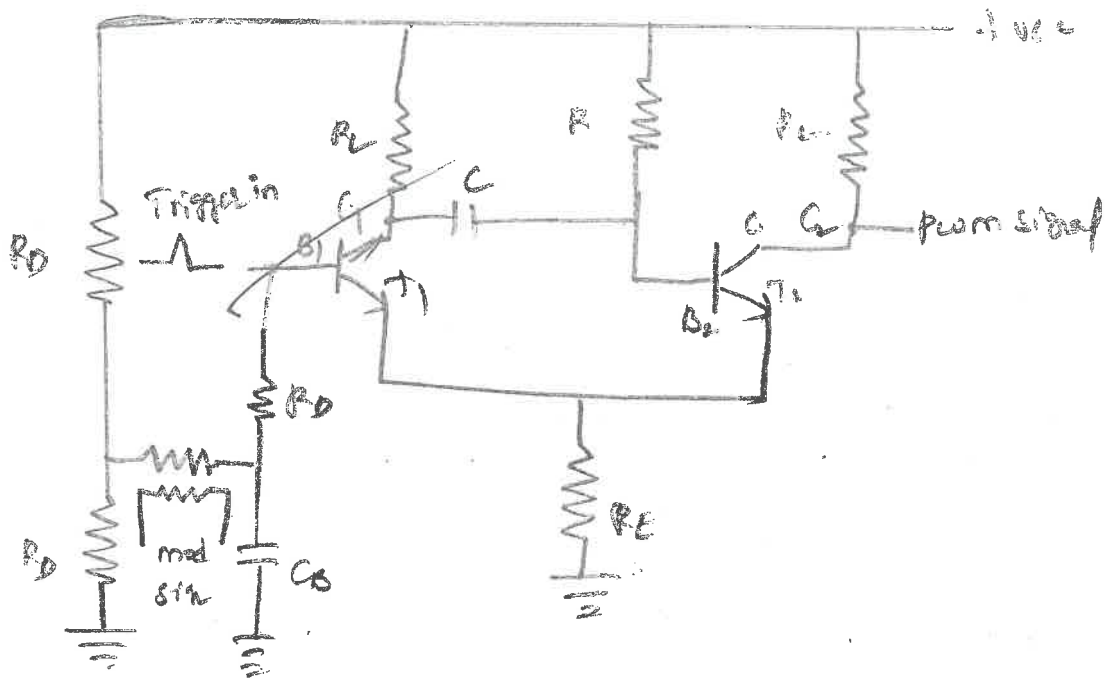
Surya
Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dt.

Assignment Received *JS*

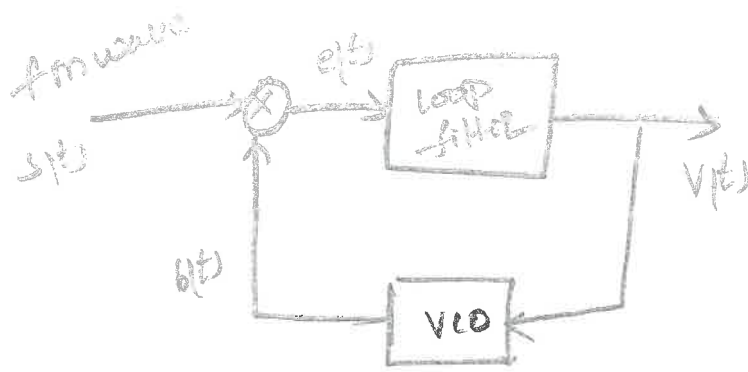
Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOG
PETLURIVARI PALEM
Narasaraopet (Mdl) Guntur Dt.

Generation of PWM

The process of changing the width of the train of pulse in accordance to the amplitude of modulating signal at the time of sampling is called pulse width modulation.



The stable state for above circuit is achieved when T_1 is off and T_2 is on. The positive going trigger pulse at B_1 switches T_1 on. As a result voltage at B_2 also falls and T_2 is switched off. C begins to charge up to the collector supply voltage at B_2 through resistor R . We can say that pulse width is controlled by the ip signal voltage and we get pulse width modulated waveform at the op. The waveform of PWM are shown in principal

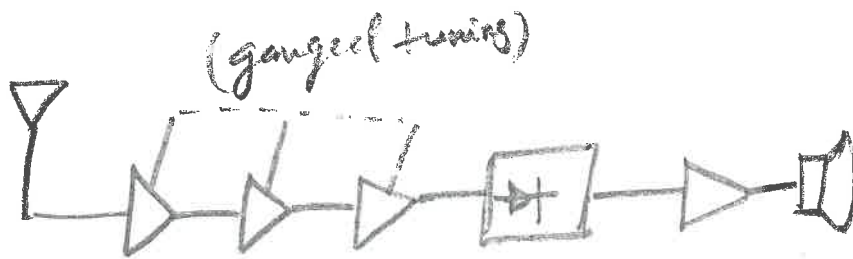


mathematical explanation

$$s(t) = A \sin[\omega_c t + \phi_1(t)]$$

$$\phi_1(t) = 2\pi k_f \int_0^t x(t) dt$$

3) The Block diagram of TRF receiver



A tuned radio frequency receiver is a type of radio receiver that is composed of one or more tuned radio frequency amplified stages followed by a detectable circuit to extract the audio signal and usually an audio frequency amplifier.

Department of Electronics & Communication Engineering
TUTORIAL TOPICS

Year / Branch / Sem:	II/ECE/II-II	Academic Year:	2022 – 23
Course Name & Code:	ANALOG COMMUNICATION & R2022043	Faculty Name:	K. SANJEEVA RAO

UNIT I

AMPLITUDE MODULATION:

- Introduction to communication system
- Need for modulation, Frequency Division Multiplexing
- Amplitude Modulation, Definition
- power relations in AM waves
- Generation of AM waves
- Detection of AM Waves

UNIT II

DSB & SSB MODULATION:

- Double side band suppressed carrier modulators
- time domain and frequency domain description
- Generation of DSBSC Waves
- Coherent detection of DSB-SC Modulated waves
- COSTAS Loop
- Frequency discrimination method for generation of AM SSB Modulated Wave
- Generation AM SSB Modulated waves
- Demodulation of SSB waves
- Generation of VSB Modulated wave
- Comparison of AM Techniques, Applications of different AM Systems, FDM.

UNIT III

ANGLE MODULATION:

- Frequency Modulation: Single tone frequency modulation
- Spectrum Analysis of Sinusoidal FM Wave
- Narrowband FM, Wideband FM
- Constant Average Power, Transmission bandwidth of FM Wave
- Generation of FM Waves
- Detection of FM Waves
- Phase locked loop
- Comparison of FM & AM.

UNIT IV

TRANSMITTERS:

- Radio Transmitter - Classification of Transmitter, AM Transmitter
- Effect of feedback on performance of AM Transmitter
- FM Transmitter –Variable reactance type and phase modulated FM Transmitter
- frequency stability in FM Transmitter.

RECEIVERS:

- Radio Receivers - Receiver Types
- Tuned radio frequency receiver
- Super heterodyne receiver
- Automatic Gain Control (AGC)
- FM Receiver, Comparison with AM Receiver
- Communication Receivers
- Amplitude Limiting

UNIT V

NOISE:

- Review of noise and noise sources
- noise figure
- Noise in Analog communication Systems
- Noise in DSB & SSB System
- Noise in AM System, Noise in Angle Modulation Systems
- Threshold effect in Angle Modulation System
- Pre-emphasis & de-emphasis

PULSE MODULATION:

- Types of Pulse modulation
- Pulse Amplitude Modulation (Single polarity, double polarity)
- PWM: Generation & demodulation of PWM
- PPM: Generation and demodulation of PPM
- Time Division Multiplexing
- TDM Vs FDM

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Midi), Guntur, Dist

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Midi), Guntur, Dist

42		TOTAL NO OF CLASSES	62
----	--	---------------------	----

FACULTY

H.O.D

PRINCIPAL

Principal
Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, Dr.

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, Dr.



A.M. REDDY

Memorial College of Engineering and Technology

Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada

SPONSORED BY

ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution

Web : www.amreddyengineering.ac.in

E.mail: principal.amreddyengineering@gmail.com

VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM,

NARASARAOPET PALNADU (DIST) - 522601,

CONTACT : 08647-247190.

II-Assignment Question Paper, June- 2023

Year/Sem: II/I	Programme: B.Tech-ECE	Course Code: R2022043	Regulation :R20	
Course Name: ANALOG COMMUNICATION		Total Marks :5		
Q.No	Answer All Questions	Marks	Levels of Bloom's taxonomy	CO
1	Define modulation and Demodulation?	1	Knowledge	1
2	Draw and Explain the Balanced ring modulator with waveforms?	2	Explanation	1
3	Explain the DSB-SC Signal detection using coherent detector?	2	Enhancement	3

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, Dt

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, Dt

ANALOG COMMUNICATIONS

BY

K. SANJEEVARAO,

Assistant Professor

Principai
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur.C

Principai
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur.C

UNIT IV

TRANSMITTERS & RECEIVERS: Radio Transmitter

Classification of Transmitter, AM

Transmitter, Effect of feedback on performance of AM Transmitter, FM Transmitter –Variable reactance type and phase modulated FM Transmitter, frequency stability in FM Transmitter.

Radio Receiver - Receiver Types - Tuned radio frequency receiver, Super heterodyne receiver, RF section and Characteristics - Frequency changing and tracking, Intermediate frequency, AGC, FM Receiver, Comparison with AM Receiver, Amplitude limiting. Communication Receivers, extensions of super heterodyne principle and additional circuits.

UNIT V

NOISE: Review of noise and noise sources, noise figure, Noise in Analog communication Systems, Noise in DSB & SSB System, Noise in AM System, Noise in Angle Modulation Systems, Threshold effect in Angle Modulation System, Pre-emphasis & de-emphasis

PULSE MODULATION: Types of Pulse modulation, PAM (Single polarity, double polarity) PWM: Generation & demodulation of PWM, PPM, Generation and demodulation of PPM, Time Division Multiplexing, TDM Vs FDM

TEXTBOOKS:

1. Principles of Communication Systems–HTaub&D.Schilling, GautamSahe, TMH, 3rd Edition, 2007.
2. Principles of Communication Systems-Simon Haykin, John Wiley, 2nd Edition, 2007.
3. Modern Digital and Analog Communication Systems –B.P.Lathi, Zhi Ding, Hari Mohan Gupta, Oxford University Press, 4th Edition, 2017

REFERENCES:

1. Electronics & Communication System– George Kennedy and Bernard Davis, TMH 2004.
2. Communication Systems–R.P.Singh, SP Sapre, Second Edition TMH, 2007.
3. Electronic Communication systems–Tomasi, Pearson, fourth Edition, 2007.


Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, D

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, D

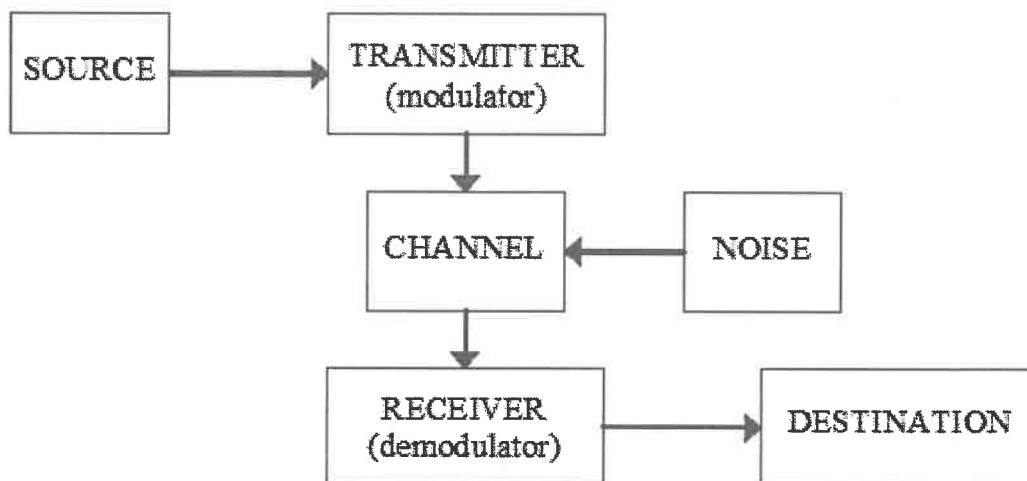
UNIT-I

Introduction to Communication System

Communication is the process by which information is exchanged between individuals through a medium.

Communication can also be defined as the transfer of information from one point in space and time to another point.

The basic block diagram of a communication system is as follows.



- **Transmitter:** Couples the message into the channel using high frequency signals.
- **Channel:** The medium used for transmission of signals
- **Modulation:** It is the process of shifting the frequency spectrum of a signal to a frequency range in which more efficient transmission can be achieved.
- **Receiver:** Restores the signal to its original form.
- **Demodulation:** It is the process of shifting the frequency spectrum back to the original baseband frequency range and reconstructing the original form.

Modulation:

Modulation is a process that causes a shift in the range of frequencies in a signal.

- Signals that occupy the same range of frequencies can be separated.
- Modulation helps in noise immunity, attenuation - depends on the physical medium.

The below figure shows the different kinds of analog modulation schemes that are available

Principal
Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dt .

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dt .

Example: Double sideband with carrier (DSB-WC), Double- sideband suppressed carrier (DSB-SC), Single sideband suppressed carrier (SSB-SC), vestigial sideband (VSB)

- **Angle modulation (frequency modulation & phase modulation)**

Example: Narrow band frequency modulation (NBFM), Wideband frequency modulation (WBFM), Narrowband phase modulation (NBPM), Wideband phase modulation (WBPM)

Pulse Modulation

- Carrier is a train of pulses
- Example: Pulse Amplitude Modulation (PAM), Pulse width modulation (PWM) , Pulse Position Modulation (PPM)

Digital Modulation


- Modulating signal is analog ○Example: Pulse Code Modulation (PCM), Delta Modulation (DM), Adaptive Delta Modulation (ADM), Differential Pulse Code Modulation (DPCM), Adaptive Differential Pulse Code Modulation (ADPCM) etc.
- Modulating signal is digital (binary modulation) ○Example: Amplitude shift keying (ASK), frequency Shift Keying (FSK), Phase Shift Keying (PSK) etc

Frequency Division Multiplexing

Multiplexing is the name given to techniques, which allow more than one message to be transferred via the same communication channel. The channel in this context could be a transmission line, *e.g.* a twisted pair or co-axial cable, a radio system or a fibre optic system *etc.*

FDM is derived from AM techniques in which the signals occupy the same physical 'line' but in different frequency bands. Each signal occupies its own specific band of frequencies all the time, *i.e.* the messages share the channel **bandwidth**.

- FDM – messages occupy **narrow** bandwidth – all the time.


Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, Dt .

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur

- Bandwidth - 10 kHz

Various forms of Amplitude Modulation

- Conventional Amplitude Modulation (Alternatively known as Full AM or Double Sideband Large carrier modulation (DSBLC) /Double Sideband Full Carrier (DSBFC)
- Double Sideband Suppressed carrier (DSBSC) modulation
- Single Sideband (SSB) modulation
- Vestigial Sideband (VSB) modulation

Time Domain and Frequency Domain Description

It is the process where, the amplitude of the carrier is varied proportional to that of the message signal.

Let $m(t)$ be the base-band signal, $m(t) \longleftrightarrow M(\omega)$ and $c(t)$ be the carrier, $c(t) = A_c \cos(\omega_c t)$. f_c is chosen such that $f_c \gg W$, where W is the maximum frequency component of $m(t)$. The amplitude modulated signal is given by

$$s(t) = A_c [1 + k_a m(t)] \cos(\omega_c t)$$

Fourier Transform on both sides of the above equation

$$S(\omega) = \pi A_c / 2 (\delta(\omega - \omega_c) + \delta(\omega + \omega_c)) + k_a A_c / 2 (M(\omega - \omega_c) + M(\omega + \omega_c))$$

k_a is a constant called amplitude sensitivity.

$k_a m(t) < 1$ and it indicates percentage modulation.

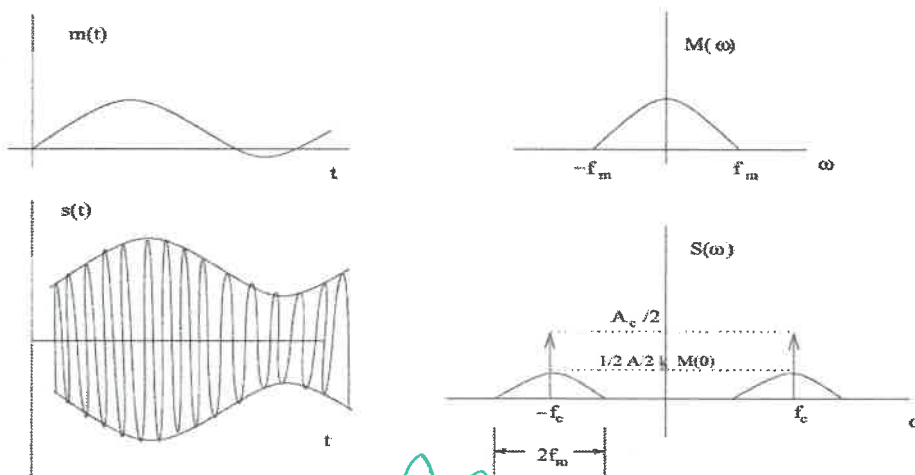


Fig.2. Amplitude modulation in time and frequency domain

Single Tone Modulation:

Power relations in AM waves:

Consider the expression for single tone/sinusoidal AM wave

$$s(t) = A_c \cos(2\pi f_c t) + \frac{1}{2} m A_c \cos[2\pi(f_c + f_m)t] + \frac{1}{2} m A_c \cos[2\pi(f_c - f_m)t] \dots\dots\dots(1)$$

This expression contains three components. They are carrier component, upper side band and lower side band. Therefore Average power of the AM wave is sum of these three components.

Therefore the total power in the amplitude modulated wave is given by

$$P_t = \frac{V_{car}^2}{R} + \frac{V_{LSB}^2}{R} + \frac{V_{USB}^2}{R} \dots\dots\dots(2)$$

Where all the voltages are rms values and R is the resistance, in which the power is dissipated.

$$P_c = \frac{V_{car}^2}{R} = \frac{\left(\frac{A_c}{\sqrt{2}}\right)^2}{R} = \frac{A_c^2}{2R}$$

$$P_{LSB} = \frac{V_{LSB}^2}{R} = \left(\frac{mA_c}{2\sqrt{2}}\right)^2 \frac{1}{R} = \frac{m^2 A_c^2}{8R} = \frac{m^2}{4} P_c$$

$$P_{USB} = \frac{V_{USB}^2}{R} = \left(\frac{mA_c}{2\sqrt{2}}\right)^2 \frac{1}{R} = \frac{m^2 A_c^2}{8R} = \frac{m^2}{4} P_c$$

Therefore total average power is given by

$$P_t = P_c + P_{LSB} + P_{USB}$$

$$P_t = P_c + \frac{m^2}{4} P_c + \frac{m^2}{4} P_c$$

$$P_t = P_c \left(1 + \frac{m^2}{4} + \frac{m^2}{4}\right)$$

$$P_t = P_c \left(1 + \frac{m^2}{2}\right) \dots\dots\dots(3)$$

The ratio of total side band power to the total power in the modulated wave is given by

Principal

A.M REDDY MEMORIAL COLLEGE OF ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur Dist.

A.M REDDY MEMORIAL COLLEGE OF ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur

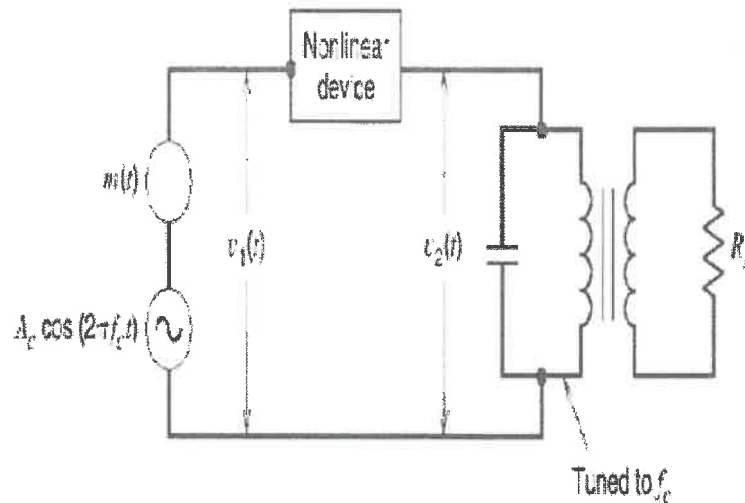


Fig.4. Square Law Modulator

Consider a non-linear device to which a carrier $c(t) = A_c \cos(2\pi f_c t)$ and an information signal $m(t)$ is fed simultaneously as shown in figure 4. The total input to the device at any instant is

$$V_{in} = c(t) + m(t)$$

$$V_{in} = A_c \cos 2\pi f_c t + m(t)$$

As the level of the input is very small, the output can be considered up to square of the input, i.e., $V_o = a_0 + a_1 V_{in} + a_2 V_{in}^2$

$$V_o = a_0 + a_1 [A_c \cos 2\pi f_c t + m(t)] + a_2 [A_c \cos 2\pi f_c t + m(t)]^2$$

$$V_o = a_0 + a_1 A_c \cos 2\pi f_c t + a_1 m(t) + \frac{a_2 A_c^2}{2} (1 + \cos 4\pi f_c t) + a_2 [m(t)]^2 + 2a_2 m(t) A_c \cos 2\pi f_c t$$

$$V_o = a_0 + a_1 A_c \cos 2\pi f_c t + a_1 m(t) + \frac{a_2 A_c^2}{2} \cos 4\pi f_c t + a_2 m^2(t) + 2a_2 m(t) A_c \cos 2\pi f_c t$$

Taking Fourier transform on both sides, we get

$$V_o(f) = \left(a_0 + \frac{a_2 A_c^2}{2}\right) \delta(f) + \frac{a_1 A_c}{2} [\delta(f - f_c) + \delta(f + f_c)] + a_1 M(f) +$$

$$\frac{a_2 A_c^2}{4} [\delta(f - 2f_c) + \delta(f + 2f_c)] + a_2 M(f) + a_2 A_c [M(f - f_c) + M(f + f_c)]$$

Therefore, the square law device output V_o consists of the dc component at $f = 0$. The information signal ranging from 0 to W Hz and its second harmonics are signal at f_c and $2f_c$.

Principal

A.M REDDY MEMORIAL COLLEGE OF ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM, Narasaraopet (Mdl), Guntur Dist. Narasaraopet (Mdl), Guntur

When the peak amplitude of $c(t)$ is maintained more than that of information signal, the operation is assumed to be dependent on only $c(t)$ irrespective of $m(t)$.

When $c(t)$ is positive, $v_2=v_1$ since the diode is forward biased. Similarly, when $c(t)$ is negative, $v_2=0$ since diode is reverse biased. Based upon above operation, switching response of the diode is periodic rectangular wave with an amplitude unity and is given by

$$p(t) = \frac{1}{2} + \frac{1}{\pi} \sum_{n=-\infty}^{\infty} \frac{(-1)^{n-1}}{2n-1} \cos(2\pi f_c t (2n-1))$$

$$p(t) = \frac{1}{2} + \frac{2}{\pi} \cos(2\pi f_c t) - \frac{2}{3\pi} \cos(6\pi f_c t) + \dots$$

Therefore the diode response V_o is a product of switching response $p(t)$ and input v_1 .

$$v_2 = v_1 * p(t)$$

$$V_2 = [A_c \cos 2\pi f_c t + m(t)] \left[\frac{1}{2} + \frac{2}{\pi} \cos 2\pi f_c t - \frac{2}{3\pi} \cos 6\pi f_c t + \dots \right]$$

Applying the Fourier Transform, we get

$$\begin{aligned} V_2(f) &= \frac{A_c}{4} [\delta(f - f_c) + \delta(f + f_c)] + \frac{M(f)}{2} + \frac{A_c}{\pi} \delta(f) \\ &+ \frac{A_c}{2\pi} [\delta(f - 2f_c) + \delta(f + 2f_c)] + \frac{1}{\pi} [M(f - f_c) + M(f + f_c)] \\ &- \frac{A_c}{6\pi} [\delta(f - 4f_c) + \delta(f + 4f_c)] - \frac{A_c}{3\pi} [\delta(f - 2f_c) + \delta(f + 2f_c)] \\ &- \frac{1}{3\pi} [M(f - 3f_c) + M(f + f_c)] \end{aligned}$$

The diode output v_2 consists of

a dc component at $f=0$.

Information signal ranging from 0 to w Hz and infinite number of frequency bands centered at $f, 2f_c, 3f_c, 4f_c, \dots$

The required AM signal centred at f_c can be separated using band pass filter. The lower cut off-frequency for the band pass filter should be between w and f_c-w and the upper cut-off frequency between f_c+w and $2f_c$. The filter output is given by the equation

Principal
A.M REDDY MEMORIAL COLLEGE OF ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasareopet (Midi), Guntur Dt.

Principal
A.M REDDY MEMORIAL COLLEGE OF ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasareopet (Midi), Guntur Dt.

$$V_o = a_o + a_1 s(t) + a_2 [s(t)]^2$$

$$V_o = a_o + a_1 A_c \cos 2\pi f_c t + a_1 A_c K_a m(t) \cos 2\pi f_c t + a_2 [A_c \cos 2\pi f_c t + A_c k_a m(t) \cos 2\pi f_c t]^2$$

Applying Fourier transform on both sides, we get

$$\begin{aligned} V_o(f) = & \left[a_o + \frac{a_2 A_c^2}{2} \right] \delta(f) + \frac{a_1 A_c}{2} [\delta(f - f_c) + \delta(f + f_c)] \\ & + \frac{a_1 A_c K_a}{2} [M(f - f_c) + M(f + f_c)] + \frac{a_2 A_c^2 K_a^2}{4} [M(f - 2f_c) + M(f + 2f_c)] \\ & + \frac{a_2 A_c^2 K_a^2}{2} \left[M(f) \right]_{\pm 2W} + \frac{a_2 A_c^2 K_a^2}{2} [M(f - 2f_c) + M(f + 2f_c)] \\ & + \frac{a_2 A_c^2}{4} [\delta(f - 2f_c) + \delta(f + 2f_c)] + a_2 A_c^2 K_a [M(f)] \end{aligned}$$

The device output consists of a dc component at $f=0$, information signal ranging from 0-W Hz and its second harmonics and frequency bands centered at f_c and $2f_c$. The required information can be separated using low pass filter with cut off frequency ranging between W and $f_c - w$. The filter output is given by

$$m'(t) = \left(a_o + \frac{a_2 A_c^2}{2} \right) + a_2 A_c^2 K_a m(t) + \frac{a_2 A_c^2 K_a^2 m^2(t)}{2}$$

DC component + message signal + second harmonic

The dc component (first term) can be eliminated using a coupling capacitor or a transformer. The effect of second harmonics of information signal can be reduced by maintaining its level very low. When $m(t)$ is very low, the filter output is given by

$$m^1(t) = a_2 A_c^2 K_a m(t)$$

When the information level is very low, the noise effect increases at the receiver, hence the system clarity is very low using square law demodulator.

Envelope Detector

It is a simple and highly effective system. This method is used in most of the commercial AM radio receivers. An envelope detector is as shown below.

Dr. J. S. Reddy

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur (Dist)

Advantages and Disadvantages of AM:

Advantages of AM:

- Generation and demodulation of AM wave are easy.
- AM systems are cost effective and easy to build.

Disadvantages:

- AM contains unwanted carrier component, hence it requires more transmission power.
- The transmission bandwidth is equal to twice the message bandwidth.


Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur (Dist)

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl) Guntur

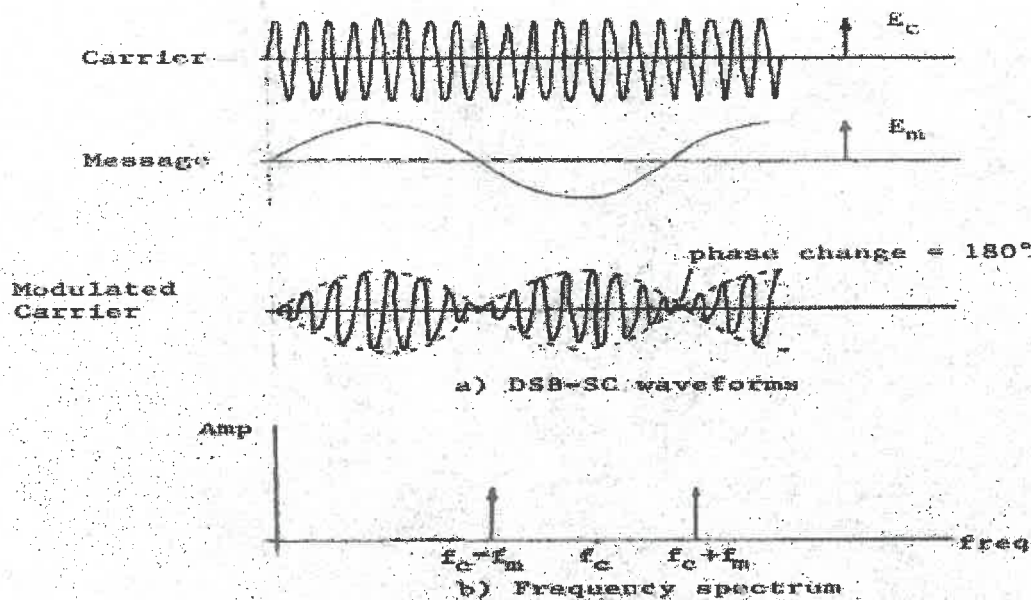


Fig.1. (a) DSB-SC waveform (b) DSB-SC Frequency Spectrum

The envelope of a DSBSC modulated signal is therefore different from the message signal and the Fourier transform of $s(t)$ is given by

$$S(f) = \frac{A_c}{2} [M(f - f_c) + M(f + f_c)]$$

For the case when base band signal $m(t)$ is limited to the interval $-W < f < W$ as shown in figure below, we find that the spectrum $S(f)$ of the DSBSC wave $s(t)$ is as illustrated below. Except for a change in scaling factor, the modulation process simply translates the spectrum of the base band signal by f_c . The transmission bandwidth required by DSBSC modulation is the same as that for AM.

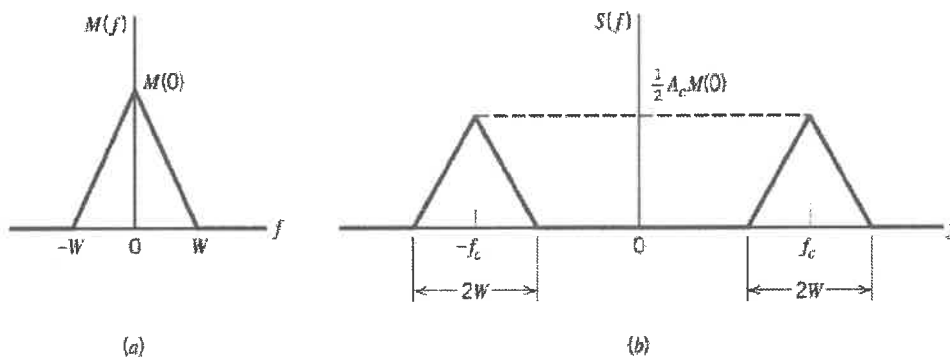


Figure: Message and the corresponding DSBSC spectrum

Generation of DSBSC Waves:

Balanced Modulator (Product Modulator)

A balanced modulator consists of two standard amplitude modulators arranged in a balanced configuration so as to suppress the carrier wave as shown in the following block

Principal
 J. J. REDDY MEMORIAL COLLEGE OF ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Md), Guntur Dt. - Narasaraopet (Md), Guntur Dt.

Thus the ring modulator in its ideal form is a product modulator for square wave carrier and the base band signal $m(t)$. The square wave carrier can be expanded using Fourier series as

$$c(t) = \frac{4}{\pi} \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{2n-1} \cos(2\pi f_c t (2n-1))$$

Therefore the ring modulator out put is given by

$$s(t) = m(t)c(t)$$

$$s(t) = m(t) \left[\frac{4}{\pi} \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{2n-1} \cos(2\pi f_c t (2n-1)) \right]$$

From the above equation it is clear that output from the modulator consists entirely of modulation products. If the message signal $m(t)$ is band limited to the frequency band $-w < f < w$, the output spectrum consists of side bands centred at f_c .

Detection of DSB-SC waves:

Coherent Detection:

The message signal $m(t)$ can be uniquely recovered from a DSBSC wave $s(t)$ by first multiplying $s(t)$ with a locally generated sinusoidal wave and then low pass filtering the product as shown.

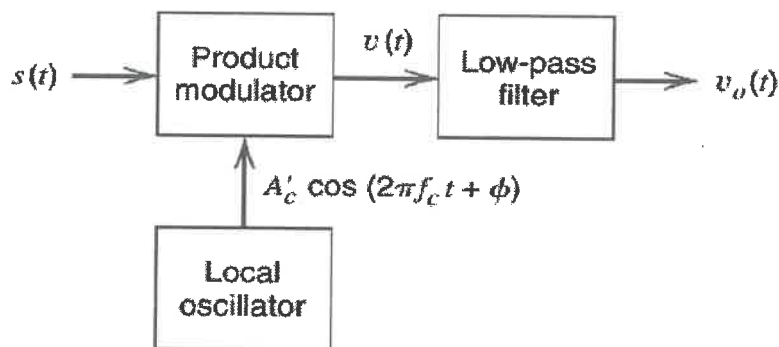

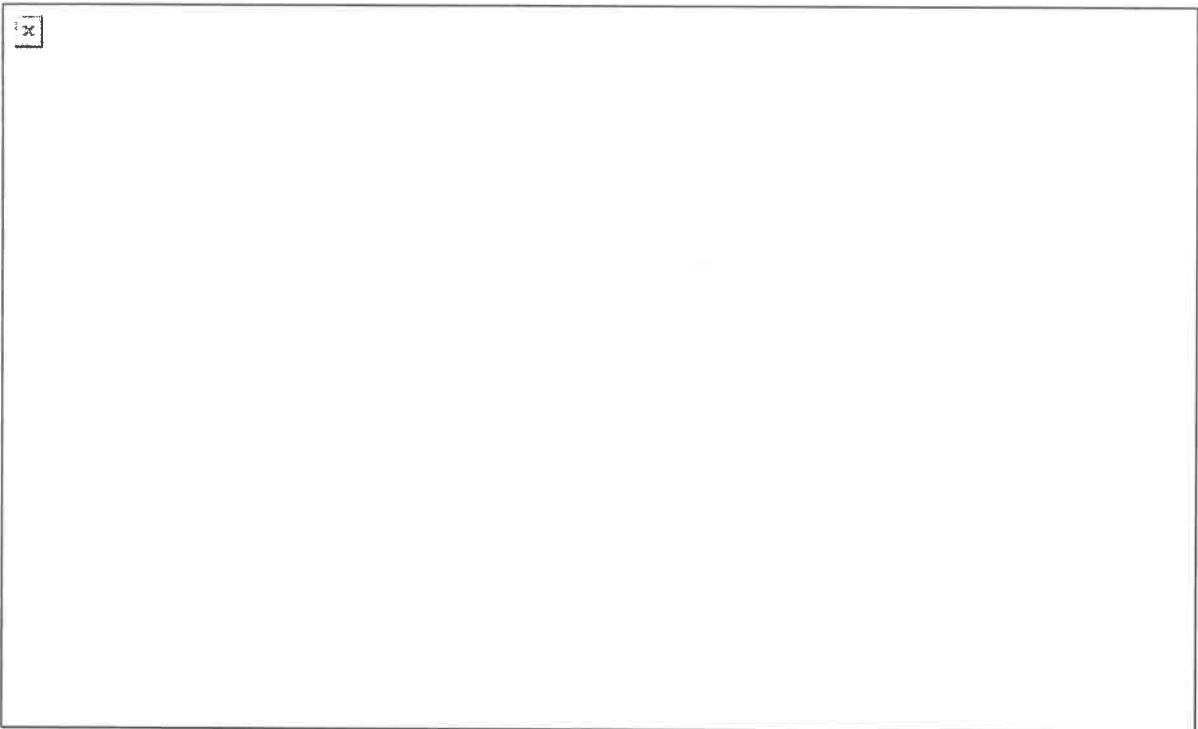


Fig.5 : Coherent detector

It is assumed that the local oscillator signal is exactly coherent or synchronized, in both frequency and phase, with the carrier wave $c(t)$ used in the product modulator to generate $s(t)$. This method of demodulation is known as coherent detection or synchronous detection.


 Principal
 A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Mdl), Guntur Dist.



F
i
g
·
7
·
C
o
s
t
a
s

R
e
c
e
i
v

er

The frequency of the local oscillator is adjusted to be the same as the carrier frequency f_c . The detector in the upper path is referred to as the in-phase coherent detector or I-channel, and that in the lower path is referred to as the quadrature-phase coherent detector or Q-channel.

These two detectors are coupled together to form a negative feedback system designed in such a way as to maintain the local oscillator synchronous with the carrier wave. Suppose the local oscillator signal is of the same phase as the carrier $c(t) = A_c \cos(2\pi f_c t)$ wave used to generate the incoming DSBSC wave. Then we find that the I-channel output contains the desired demodulated signal $m(t)$, whereas the Q-channel output is zero due to quadrature null effect of the Q-channel. Suppose that the local oscillator phase drifts from its proper value by a small angle ϕ radians. The I-channel output will remain essentially unchanged, but there will be some signal appearing at the Q-channel output, which is proportional to $\sin(\phi) \approx \phi$ for small ϕ .

This Q-channel output will have same polarity as the I-channel output for one direction of local oscillator phase drift and opposite polarity for the opposite direction of local oscillator phase drift. Thus, by combining the I-channel and Q-channel outputs in a phase discriminator (which consists of a multiplier followed by a LPF), a dc control signal is obtained that automatically corrects for the local phase errors in the voltage-controlled oscillator.

Radio Transmitters

There are two approaches in generating an AM signal. These are known as low and high-level modulation. They're easy to identify: A low level AM signal performs the

Principal
ANANDRAJ COLLEGE OF
ENGINEERING & TECHNOLOGY
PETTURIVARA PALEM
Narasaraopet (M.D.)
Guntur (D)

Voltage Regulation: An oscillator can also be pulled off frequency if its power supply voltage isn't held constant. In most transmitters, the supply voltage to the oscillator is regulated at a constant value. The regulated voltage value is often between 5 and 9 volts; zener diodes and three-terminal regulator ICs are commonly used voltage regulators. Voltage regulation is especially important when a transmitter is being powered by batteries or an automobile's electrical system. As a battery discharges, its terminal voltage falls. The DC supply voltage in a car can be anywhere between 12 and 16 volts, depending on engine RPM and other electrical load conditions within the vehicle.

Modulator: The stabilized RF carrier signal feeds one input of the modulator stage. The modulator is a variable-gain (nonlinear) amplifier. To work, it must have an RF carrier signal and an AF information signal. In a low-level transmitter, the power levels are low in the oscillator, buffer, and modulator stages; typically, the modulator output is around 10 mW (700 mV RMS into 50 ohms) or less.

AF Voltage Amplifier: In order for the modulator to function, it needs an information signal. A microphone is one way of developing the intelligence signal, however, it only produces a few millivolts of signal. This simply isn't enough to operate the modulator, so a voltage amplifier is used to boost the microphone's signal. The signal level at the output of the AF voltage amplifier is usually at least 1 volt RMS; it is highly dependent upon the transmitter's design. Notice that the AF amplifier in the transmitter is only providing a voltage gain, and not necessarily a current gain for the microphone's signal. The power levels are quite small at the output of this amplifier; a few mW at best.

RF Power Amplifier: At test point D the modulator has created an AM signal by impressing the information signal from test point C onto the stabilized carrier signal from test point B at the buffer amplifier output. This signal (test point D) is a complete AM signal, but has only a few milliwatts of power. The RF power amplifier is normally built with several stages. These stages increase both the voltage and current of the AM signal. We say that power amplification occurs when a circuit provides a current gain. In order to accurately amplify the tiny AM signal from the modulator, the RF power amplifier stages must be linear. You might recall that amplifiers are divided up into "classes," according to the conduction angle of the active device within. Class A and class B amplifiers are considered to be linear amplifiers, so the RF power amplifier stages will normally be constructed using one or both of these types of amplifiers. Therefore, the signal at test point E looks just like that of test point D; it's just much bigger in voltage and current.

Antenna Coupler: The antenna coupler is usually part of the last or final RF power amplifier, and as such, is not really a separate active stage. It performs no amplification, and has no active devices. It performs two important jobs: Impedance matching and filtering. For an RF power amplifier to function correctly, it must be supplied with a load resistance equal to that for which it was designed.

The antenna coupler also acts as a low-pass filter. This filtering reduces the amplitude of harmonic energies that may be present in the power amplifier's output. (All amplifiers generate harmonic distortion, even "linear" ones.) For example, the transmitter may be tuned to operate on 1000 kHz. Because of small nonlinearities in the amplifiers of the transmitter,

Principal
MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARIPALEM
Narasaraopet (M.D.), Guntur (Dt.)

High Level Transmitters

- Have better DC efficiency than low-level transmitters, and are very well suited for battery operation.
- Are restricted to generating AM modulation only.

Introduction of SSB-SC

Standard AM and DSBSC require transmission bandwidth equal to twice the message bandwidth. In both the cases spectrum contains two side bands of width W Hz, each. But the upper and lower sides are uniquely related to each other by the virtue of their symmetry about the carrier frequency. That is, given the amplitude and phase spectra of either side band, the other can be uniquely determined. Thus, if only one side band is transmitted, and if both the carrier and the other side band are suppressed at the transmitter, no information is lost. This kind of modulation is called SSBSC and spectral comparison between DSBSC and SSBSC is shown in the figures 1 and 2.

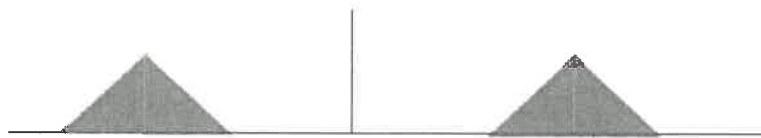


Figure.1 : Spectrum of the DSBSC wave



Figure .2 : Spectrum of the SSBSC wave

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PELLURIVARI PALEM
Narasaraopet (M.D), Guntur Dist.

modulation is to translate the spectrum of the modulating wave, either with or without inversion, to a new location in the frequency domain. The advantage of SSB modulation is reduced bandwidth and the elimination of high power carrier wave. The main disadvantage is the cost and complexity of its implementation.

Generation of SSB wave:

Frequency discrimination method

Consider the generation of SSB modulated signal containing the upper side band only. From a practical point of view, the most severe requirement of SSB generation arises from the unwanted sideband, the nearest component of which is separated from the desired side band by twice the lowest frequency component of the message signal. It implies that, for the generation of an SSB wave to be possible, the message spectrum must have an energy gap centered at the origin as shown in figure 7. This requirement is naturally satisfied by voice signals, whose energy gap is about 600Hz wide.

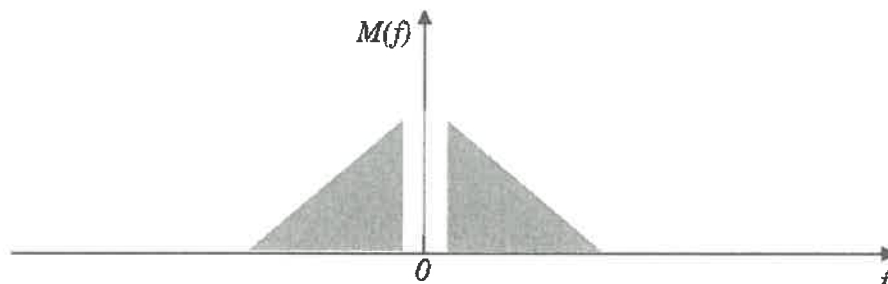


Figure .7 : Message spectrum with energy gap at the origin

The frequency discrimination or filter method of SSB generation consists of a product modulator, which produces DSBSC signal and a band-pass filter to extract the desired side band and reject the other and is shown in the figure 8.

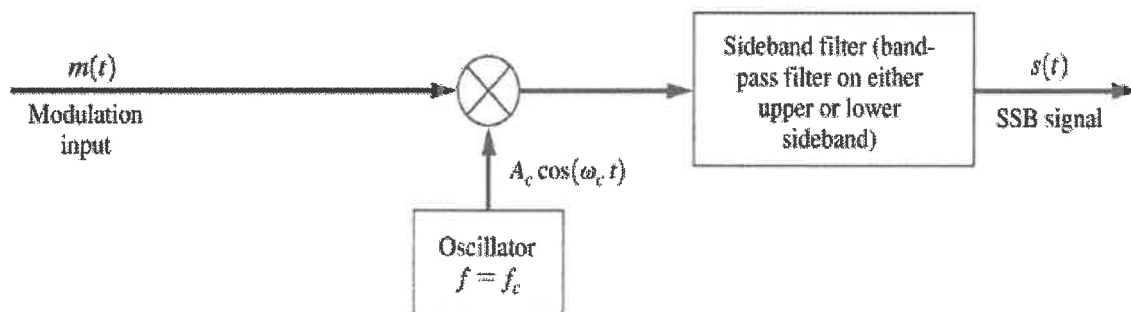


Figure .8 : Frequency discriminator to generate SSBSC wave

Application of this method requires that the message signal satisfies two conditions:

1. The message signal $m(t)$ has no low-frequency content. Example: speech, audio, music.
2. The highest frequency component W of the message signal $m(t)$ is much less than the carrier frequency f_c .

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURVA
PETLURVA
Narasaraopet (M.D), Guntur District
Narasaraopet (M.D), Guntur District

$$H(f) = \begin{cases} -j, f > 0 \\ 0, f = 0 \\ j, f < 0 \end{cases} \quad \text{----- (1)}$$

and the Signum function given by

$$\text{sgn}(f) = \begin{cases} 1, f > 0 \\ 0, f = 0 \\ -1, f < 0 \end{cases}$$

The function $H(f)$ can be expressed using Signum function as given by 2

$$H(f) = -j \text{sgn}(f) \quad \text{----- (2)}$$

We know that $1e^{-j\pi/2} = -j$, $1e^{j\pi/2} = j$ and $e^{\pm j\theta} = \cos(\theta) \pm j \sin(\theta)$


Therefore,

$$H(f) = \begin{cases} 1e^{-j\pi/2}, f > 0 \\ 1e^{j\pi/2}, f < 0 \end{cases}$$

Thus the magnitude $|H(f)| = 1$, for all f , and angle

$$\angle H(f) = \begin{cases} -\pi/2, f > 0 \\ +\pi/2, f < 0 \end{cases}$$

The device which possesses such a property is called Hilbert transformer. Whenever a signal is applied to the Hilbert transformer, the amplitudes of all frequency components of the input signal remain unaffected. It produces a phase shift of -90° for all positive frequencies, while a phase shifts of 90° for all negative frequencies of the signal.


 Principal
 A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Mdi), Guntur Dist.

Principal
 A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Mdi), Guntur Dist.

$$\hat{x}(t) = x(t) * h(t)$$

$$\hat{x}(t) = x(t) * \frac{1}{\pi t}$$

$$\hat{x}(t) = \frac{1}{\pi} \int_{-\infty}^{+\infty} \frac{x(\tau)}{(t-\tau)} d\tau \quad \text{----- (4)}$$

The equation 3.5 gives the Hilbert transform of $x(t)$.

The inverse Hilbert transform $x(t)$ is given by

$$x(t) = \frac{-1}{\pi} \int_{-\infty}^{+\infty} \frac{\hat{x}(\tau)}{(t-\tau)} d\tau \quad \text{----- (5)}$$

We have $\hat{x}(t) = x(t) * h(t)$

The Fourier transform $\hat{X}(f)$ of $\hat{x}(t)$ is given by

$$\hat{X}(f) = X(f)H(f)$$

$$\hat{X}(f) = -j \operatorname{sgn}(f) X(f) \quad \text{----- (6)}$$

Jee
Principal

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY PETLURIVARI PALEM
PETLURIVARI PALEM Narasaraopet (Md), Guntur C
Narasaraopet (Md), Guntur, Dt

$$S_Q(f) = \begin{cases} j[S(f-f_c) - S(f+f_c)], & -w \leq f \leq w \\ 0, & \text{elsewhere} \end{cases} \quad \text{----- (3)}$$

where $-w < f < w$ defines the frequency band occupied by the message signal $m(t)$.

Consider the SSB wave that is obtained by transmitting only the upper side band, shown in figure 10 . Two frequency shifted spectras $s(f-f_c)$ and $s(f+f_c)$ are shown in figure 11 and figure 12 respectively. Therefore, from equations 2 and 3 , it follows that the corresponding spectra of the in-phase component $S_I(t)$ and the quadrature component $S_Q(t)$ are as shown in figure 13 and 14 respectively.

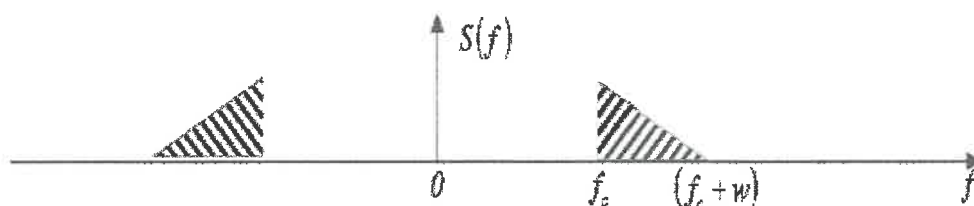


Figure 10 : Spectrum of SSBSC-USB

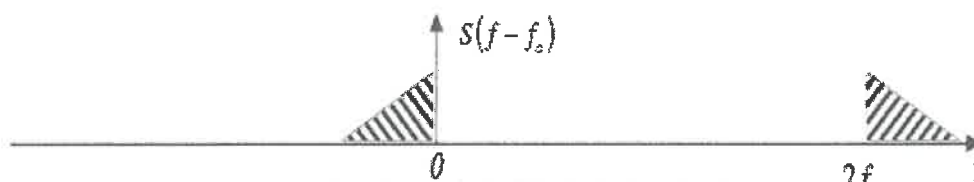


Figure 11 : Spectrum of SSBSC-USB shifted right by f_c

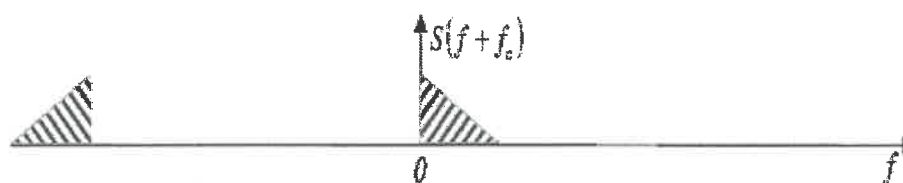


Figure 12 : Spectrum of SSBSC-USB shifted left by f_c

Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM,
Narasaraopet (Mdi), Guntur, Dr.

Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM,
Narasaraopet

But from the discussions on Hilbert transforms, it is shown that

$$-j \operatorname{sgn}(f) M(f) = \hat{M}(f) \quad \text{----- (6)}$$

where $\hat{M}(f)$ is the Fourier transform of the Hilbert transform of $m(t)$. Hence the substituting equation (6) in (5), we get

$$s_Q(f) = \frac{1}{2} A_c \hat{M}(f) \quad \text{----- (7)}$$

Therefore quadrature component $s_Q(t)$ is defined by equation 8

$$s_Q(t) = \frac{1}{2} A_c \hat{m}(t) \quad \text{----- (8)}$$

Therefore substituting equations (4) and (8) in equation in (1), we find that canonical representation of an SSB wave $s(t)$ obtained by transmitting only the upper side band is given by the equation 9

$$s_U(t) = \frac{1}{2} A_c m(t) \cos(2\pi f_c t) - \frac{1}{2} A_c \hat{m}(t) \sin(2\pi f_c t) \quad \text{----- (9)}$$

Following the same procedure, we can find the canonical representation for an SSB wave $s_L(t)$ obtained by transmitting only the lower side band is given by

$$s_L(t) = \frac{1}{2} A_c m(t) \cos(2\pi f_c t) + \frac{1}{2} A_c \hat{m}(t) \sin(2\pi f_c t) \quad \text{----- (10)}$$

Phase discrimination method for generating SSB wave:

Time domain description of SSB modulation leads to another method of SSB generation using the equations 9 or 10. The block diagram of phase discriminator is as shown in figure 15.

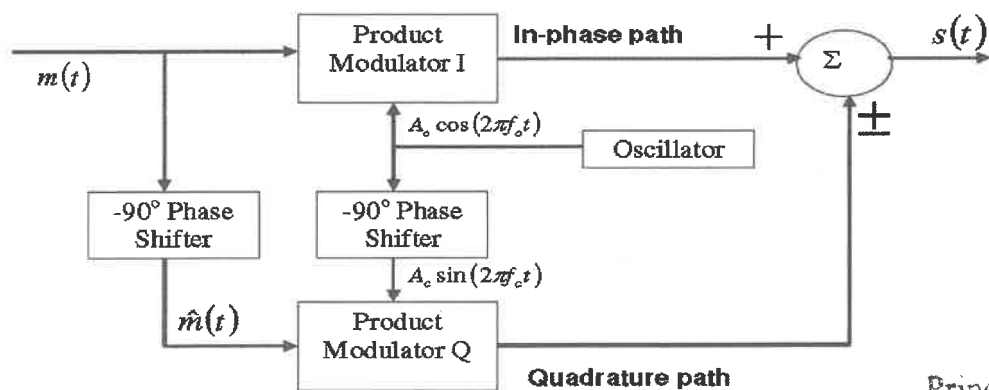


Figure 15 : Block diagram of phase discriminator

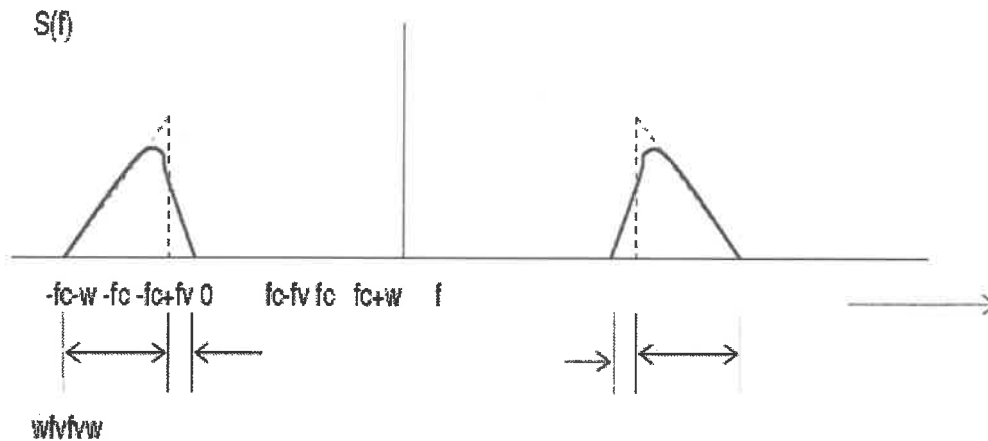
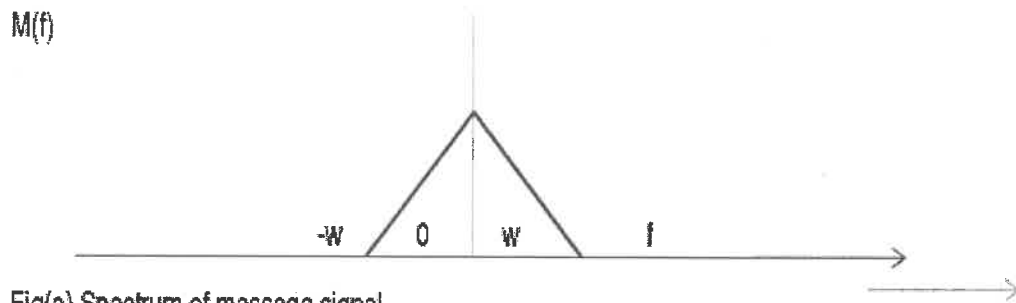
Principal

A.M REDDY MEMORIAL COLLEGE OF ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (M.V) Guntur Dist.

Vestigial sideband is a type of Amplitude modulation in which one side band is completely passed along with trace or tail or vestige of the other side band. VSB is a compromise between SSB and DSBSC modulation. In SSB, we send only one side band, the Bandwidth required to send SSB wave is w . SSB is not appropriate way of modulation when the message signal contains significant components at extremely low frequencies. To overcome this VSB is used.

Frequency Domain Description

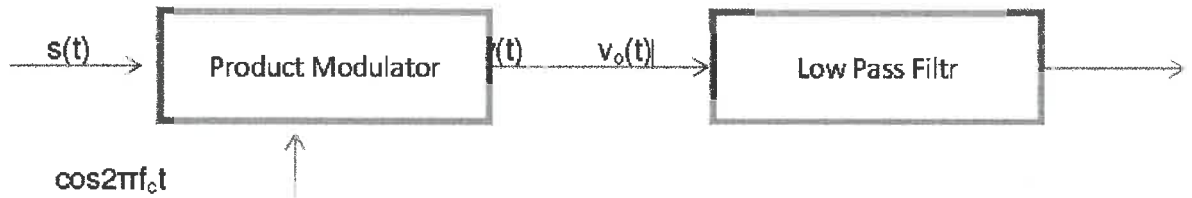
The following Fig illustrates the spectrum of VSB modulated wave $s(t)$ with respect to the message $m(t)$ (band limited)



Assume that the Lower side band is modified into the vestigial side band. The vestige of the lower sideband compensates for the amount removed from the upper sideband. The bandwidth required to send VSB wave is

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Midi), Guntur Dist.

coherent detector and determining the necessary condition for undistorted version of the message signal $m(t)$. Thus, $s(t)$ is multiplied by a locally generated sinusoidal wave $\cos(2\pi f_c t)$ which is synchronous with the carrier wave $A_c \cos(2\pi f_c t)$ in both frequency and phase, as in fig below,



Fig(b). Block diagram of VSB Demodulator

Then, $v(t) = s(t) \cdot \cos(2\pi f_c t)$ -----(2)

In frequency domain Eqn (2) becomes,

$$V(f) = \frac{1}{2} [S(f - f_c) + S(f + f_c)]$$
 -----(3)

Substitution of Eqn (1) in Eqn (3) gives

$$V(f) = \frac{1}{2} [A_c / 2 [M(f - f_c - f_c) + M(f - f_c + f_c)] H(f - f_c) + \frac{1}{2} [A_c / 2 [M(f + f_c - f_c) + M(f + f_c + f_c)] H(f + f_c)]$$

$$V(f) = \frac{1}{2} [A_c / 2 [M(f - 2f_c) + M(f)] H(f - f_c) + \frac{1}{2} [A_c / 2 [M(f) + M(f + 2f_c)] H(f + f_c)]$$

$$V(f) = A_c / 4 M(f) [H(f - f_c) + H(f + f_c)] + A_c / 4 [M(f - 2f_c) H(f - f_c) + M(f + 2f_c) H(f + f_c)]$$
 -----(4)

The spectrum of $V(f)$ as shown in fig below,

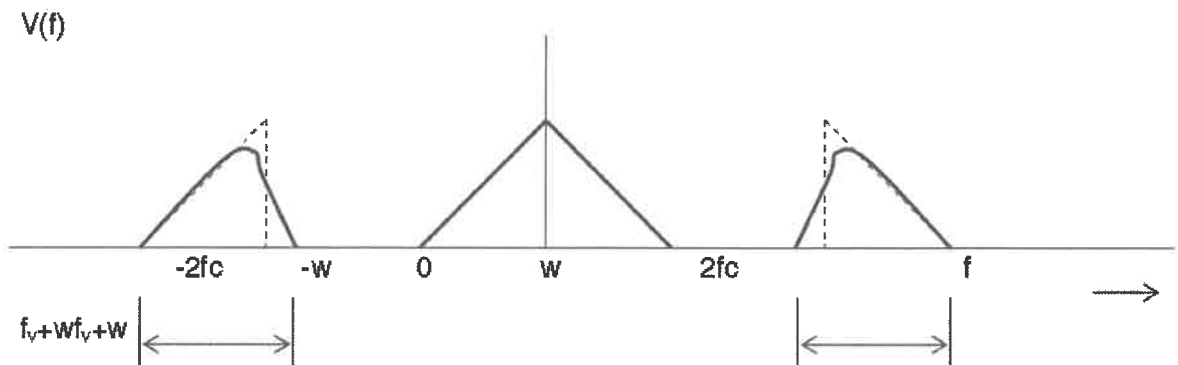


Fig ©. Spectrum of the product modulator output $v(t)$

Pass $v(t)$ to a Low pass filter to eliminate VSB wave corresponding to $2f_c$.

$$V_o(f) = A_c / 4 M(f) [H(f - f_c) + H(f + f_c)]$$
 -----(5)

Principal
 J. REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Mdl), Guntur, Dr

Time Domain Description:

Time domain representation of VSB modulated wave, procedure is similar to SSB Modulated waves. Let $s(t)$ denote a VSB modulated wave and assuming that $s(t)$ containing Upper sideband along with the Vestige of the Lower sideband. VSB modulated wave $s(t)$ is the output from Sideband shaping filter, whose input is DSBSC wave. The filter transfer function $H(f)$ is of the form as in fig below,

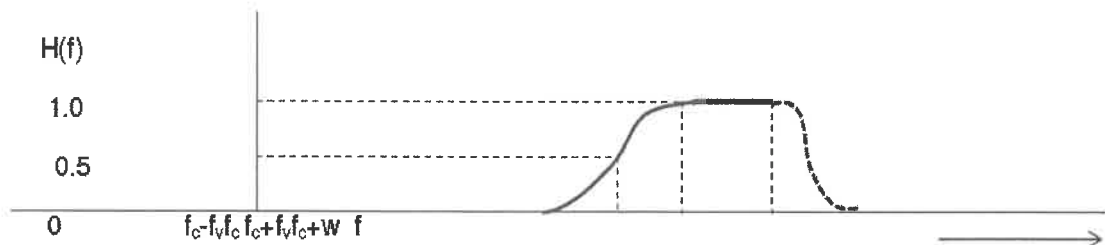


Fig (1) $H(f)$ of sideband shaping filter

The DSBSC Modulated wave is

$$S_{DSBSC}(t) = A_c m(t) \cos 2\pi f_c t \text{ -----(1)}$$

It is a band pass signal and has in-phase component only. Its low pass complex envelope is given by

$$\tilde{S}_{DSBSC}(t) = A_c m(t) \text{ -----(2)}$$

The VSB modulated wave is a band pass signal.

Let the low pass signal $\tilde{S}(t)$ denote the complex envelope of VSB wave $s(t)$, then

$$s(t) = \text{Re}[\tilde{S}(t) \exp(j2\pi f_c t)] \text{ -----(3)}$$

To determine $\tilde{S}(t)$ we proceed as follows

1. The side band shaping filter transfer function $H(f)$ is replaced by its equivalent complex low pass transfer function denoted by $\tilde{H}(f)$ as shown in fig below

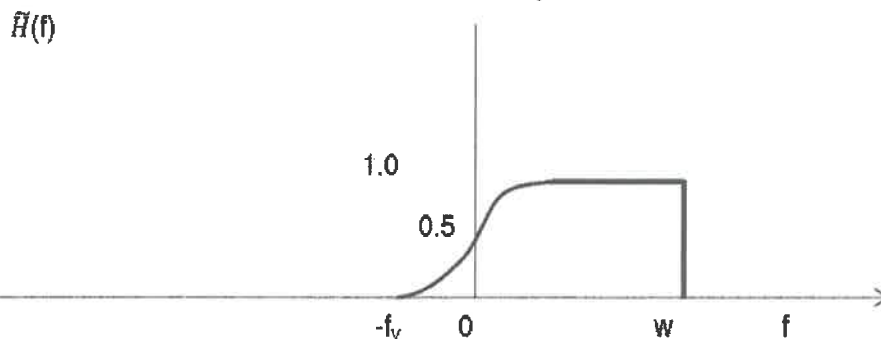


Fig (2) Low pass equivalent to $H(f)$

Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dist.

Note:

1. If vestigial side band is increased to full side

band, VSB becomes DSCSB ,i.e., $m_Q(t) = 0$.

2. If vestigial side band is reduced to Zero, VSB becomes SSB.

i.e., $m_Q(t) = \hat{m}(t)$


Where $\hat{m}(t)$ is the Hilbert transform of $m(t)$.

Similarly If VSB containing a vestige of the Upper sideband, then $s(t)$ is given by

$$S(t) = A/2 m(t) \cos 2\pi f_c t + A/2 m_Q(t) \sin 2\pi f_c t \text{ -----(14)}$$

Envelope detection of a VSB Wave plus Carrier

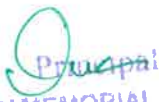
Principal
A.M REDDY MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEMPALLE
Narasaraopet (Mdi), Guntur (Dt.)


Principal
A.M REDDY MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEMPALLE
Narasaraopet (Mdi), Guntur (Dt.)

Sr. No.	Parameter	Standard AM	SSB	DSBSC	VSB
1	Power	High	Less	Medium	Less than DSBSC but greater than SSB
2	Bandwidth	$2 f_m$	f_m	$2 f_m$	$f_m < B_w < 2 f_m$
3	Carrier suppression	No	Yes	Yes	No
4	Receiver complexity	Simple	Complex	Complex	Simple
5	Application	Radio communication	Point to point communication preferred for long distance transmission.	Point to point communication	Television broadcasting
6	Modulation type	Non linear	Linear	Linear	Linear
7	Sideband suppression	No	One sided completely	No	One sideband suppressed partly
8	Transmission efficiency	Minimum	Maximum	Moderate	Moderate

Applications of different AM systems:

- Amplitude Modulation: AM radio, Short wave radio broadcast
- DSB-SC: Data Modems, Color TV's color signals.
- SSB: Telephone
- VSB: TV picture signals


 Principal
 A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Mdl), Guntur Dt

where $\phi(t)$ is a function of time. The frequency of $y(t)$ in this case depends on the function of $\phi(t)$ and may itself be a function of time. The instantaneous frequency of $y(t)$ given above is defined as

$$\omega_i(t) = \frac{d\phi(t)}{dt}$$

As a checkup for this definition, we know that the instantaneous frequency of $x(t)$ is equal to its frequency at all times (since the instantaneous frequency for that function is constant) and is equal to ω_c . Clearly this satisfies the definition of the instantaneous frequency since $\phi(t) = \omega_c t + \phi_0$ and therefore $\omega_i(t) = \omega_c$.

If we know the instantaneous frequency of some sinusoid from $-\infty$ to sometime t , we can find the angle of that sinusoid at time t using

$$\phi(t) = \int_{-\infty}^t \omega_i(\tau) d\tau$$

Changing the angle $\phi(t)$ of some sinusoid is the bases for the two types of angle modulation: Phase and Frequency modulation techniques.

Phase Modulation (PM)

In this type of modulation, the phase of the carrier signal is directly changed by the message signal. The phase modulated signal will have the form

$$g_{PM}(t) = A \cos[\omega_c t + k_p m(t)],$$

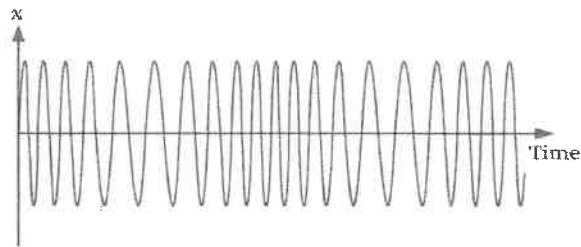
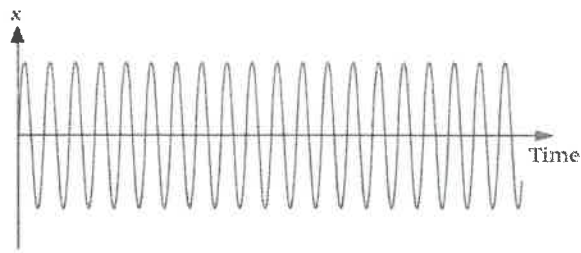
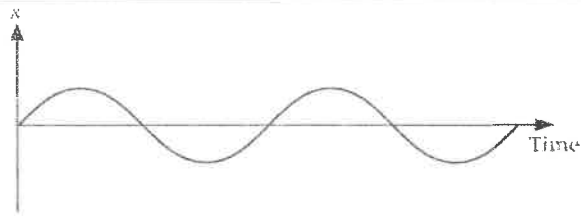
where A is a constant, ω_c is the carrier frequency, $m(t)$ is the message signal, and k_p is a parameter that specifies how much change in the angle occurs for every unit of change of $m(t)$. The phase and instantaneous frequency of this signal are

$$\begin{aligned} \phi_{PM}(t) &= \omega_c t + k_p m(t), \\ \omega_i(t) &= \omega_c + k_p \frac{dm(t)}{dt}. \end{aligned}$$

So, the frequency of a PM signal is proportional to the derivative of the message signal.

Frequency Modulation (FM)

This type of modulation changes the frequency of the carrier (not the phase as in PM) directly with the message signal. The FM modulated signal is



Notice that as the information signal increases, the carrier frequency increases, and as the information signal decreases, the carrier frequency decreases. The

frequency f_i of the information signal controls the rate at which the carrier frequency increases and decreases. As with AM, f_i must be less than f_c . The amplitude of the carrier remains constant throughout this process.

When the information voltage reaches its maximum value then the change in frequency of the carrier will have also reached its maximum deviation above the nominal value. Similarly when the information reaches a minimum the carrier will be at its lowest frequency below the nominal carrier frequency value. When the information signal is zero, then no deviation of the carrier will occur.

The maximum change that can occur to the carrier from its base value f_c is called the frequency deviation, and is given the symbol Δf_c . This sets the dynamic range (i.e. voltage range) of the transmission. The dynamic range is the ratio of the largest and smallest analogue information signals that can be transmitted.

Bandwidth of FM and PM Signals

The bandwidth of the different AM modulation techniques ranges from the bandwidth of the message signal (for SSB) to twice the bandwidth of the message signal (for DSBSC and Full AM). When FM signals were first proposed, it was thought that their bandwidth can be reduced to an arbitrarily small value. Compared to the bandwidth of different AM modulation techniques, this would in theory be a big advantage. It was assumed that a signal with an instantaneous frequency that changes over of range of Δf Hz would have a bandwidth of Δf Hz. When experiments were done, it was discovered that this was not the case. It was discovered that the bandwidth of FM signals for a specific message signal was at

Principal
A.M REDDY
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopeta, Guntur, Dr.

Now we can expand the term $e^{jka(t)}$ in $\hat{g}_{FM}(t)$, which gives

$$\hat{g}_{FM}(t) = A e^{j\omega_c t} \left[1 + jka(t) - \frac{1}{2} k^2 a^2(t) - \frac{j}{6} k^3 a^3(t) + \frac{1}{24} k^4 a^4(t) + \dots \right]$$

Since k_f and $a(t)$ are real ($a(t)$ is real because it is the integral of a real function $m(t)$), and since $\text{Re}\{e^{j\omega_c t}\} = \cos(\omega_c t)$ and $\text{Re}\{je^{j\omega_c t}\} = -\sin(\omega_c t)$, then

$$g_{FM}(t) = \text{Re}\{\hat{g}_{FM}(t)\} = A \left[\cos(\omega_c t) + ka(t) \sin(\omega_c t) - \frac{k^2 a^2(t)}{2} \cos(\omega_c t) - \frac{k^3 a^3(t)}{6} \sin(\omega_c t) + \frac{k^4 a^4(t)}{24} \cos(\omega_c t) + \dots \right]$$

The assumption we made for narrowband FM is $(ka(t) \ll 1)$. This assumption will result in making all the terms with powers of $ka(t)$ greater than 1 to be small compared to the first two terms. So, the following is a reasonable approximation for $g_{FM}(t)$

$$g_{FM \text{ Narrowband}}(t) \approx A \left[\cos(\omega_c t) + ka(t) \sin(\omega_c t) \right], \quad \text{when } ka(t) \ll 1.$$

It must be stressed that the above approximation is only valid for narrowband FM signals that satisfy the condition $(ka(t) \ll 1)$. The above signal is simply the addition (or actually the subtraction) of a cosine (the carrier) with a DSBSC signal (but using a sine as the carrier). The message signal that modulates the DSBSC signal is not $m(t)$ but its integration $a(t)$. One of the properties of the Fourier transform informs us that the bandwidth of a signal $m(t)$ and its integration $a(t)$ (and its derivative too) are the same (verify this). Therefore, the bandwidth of the narrowband FM signal is

$$BW_{FM \text{ Narrowband}} \approx BW_{DSBSC} \approx 2BW_{m(t)}$$

Principal
A.M REDDY MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (M.S), Guntur Dist.

*highest carrier frequency and
reject all others*

A narrowband FM signal can be generated easily using the block diagram of the narrowband FM modulator that was described in a previous lecture. The narrowband FM modulator generates a narrowband FM signal using simple components such as an integrator (an OpAmp), oscillators, multipliers, and adders. The generated narrowband FM signal can be converted to a wideband FM signal by simply passing it through a non-linear device with power P . Both the carrier frequency and the frequency deviation Δf of the narrowband signal are increased by a factor P . Sometimes, the desired increase in the carrier frequency and the desired increase in Δf are different. In this case, we increase Δf to the desired value and use a frequency shifter (multiplication by a sinusoid followed by a BPF) to change the carrier frequency to the desired value.

SINGLE-TONE FREQUENCY MODULATION

Time-Domain Expression

Since the FM wave is a nonlinear function of the modulating wave, the frequency modulation is a nonlinear process. The analysis of nonlinear process is the difficult task. In this section, we will study single-tone frequency modulation in detail to simplify the analysis and to get thorough understanding about FM.

Let us consider a single-tone sinusoidal message signal defined by

$$n(t) = A_n \cos(2\pi f_n t) \quad (5.13)$$

The instantaneous frequency from Eq. (5.8) is then

$$f(t) = f_c + k_f A_n \cos(2\pi f_n t) = f_c + \Delta f \cos(2\pi f_n t) \quad (5.14)$$

where

$$\Delta f = k_f A_n$$


Principal
A.M REDDY MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dist.

is the modulation index of the single-tone phase modulated wave.

The frequency deviation of the single-tone PM wave is

$$s_{FM}(t) = A_c \cos[2\pi f_c t + \beta_f \sin(2\pi f_m t)]$$

Spectral Analysis of Single-Tone FM Wave

The above Eq. can be rewritten as

$$s_{FM}(t) = \text{Re}\{A_c e^{j2\pi f_c t} e^{j\beta \sin(2\pi f_m t)}\}$$

For simplicity, the modulation index of FM has been considered as β instead of β_f afterward. Since $\sin(2\pi f_m t)$ is periodic with fundamental period $T = 1/f_m$, the complex exponential $e^{j\beta \sin(2\pi f_m t)}$ is also periodic with the same fundamental period. Therefore, this complex exponential can be expanded in Fourier series representation as

$$e^{j\beta \sin(2\pi f_m t)} = \sum_{n=-\infty}^{\infty} c_n e^{j2\pi n f_m t}$$

where the Fourier series coefficients c_n are obtained as


Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dist.

The above eq is the expression for narrow band FM wave

In this case $\cos[\phi(t)] \approx 1$ and $\sin[\phi(t)] \approx \phi(t)$

$$s(t) = A_c \cos(2\pi f_c t) - A_c \sin(2\pi f_c t) \phi(t)$$

$$\text{or, } s(t) = A_c \cos(2\pi f_c t) - 2\pi A_c k_f \sin(2\pi f_c t) \int_0^t m(t) dt$$

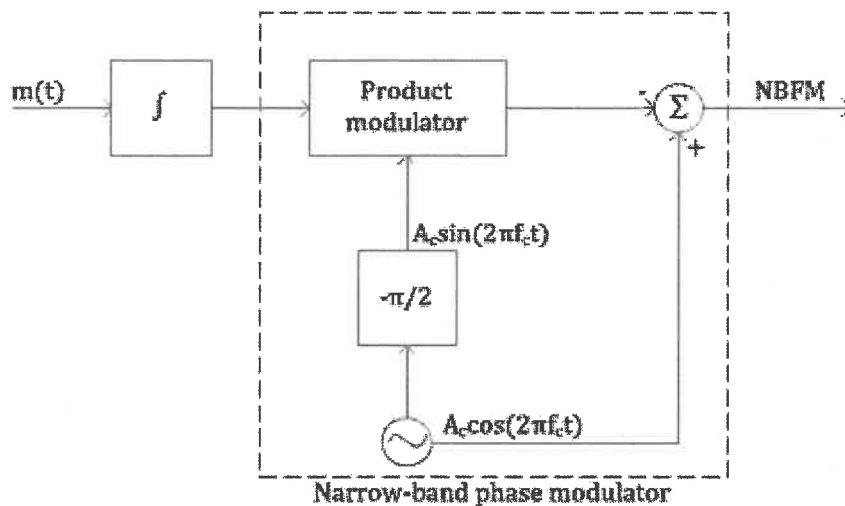


Fig: Narrowband FM Generator

The frequency deviation Δf is very small in narrow-band FM wave. To produce wideband FM, we have to increase the value of Δf to a desired level. This is achieved by means of one or multiple frequency multipliers. A frequency multiplier consists of a nonlinear device and a bandpass filter. The n^{th} order nonlinear device produces a dc component and n number of frequency modulated waves with carrier frequencies $f_c, 2f_c, \dots, nf_c$ and frequency deviations $\Delta f, 2\Delta f, \dots, n\Delta f$, respectively. If we want an FM wave with frequency deviation of $6\Delta f$, then we may use a 6th order nonlinear device or one 2^{nd} order and one 3^{rd} order nonlinear devices in cascade followed by a bandpass filter centered at $6f_c$. Normally, we may

$$f(t) = \frac{1}{2\pi\sqrt{(L_1 + L_2)C(t)}}$$

$$f(t) = \frac{1}{2\pi\sqrt{(L_1 + L_2)(C_0 - km(t))}}$$

$$= \frac{1}{2\pi\sqrt{(L_1 + L_2)C_0}} \frac{1}{\sqrt{1 - \frac{km(t)}{C_0}}}$$

$$\text{or, } f(t) = f_c \left(1 - \frac{km(t)}{C_0}\right)^{-1/2}$$

where f_c is the unmodulated frequency of oscillation. Assuming,

$$\frac{km(t)}{C_0} \ll 1$$

we have from binomial expansion,

$$\left(1 - \frac{km(t)}{C_0}\right)^{-1/2} \approx 1 + \frac{km(t)}{2C_0}$$

$$f(t) \approx f_c \left(1 + \frac{km(t)}{2C_0}\right)$$

$$= f_c + \frac{kf_c m(t)}{2C_0}$$

$$\text{or, } f(t) = f_c + k_f m(t)$$

$$k_f = \frac{kf_c}{2C_0}$$

is the frequency sensitivity of the modulator. The Eq. (5.42) is the required expression for the instantaneous frequency of an FM wave. In this way, we can generate an FM wave by direct method.

Direct FM may be generated also by a device in which the inductance of the resonant circuit is linearly varied by a modulating signal $n(t)$; in this case the modulating signal being the current.

The main advantage of the direct method is that it produces sufficiently high frequency deviation, thus requiring little frequency multiplication. But, it has poor frequency stability. A feedback scheme is used to stabilize the frequency in which the output frequency is compared with the constant frequency generated by highly stable crystal oscillator and the error signal is feedback to stabilize the frequency.

Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur (Dt)

Here both the amplitude and frequency of this signal are modulated.

In this case, the differentiator is nothing but a circuit that converts change in frequency into corresponding change in voltage or current as shown in Fig. 5.11. The ideal differentiator has transfer function

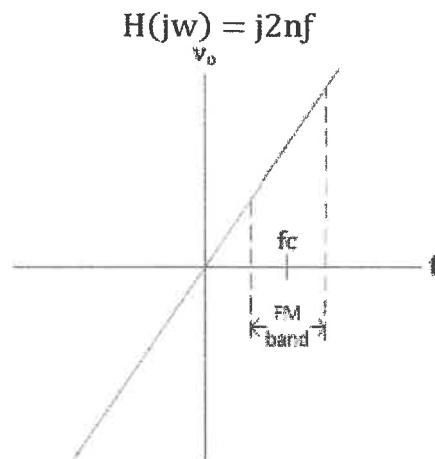


Figure : Transfer function of ideal differentiator.

Instead of ideal differentiator, any circuit can be used whose frequency response is linear for some band in positive slope. This method is known as slope detection. For this, linear segment with positive slope of RC high pass filter or LC tank circuit can be used. Figure 5.13 shows the use of an LC circuit as a differentiator.

The drawback is the limited linear portion in the

slope of the tank circuit. This is not suitable for wideband FM where the peak frequency deviation is high.

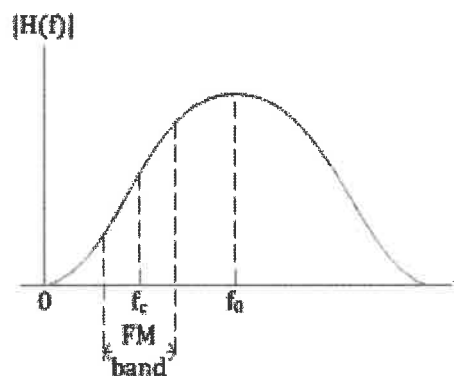


Figure : Use of LC tank circuit as a differentiator.

A better solution is the ratio or balanced slope detector in which two tank circuits tuned at $f_c + \Delta f$ and $f_c - \Delta f$ are used to extend the linear portion as shown in below figure.

Let the VCO output be defined by

$$v_{VCO}(t) = A_v \sin[2\pi f_c t + \phi_2(t)]$$

where

Here k_v is the frequency sensitivity of the VCO measured in hertz per volt. The multiplication of $s(t)$ and $v_{VCO}(t)$ results

$$\begin{aligned} s(t)v_{VCO}(t) &= A_c \cos[2\pi f_c t + \phi_1(t)] A_v \sin[2\pi f_c t + \phi_2(t)] \\ &= \frac{A_c A_v}{2} \sin[4\pi f_c t + \phi_1(t) + \phi_2(t)] + \frac{A_c A_v}{2} \sin[\phi_2(t) - \phi_1(t)] \end{aligned}$$

The high-frequency component is removed by the low-pass filtering of the loop filter. Therefore, the input signal to the loop filter can be considered as

$$e(t) = \frac{A_c A_v}{2} \sin[\phi_2(t) - \phi_1(t)]$$

The difference $\phi_2(t) - \phi_1(t) = \phi_e(t)$ constitutes the phase error. Let us assume that the PLL is in phase lock so that the phase error is very small. Then,

$$\sin[\phi_2(t) - \phi_1(t)] \approx \phi_2(t) - \phi_1(t)$$

$$\phi_e(t) = 2\pi k_v \int_0^t v(t) dt - \phi_1(t)$$

Principal
A.M REDDY MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur (Dr. ...)

of the message signal. Consequently, the noise at the output of the loop filter is also limited to the bandwidth W . On the other hand, the output from the VCO is a wideband FM signal with an instantaneous frequency that follows the instantaneous frequency of the received FM signal.

PREEMPHASIS AND DEEMPHASIS NETWORKS

In FM, the noise increases linearly with frequency. By this, the higher frequency components of message signal are badly affected by the noise. To solve this problem, we can use a preemphasis filter of transfer function $H_p(f)$ at the transmitter to boost the higher frequency components before modulation. Similarly, at the receiver, the deemphasis filter of transfer function $H_d(f)$ can be used after demodulator to attenuate the higher frequency components thereby restoring the original message signal.

The preemphasis network and its frequency response are shown in Figure 5.19 (a) and (b) respectively. Similarly, the counter part for deemphasis network is shown in Figure 5.20.

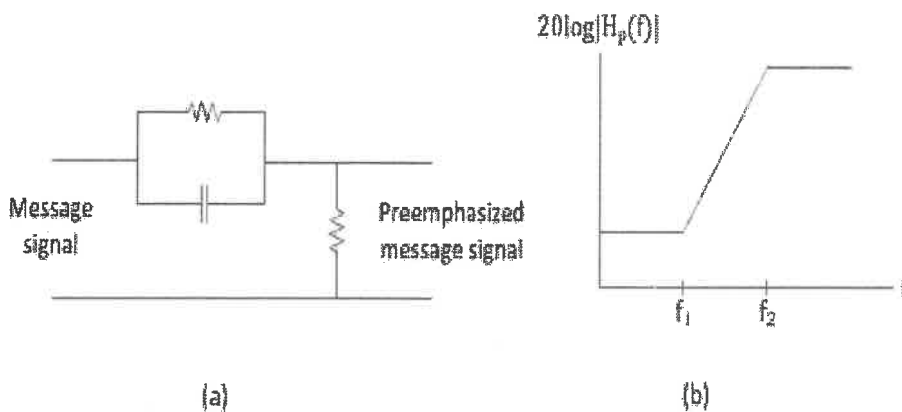
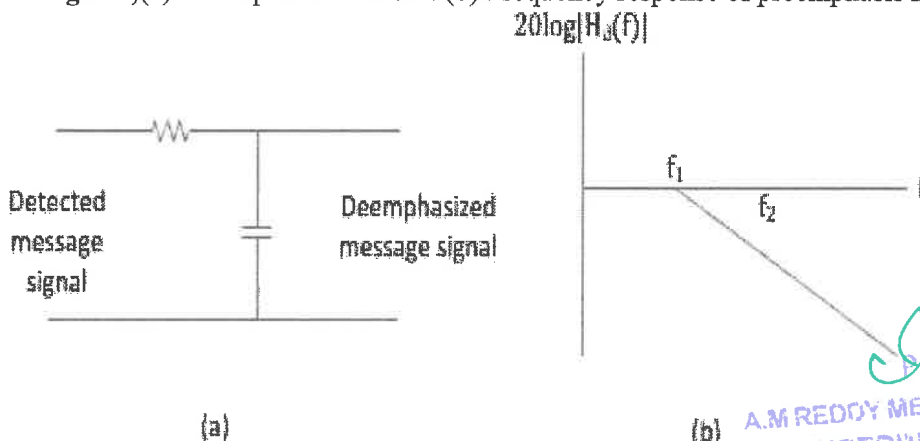


Figure ;(a) Preemphasis network. (b) Frequency response of preemphasis network.



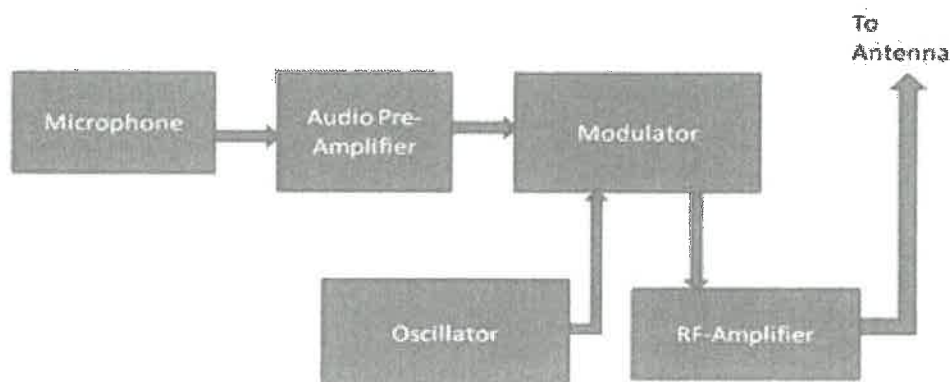
(b) Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Rd), Guntur (Dr -

4.	Transmitters are relatively simple & cheap.	Transmitters are complex and hence expensive.
5.	The average power in modulated wave is greater than carrier power. This added power is provided by modulating source.	The average power in frequency modulated wave is same as contained in un-modulated wave.
6.	More susceptible to noise interference and has low signal to noise ratio, it is more difficult to eliminate effects of noise.	Noise can be easily minimized amplitude variations can be eliminated by using limiter.
7.	it is not possible to operate without interference.	it is possible to operate several independent transmitters on same frequency.
8.	The maximum value of modulation index = 1, other wise over-modulation would result in distortions.	No restriction is placed on modulation index.

FM Transmitter

The FM transmitter is a single transistor circuit. In the telecommunication, the frequency modulation (FM) transfers the information by varying the frequency of carrier wave according to the message signal. Generally, the FM transmitter uses VHF radio frequencies of 87.5 to 108.0 MHz to transmit & receive the FM signal. This transmitter accomplishes the most excellent range with less power. The performance and working of the wireless audio transmitter circuit is depends on the induction coil & variable capacitor. This article will explain about the working of the FM transmitter circuit with its applications.

The FM transmitter is a low power transmitter and it uses FM waves for transmitting the sound, this transmitter transmits the audio signals through the carrier wave by the difference of frequency. The carrier wave frequency is equivalent to the audio signal of the amplitude and the FM transmitter produce VHF band of 88 to 108 MHz. Please follow the below link for: [Know all About Power Amplifiers for FM Transmitter](#)



Block Diagram of FM Transmitter

Working of FM Transmitter Circuit

Principal
 A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Dist), Guntur Dist

- The correctional facilities have used in the FM transmitters to reduce the prison noise in common areas.

Advantages of the FM Transmitters

- The FM transmitters are easy to use and the price is low
- The efficiency of the transmitter is very high
- It has a large operating range
- This transmitter will reject the noise signal from an amplitude variation.


Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur, Orissa

- Shot noise
- Noise temperature
- Quantization noise

Noise temperature

Equivalent noise temperature is not the physical temperature of amplifier, but a theoretical construct, that is an equivalent temperature that produces that amount of noise power

$$T_e = (F - 1)$$

White noise

One of the very important random processes is the *white noise* process. Noises in many practical situations are approximated by the white noise process. Most importantly, the white noise plays an important role in modelling of WSS signals.

A white noise process $\{W(t)\}$ is a random process that has constant power spectral density at all frequencies. Thus

$$S_W(\omega) = \frac{N_0}{2} \quad -\infty < \omega < \infty$$

where N_0 is a real constant and called the *intensity* of the white noise. The corresponding autocorrelation function is given by

$$R_W(\tau) = \frac{N}{2} \delta(\tau) \quad \text{where } \delta(\tau) \text{ is the Dirac delta.}$$

The average power of white noise

$$P_{avg} = EW^2(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \frac{N}{2} d\omega \rightarrow \infty$$

The autocorrelation function and the PSD of a white noise process is shown in Figure 1 below.


 Principal
 A.M. REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (M.D.), Guntur Dist.

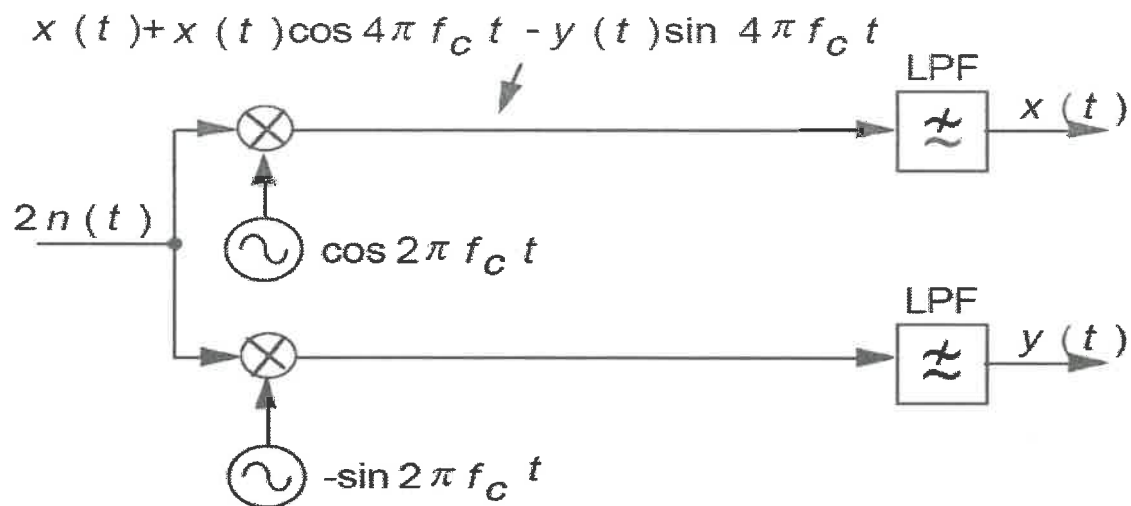


Fig: Generation of quadrature components of $n(t)$.

- Filters at the receiver have enough bandwidth to pass the desired signal but not too big to pass excess noise.
- Narrowband (NB) f_c center frequency is much bigger than the bandwidth.
- Noise at the output of such filters is called narrowband noise (NBN).
- NBN has spectral concentrated about some mid-band frequency f_c
- The sample function of such NBN $n(t)$ appears as a sine wave of frequency f_c which modulates slowly in amplitude and phase

Input signal-to-noise ratio (SNR_I): is the ratio of the average power of modulated signal $s(t)$ to the average power of the filtered noise.

Output signal-to-noise ratio (SNR_O): is the ratio of the average power of demodulated message to the average power of the noise, both measured at the receiver output.

Channel signal-to-noise ratio (SNR_C): is the ratio of the average power of modulated signal $s(t)$ to the average power of the noise in the message bandwidth, both measured at the receiver input.


 Principal
 A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Mdl), Guntur (Dy)

Demodulate the received signal by first multiplying $r(t)$ by a locally generated sinusoid $\cos(2\pi f_c t + \phi)$, where ϕ is the phase of the sinusoid. Then passing the product signal through an ideal lowpass filter having a bandwidth W .

The multiplication of $r(t)$ with $\cos(2\pi f_c t + \phi)$ yields

$$\begin{aligned} r(t) \cos(2\pi f_c t + \phi) &= u(t) \cos(2\pi f_c t + \phi) + n(t) \cos(2\pi f_c t + \phi) \\ &= A_c m(t) \cos(2\pi f_c t) \cos(2\pi f_c t + \phi) \\ &\quad + n_c(t) \cos(2\pi f_c t) \cos(2\pi f_c t + \phi) - n_s(t) \sin(2\pi f_c t) \cos(2\pi f_c t + \phi) \\ &= \frac{1}{2} A_c m(t) \cos(\phi) + \frac{1}{2} A_c m(t) \cos(4\pi f_c t + \phi) \\ &\quad + \frac{1}{2} [n_c(t) \cos(\phi) + n_s(t) \sin(\phi)] + \frac{1}{2} [n_c(t) \cos(4\pi f_c t + \phi) - n_s(t) \sin(4\pi f_c t + \phi)] \end{aligned}$$

The low pass filter rejects the double frequency components and passes only the low pass components.

$$y(t) = \frac{1}{2} A_c m(t) \cos(\phi) + \frac{1}{2} [n_c(t) \cos(\phi) + n_s(t) \sin(\phi)]$$

the effect of a phase difference between the received carrier and a locally generated carrier at the receiver is a drop equal to $\cos(\phi)$ in the received signal power.

Phase-locked loop

The effect of a phase-locked loop is to generate phase of the received carrier at the receiver.

If a phase-locked loop is employed, then $\phi = 0$ and the demodulator is called a coherent or synchronous demodulator.

In our analysis in this section, we assume that we are employing a coherent demodulator. With this assumption, we assume that $\phi = 0$

$$y(t) = \frac{1}{2} [A_c m(t) + n_c(t)]$$

Therefore, at the receiver output, the message signal and the noise components are additive and we are able to define a meaningful SNR. The message signal power is given by

$$P_o = \frac{A_c^2}{4} P_M$$

Power P_M is the content of the message signal

The noise power is given by

$$P_{no} = \frac{1}{4} P_{nc} = \frac{1}{4} P_n$$

 Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, A.P.

Parallel to our discussion of DSB, we have

$$\begin{aligned}
 P_c &= \frac{A_c^2}{4} P_M \\
 P_{n_c} &= \frac{1}{4} P_n = \frac{1}{4} P_c \\
 P_n &= \int_{-\infty}^{\infty} S_n(f) df = \frac{N_0}{2} \times 2W = WN_0 \\
 \left(\frac{S}{N}\right)_0 &= \frac{P_c}{P_{n_c}} = \frac{A_c^2 P_M}{WN_0} \\
 P_R &= P_U = A_c^2 P_M \\
 \left(\frac{S}{N}\right)_{0_{SSB}} &= \frac{P_R}{N_c W} = \left(\frac{S}{N}\right)_b
 \end{aligned}$$

The signal-to-noise ratio in an SSB system is equivalent to that of a DSB system.

Noise in Conventional AM

DSB AM signal : $u(t) = A_c [1 + am_n(t)] \cos(2\pi f_c t)$

Received signal at the input to the demodulator

$$\begin{aligned}
 r(t) &= A_c [1 + am_n(t)] \cos(2\pi f_c t) + n(t) \\
 &= A_c [1 + am_n(t)] \cos(2\pi f_c t) + n_c(t) \cos(2\pi f_c t) - n_s(t) \sin(2\pi f_c t) \\
 &= [A_c [1 + am_n(t)] + n_c(t)] \cos(2\pi f_c t) - n_s(t) \sin(2\pi f_c t)
 \end{aligned}$$

Where a is the modulation index

$mn(t)$ is normalized so that its minimum value is -1

If a synchronous demodulator is employed, the situation is basically similar to the DSB case, except that we have $1 + amn(t)$ instead of $m(t)$.

$$y(t) = \frac{1}{2} [A_c am_n(t) + n_c(t)]$$

Received signal power

$$P_R = \frac{A_c^2}{2} [1 + a^2 P_{M_n}]$$

□ Assumed that the message process is zero mean.

Now we can derive the output SNR as

$$\begin{aligned}
 \left(\frac{S}{N}\right)_{0_{AM}} &= \frac{\frac{1}{4} A_c^2 a^2 P_{M_n}}{\frac{1}{4} P_{n_c}} = \frac{A_c^2 a^2 P_{M_n}}{2N_0 W} = \frac{a^2 P_{M_n}}{1 + a^2 P_{M_n}} \frac{\frac{A_c^2}{2} [1 + a^2 P_{M_n}]}{N_0 W} \\
 &= \frac{a^2 P_{M_n}}{1 + a^2 P_{M_n}} \frac{P_R}{N_0 W} = \frac{a^2 P_{M_n}}{1 + a^2 P_{M_n}} \left(\frac{S}{N}\right)_b = \eta \left(\frac{S}{N}\right)_b
 \end{aligned}$$

□ η denotes the modulation efficiency

□ Since $a^2 P_{M_n} < 1 + a^2 P_{M_n}$, the SNR in conventional AM is always smaller than the SNR in a baseband system.

➤ In practical applications, the modulation index a is in the range of 0.8-0.9.

Dr. J. V. S. S. S. S.
Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur(Dist)

$$\begin{aligned}
V_r(t) &= \sqrt{A_c^2 [1 + am_n(t)] + n_c(t)}^2 + n_s(t)^2 \\
&= \sqrt{A_c^2 [1 + am_n(t)]^2 + n_c^2(t) + n_s^2(t) + 2A_c n_c(t) [1 + am_n(t)]} \\
&\xrightarrow{a} \sqrt{(n_c^2(t) + n_s^2(t)) \left[1 + \frac{2A_c n_c(t)}{n_c^2(t) + n_s^2(t)} (1 + am_n(t)) \right]} \\
&\xrightarrow{b} V_n(t) \left[1 + \frac{A_c n_c(t)}{V_n^2(t)} (1 + am_n(t)) \right] \\
&= V_n(t) + \frac{A_c n_c(t)}{V_n(t)} (1 + am_n(t))
\end{aligned}$$

(a): $A_c^2 [1 + am_n(t)]^2$ is small compared with the other components

(b): $\sqrt{n_c^2(t) + n_s^2(t)} = V_n(t)$: the envelope of the noise process

Use the approximation

$$\sqrt{1 + \varepsilon} \approx 1 + \frac{\varepsilon}{2}, \text{ for small } \varepsilon, \text{ where } \varepsilon = \frac{2A_c n_c(t)}{n_c^2(t) + n_s^2(t)} (1 + am_n(t))$$

Then

$$V_r(t) = V_n(t) + \frac{A_c n_c(t)}{V_n(t)} (1 + am_n(t))$$

We observe that, at the demodulator output, the signal and the noise components are no longer additive. In fact, the signal component is multiplied by noise and is no longer distinguishable. In this case, no meaningful SNR can be defined. We say that this system is operating below the threshold. The subject of threshold and its effect on the performance of a communication system will be covered in more detail when we discuss the noise performance in angle modulation.

Effect of threshold in angle modulation system:

FM THRESHOLD EFFECT FM threshold is usually defined as a Carrier-to-Noise ratio at which demodulated Signal-to-Noise ratio falls 1dB below the linear relationship. This is the effect produced in an FM receiver when noise limits the desired information signal. It occurs at about 10 dB, as earlier stated in 5 the introduction, which is at a point where the FM signal-to-Noise improvement is measured. Below the FM threshold point, the noise signal (whose amplitude and phase are randomly varying) may instantaneously have amplitude greater than that of the wanted signal. When this happens, the noise will produce a sudden change in the phase of the FM demodulator output. In an audio system, this sudden phase change makes a "click". In video applications the term "click noise" is used to describe short horizontal black and white lines that appear randomly over a picture

Note: if bandwidth ratio is increased by a factor 2. Then $\frac{V_{FM}}{V_{AM}}$ increases by a factor 4

This exchange of bandwidth and noise performance is an important feature of FM

$$\text{Figure of merit } (\gamma) = \frac{SNR_o}{SNR_c}$$

CW- Modulation System	SNR_o	SNR_c	Figure of merit	Figure of merit (single tone)
DSB-SC	$\frac{C^2 A_c^2 P}{2WN_0}$	$\frac{C^2 A_c^2 P}{2WN_0}$	1	1
SSB	$\frac{C^2 A_c^2 P}{4WN_0}$	$\frac{C^2 A_c^2 P}{4WN_0}$	1	1
AM	$\frac{A_c^2 k_a^2 P}{2WN_0}$	$\frac{A_c^2 (1 + k_a^2 P)}{2WN_0}$	$\approx \frac{k_a^2 P}{1 + k_a^2 P} < 1$	$\frac{\mu^2}{2 + \mu^2}$
FM	$\frac{3A_c^2 k_f^2 P}{2N_0 W^3}$	$\frac{A_c^2}{2WN_0}$	$\frac{3k_f^2 P}{W^2}$	$\frac{3}{2} \beta^2$

P is the average power of the message signal.

C^2 is a constant that ensures that the ratio is dimensionless.

W is the message bandwidth.

A_c is the amplitude of the carrier signal.

k_a is the amplitude sensitivity of the modulator.

$\mu = k_a A_m$ and A_m is the amplitude sinusoidal wave

$\beta = \frac{\Delta f}{W}$ is the modulation index.

k_f is the frequency sensitivity of the modulator.

Δf is the frequency deviation.

 Principal

A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dt.

In a receiver, tuned circuits are made variable so that they can be set to the frequency of the desired signal. In most of the receivers, the capacitors in the tuned circuits are made variable. These capacitors are 'ganged' between the stages so that they all can be changed simultaneously when the tuning knob is rotated. To have perfect tuning the capacitor values between the stages must be exactly same but this is not the case. The differences in the capacitors cause the resonant frequency of each tuned circuit to be slightly different, thereby increasing the pass band.

2. Instability

As high gain is achieved at one frequency by a multistage amplifier, there are more chances of positive feedback (of getting back the small part of output of the last stage at the input to the first with the correct polarity) through some stray path, resulting in oscillations. These oscillations are unavoidable at high frequencies.

3. Variable Bandwidth

TRF receivers suffer from a variation in bandwidth over the tuning range. Consider a medium wave receiver required to tune over 535 kHz to 1640 kHz and it provides the necessary bandwidth of 10 kHz at 535 kHz. Let us calculate Q of this circuit.

$$Q = \frac{f}{\text{Bandwidth}} = \frac{535 \text{ kHz}}{10 \text{ kHz}} = 53.5$$

Now consider the frequency at the other end of the broadcast band, i.e. 1640 kHz. At 1640 kHz, Q of the coil should be 164 (1640 kHz / 10 kHz). However, in practice due to various losses depending on frequency, we will not get so large increase in Q. Let us assume that at 1640 kHz frequency Q is increased to value 100 instead of 164. With this Q of the tuned circuit bandwidth can be calculated as follows

$$\text{Bandwidth} = \frac{f}{Q} = \frac{1640 \text{ kHz}}{100} = 16.4 \text{ kHz}$$


We know, necessary bandwidth is 10 kHz. This increase in bandwidth of tuned circuit, pick up the adjacent stations along with station it is tuned for, providing insufficient adjacent frequency rejection. In other words we can say that in TRF receivers the bandwidth of the tuned circuit varies over the frequency range, resulting in poor selectivity of the receiver.

Because of the problems of tracking, instability and bandwidth variation, the TRF receivers have almost been replaced by superheterodyne receivers.

Problems in TRF Receivers:

Jee
Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dt.

Characteristics of Radio Receiver:


Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur Dist.

Blocks in Super heterodyne Receiver:

- **Basic principle** ○Mixing
 - Intermediate frequency of 455 KHz
 - Ganged tuning
- **RF section** ○Tuning circuits – reject interference and reduce noise figure ○Wide band RF amplifier
- **Local Oscillator** ○995 KHz to 2105 KHz ○Tracking
- **IF amplifier** ○Very narrow band width Class A amplifier – selects 455 KHz only
 - Provides much of the gain
 - Double tuned circuits
- **Detector** ○RF is filtered to ground

1. RF Amplifier:


Principal
A.M REDDY MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (M.D), Guntur(D

The frequency converter is a nonlinear resistance having two sets of input terminals and one set of output terminal. The two inputs to the frequency converter are the input signal along with any modulation and the input from a local oscillator (LO). The output contains several frequencies including the difference between the input frequencies. The difference frequency is called intermediate frequency and output circuit of the mixer is tuned for the intermediate frequency.

Separately Excited Mixer:

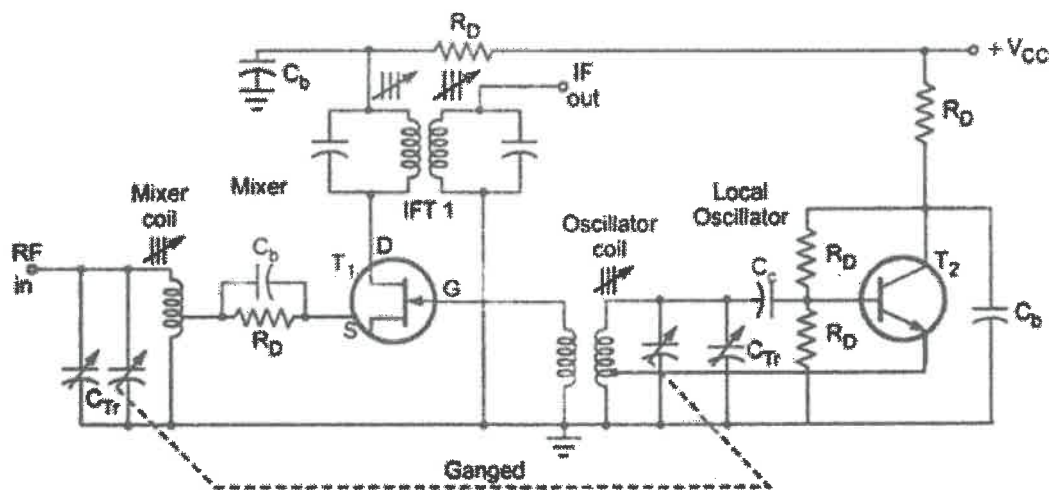


Fig.5 Separately Excited FET Mixer

Fig. 5 shows the separately excited mixer using FET. Here, one device acts as a mixer while the other supplies the necessary oscillations. The bipolar transistor T_2 , forms the Hartley oscillator circuit. It oscillates with local frequency (f_o). FET T_1 , is a mixer, whose gate is fed with the output of local oscillator and its bias is adjusted such that it operates in a nonlinear portion of its characteristic. The local oscillator varies the gate bias of the FET to vary its transconductance in a nonlinear manner, resulting intermediate frequency (IF) at the output. The output is taken through double tuned transformer in the drain of the mixer and fed to the IF amplifier. The ganged tuning capacitor allows simultaneous tuning of mixer and local oscillator.

The C_{Tr} , a small trimmer capacitors across each of the tuning capacitors are used for fine adjustments.

Self Excited Mixer:

Principal
A.M REDDY MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Dist), Guntur(Dr.)

In shortwave broadcasting, the operating limit for receivers is 36 MHz. For such operating limit local oscillators such as Armstrong, Hartley, Colpitts, Clapp or ultra-audion are used. The Colpitts, Clapp and ultra-audion oscillators are used at the top of the operating limit, whereas Hartley oscillator is used for frequencies below 120 MHz. All these oscillators are LC oscillators and each employs only one tuned circuit to determine its frequency. When higher frequency stability of local oscillator is required, the circuits like AFC (Automatic Frequency Control) are used.

5. IF Amplifier

Fig.7 Two Stage IF Amplifier

Jua
Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (M.D.), Guntur Dt

Fig. 8 shows the simple AGC circuit. In this circuit, dc bias produced by half wave rectifier as a AM detector, is used to control the gain of RF or IF amplifier. Before application of this voltage to the base of the RF and / or IF stage amplifier the audio signal is removed by the lowpass filter. The time constant of the filter is kept at least 10 times longer than the period of the lowest modulation frequency received. If the time constant is kept longer, it will give better filtering, but it will cause an annoying delay in the application of the AGC control when tuning from one signal to another. The recovered signal is then passed through C_c to remove the dc. The resulting ac signal is further amplified and applied to the loudspeaker.

Delayed AGC

Simple AGC is clearly an improvement over no AGC at all. Unfortunately, in simple AGC circuit, the unwanted weak signals(noise signals) are amplified with high gain. To

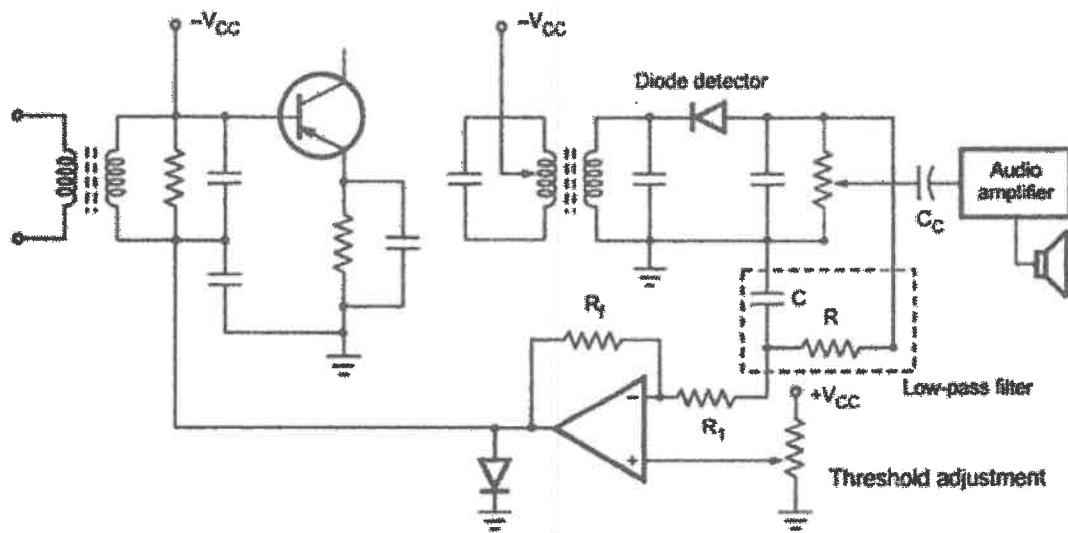


Fig.9. Delayed AGC circuit

avoid this, in delayed AGC circuits, AGC bias is not applied to amplifiers until signal strength has reached a predetermined level, after which AGC bias is applied as with simple AGC, but more strongly.

Here, AGC output is applied to the difference amplifier. It gives negative dc AGC only when AGC output generated by diode detector is above certain dc threshold voltage. This threshold voltage can be adjusted by adjusting the voltage at the positive input of the operational amplifier.

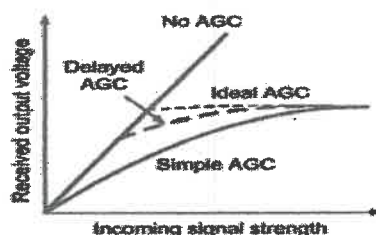


Fig.10. Response of receiver with various AGC circuits.

Principal
A.M REDDY MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdi), Guntur

already discussed. The same criteria apply in the selection of the intermediate frequency, and IF amplifiers are basically similar. A number of concepts have very similar meanings so that only the differences and special applications need be pointed out.

RF amplifiers An RF amplifier is always used in an FM receiver. Its main purpose is to reduce the noise figure, which could otherwise be a problem because of the large bandwidths needed for FM. It is also required to match the input impedance of the receiver to that of the antenna. To meet the second requirement, grounded gate (or base) or cascode amplifiers are employed. Both types have the property of low input impedance and matching the antenna, while neither requires neutralization. This is because the input electrode is grounded on either type of amplifier, effectively isolating input from output. A typical FET grounded-gate RF amplifier is shown in Figure It has all the good points mentioned and the added features of low distortion and simple operation.

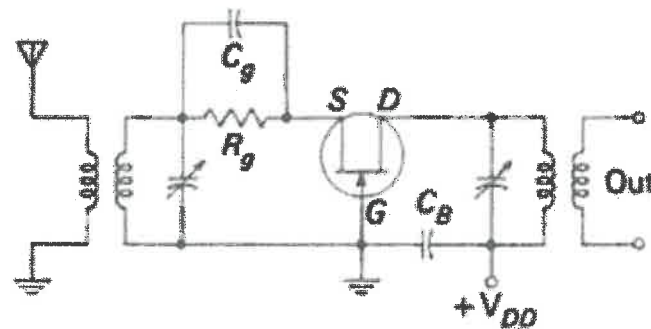


FIGURE Grounded-gate FET RF amplifier.

Oscillators and mixers The oscillator circuit takes any of the usual forms, with the Colpitts and Clapp predominant, being suited to VHF operation. Tracking is not normally much of a problem in FM broadcast receivers. This is because the tuning frequency range is only 1.25:1, much less than in AM broadcasting.

A very satisfactory arrangement for the front end of an FM receiver consists of FETs for the RF amplifier and mixer, and a bipolar transistor oscillator. As implied by this statement, separately excited oscillators are normally used

Principal
A.M REDDY MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur (Dt)

Amplitude Limiter:

In order to make full use of the advantages offered by FM, a demodulator must be preceded by an amplitude limiter, on the grounds that any amplitude changes in the signal fed to the FM demodulator are spurious.

They must therefore be removed if distortion is to be avoided. The point is significant, since most FM demodulators react to amplitude changes as well as frequency changes. The limiter is a form of clipping device, a circuit whose output tends to remain constant despite changes in the input signal. Most limiters behave in this fashion, provided that the input voltage remains within a certain range. The common type of limiter uses two separate electrical effects to provide a relatively constant output. There are leak-type bias and early (collector) saturation.


Principal
A.M REDDY MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur, D.

It is possible for the gate-drain section to become forward-biased under saturation conditions, causing a short circuit between input and output. To avert this, a resistance of a few hundred ohms is placed between the drain and its tank. This is R of Figure

PULSE MODULATION

Introduction:

Pulse Modulation

- Carrier is a train of pulses
- Example: Pulse Amplitude Modulation (PAM), Pulse width modulation (PWM), Pulse Position Modulation (PPM)

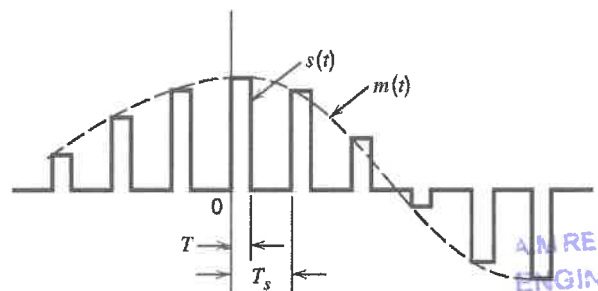
Types of Pulse Modulation:

- The immediate result of sampling is a pulse-amplitude modulation (PAM) signal
- PAM is an analog scheme in which the amplitude of the pulse is proportional to the amplitude of the signal at the instant of sampling
- Another analog pulse-forming technique is known as **pulse-duration modulation (PDM)**. This is also known as **pulse-width modulation**

(PWM)•Pulse-position modulation is closely related to PDM

Pulse Amplitude Modulation:

In PAM, amplitude of pulses is varied in accordance with instantaneous value of modulating signal.



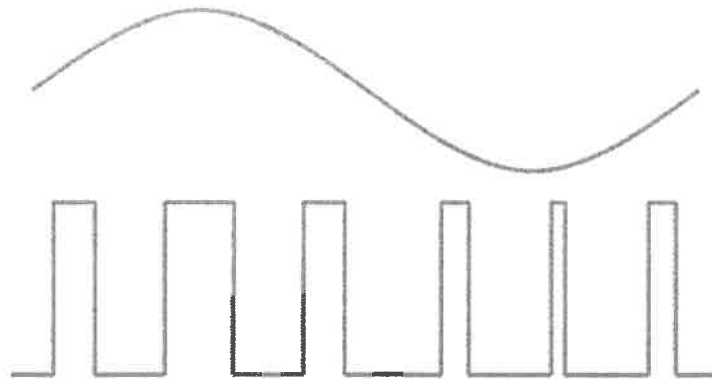
PAM Generation:

The carrier is in the form of narrow pulses having frequency f_c . The uniform sampling takes place in multiplier to generate PAM signal. Samples are placed T_s sec away from each other.

Principal
A.M. REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (M.D.), Guntur (Dt)

Pulse Width Modulation:

- In this type, the amplitude is maintained constant but the width of each pulse is varied in accordance with instantaneous value of the analog signal.



- In PWM information is contained in width variation. This is similar to FM.
- In pulse width modulation (PWM), the width of each pulse is made directly proportional to the amplitude of the information signal.

Pulse Position Modulation:

- In this type, the sampled waveform has fixed amplitude and width whereas the position of each pulse is varied as per instantaneous value of the analog signal.
- PPM signal is further modification of a PWM signal.

PPM & PWM Modulator:

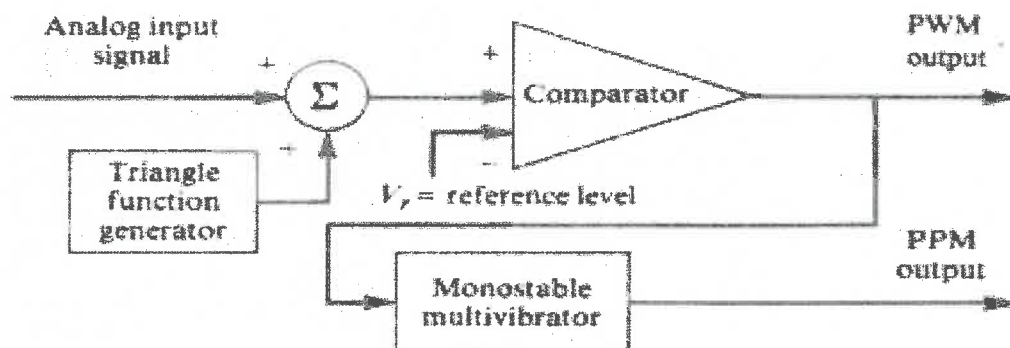


Fig.14. PWM & PPM Modulator

- The PPM signal can be generated from PWM signal.
- The PWM pulses obtained at the comparator output are applied to a mono stable multi vibrator which is negative edge triggered.



A.M. REDDY

Memorial College of Engineering and Technology
 Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada
 SPONSORED BY
 ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003

An ISO 9001:2015 Certified Institution

Web : www.amreddyengineering.ac.in
 E-Mail: principal.amreddyengineering@gmail.com
 VINUKUNDA ROAD, MASTAN REDDY NAGAR, PETLURIVARI PALEM,
 NARASARAO PET PALNADU (DIST) - 522601,
 CONTACT : 08647-247105.

III B.TECH II SEM

DEPARTMENT OF CSE

W.E.F: 09-01-2023

Period	1	2	3	4		5	6	7
Day/Time	9:30 TO 10:20	10:20 TO 11:10	11:20 TO 12:10	12:10 TO 1:00	1:00 TO 1:50	1:50 TO 2:40	2:40 TO 3:30	3:40 TO 4:20
MON	CD	FMPMC	OOAD	ES	B R E A K	CD LAB		
TUE	OOAD	ML	CNS	ML		ES	FMPMC	LIB
WED	CD	CNS LAB				FMPMC	OOAD	ML
THUR	CD	FMPMC	CNS	Tutorial		ML LAB		
FRI	CD	ML	CNS	OOAD		SOC LAB		
SAT	OOAD	ES	CNS	ML		CD	FMPMC	SPORTS

S.No.	SUBJECTS	SUBJECTS NAMES	FACULTY NAMES
1	CNS	CRYPTOGRAPHY AND NETWORK SECURITY	Mr V.V.B CHARI
2	OOAD	OBJECT ORIENTED ANALYSIS AND DESIGN	Mr S k Moulali
3	ML	MACHINE LEARNING	Mr A MADHAVA REDDY
4	CD	COMPILER DESIGN	Mr K RAMALINGA REDDY
5	FMPMC	Fundamentals of Micro Processors & Micro Controllars	Mr. CH. RAGHUNATHA BABU
6	CNS LAB	CRYPTOGRAPHY AND NETWORK SECURITY LAB	Mr V.V.B CHARI
7	ML LAB	MACHINE LEARNING LAB	Mr A MADHAVA REDDY
8	CD LAB	COMPILER DESIGN LAB	Mr K RAMALINGA REDDY
9	SOC	MEAN STACK TECHNOLOGY	Mr G.MOHAN SINGH & Mr K. SRINIVASA RAO
10	ES	EMPLOYBILITY SKIIS-II	Mr. T.RAVI SANKAR

[Signature]
Incharge

[Signature]
HOD

[Signature]
Principal
 A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Dist) Guntur Dt

[Signature]
Principal
 A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Dist) Guntur Dt



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA – 533 003, Andhra Pradesh, India

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

III Year – II Semester		L	T	P	C
		3	0	0	3
CRYPTOGRAPHY AND NETWORK SECURITY					

Course Objectives:

The main objectives of this course are to explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, public key algorithms, design issues and working principles of various authentication protocols and various secure communication standards including Kerberos, IPsec, and SSL/TLS.

Course Outcomes : At the end of the course, student will be able to

- Explain different security threats and countermeasures and foundation course of cryptography mathematics.
- Classify the basic principles of symmetric key algorithms and operations of some symmetric key algorithms and asymmetric key cryptography
- Revise the basic principles of Public key algorithms and Working operations of some Asymmetric key algorithms such as RSA, ECC and some more
- Design applications of hash algorithms, digital signatures and key management techniques
- Determine the knowledge of Application layer, Transport layer and Network layer security Protocols such as PGP, S/MIME, SSL, TSL, and IPsec .

UNIT I:

Basic Principles : Security Goals, Cryptographic Attacks, Services and Mechanisms, Mathematics of Cryptography.

UNIT II:

Symmetric Encryption: Mathematics of Symmetric Key Cryptography, Introduction to Modern Symmetric Key Ciphers, Data Encryption Standard, Advanced Encryption Standard.

UNIT III:

Asymmetric Encryption: Mathematics of Asymmetric Key Cryptography, Asymmetric Key Cryptography

UNIT IV:

Data Integrity, Digital Signature Schemes & Key Management : Message Integrity and Message Authentication, Cryptographic Hash Functions, Digital Signaturé, Key Management.

UNIT V:

Network Security-I: Security at application layer: PGP and S/MIME, Security at the Transport Layer: SSL and TLS, **Network Security-II :** Security at the Network Layer: IPsec, System Security

Text Books:

1. Cryptography and Network Security, 3rd Edition Behrouz A Forouzan, Deb deep Mukhopadhyay, McGraw Hill, 2015
2. Cryptography and Network Security, 4th Edition, William Stallings, (6e) Pearson, 2006
3. Everyday Cryptography, 1st Edition, Keith M. Martin, Oxford, 2016

Reference Books:

1. Network Security and Cryptography, 1st Edition, Bernard Meneges, Cengage Learning, 2018

Principal
 A.M. REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETTURIVARI PALEM
 Narasimapuram (Midi), Guntur (Dt)

**A.M. REDDY**

Memorial College of Engineering and Technology
Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada
SPONSORED BY
ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003


An ISO 9001:2015 Certified Institution
Web : www.amreddyengineering.ac.in
E.mail: principal.amreddyengineering@gmail.com

Department of CSE**III B.Tech/II Sem**

S.NO	REGD.NO	STUDENT NAME
1	20HM1A0501	ADDANKI AJAY
2	20HM1A0502	BEJJIPALLI JEEVAMANI
3	20HM1A0503	BOKKA VENKAT RAO
4	20HM1A0504	BOYA VISHNUVARDHAN
5	20HM1A0505	CHIRUGURI AKHIL
6	20HM1A0506	CHITIMITI ASHOK CHAKRAVARTHI REDDY
7	20HM1A0507	DARNASI RAKSHITHA
8	20HM1A0508	DUGGIMI SAI KUMAR
9	20HM1A0509	EDIGA VAMSI GOUD
10	20HM1A0510	GALLA MOHAN KUMAR
11	20HM1A0512	GOGULA UMAMAHESWARI
12	20HM1A0513	GORANTLA SAI PUNEETH
13	20HM1A0515	KAMBAM ASWINI
14	20HM1A0516	KAMINENI PRIYANKA
15	20HM1A0517	KANDUKURI NEWTON
16	20HM1A0518	KANNEDARI VINAYKUMAR
17	20HM1A0519	KAPU VISHNUVARDHAN REDDY
18	20HM1A0520	KAVALI NARENDRA
19	20HM1A0522	KUDUMULA SUMITHRA
20	20HM1A0521	KOSURU NAGA MANIKANTA
21	20HM1A0523	MADDIRALA HIMA BINDU
22	20HM1A0524	MALYAM AKHILAMMA
23	20HM1A0525	MANDA AJAY
24	20HM1A0526	MANNUVA MALLIKHARJUNA
25	20HM1A0527	MEENIGA SRAVANI
26	20HM1A0528	NALAGANGU VENKATA PRAVEEN
27	20HM1A0529	NALLAGANGULA SARAN VENKATA ACHI REDDY

A.M. REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Rd), Guntur (Dt)

28	20HM1A0530	NUNSAVATHU TIRUMALA BAI
29	20HM1A0531	PALLAPU SAILAJA
30	20HM1A0532	PATHIPATI HEMALATHA
31	20HM1A0533	PATHIPATI MAHESH
32	20HM1A0534	PULI PUSHPALATHA
33	20HM1A0535	RACHAGORLA JANKIRAM
34	20HM1A0536	RAPTHADU SREENATH
35	20HM1A0537	SAKE VINOD
36	20HM1A0538	SANIVARPU VISWAS MARREDDY
37	20HM1A0539	SHAIK ROSHINI
38	20HM1A0540	SHYAMALA KAVYA
39	20HM1A0542	TALARI MAHESH
40	20HM1A0543	TAMMU CHANDU
41	20HM1A0545	THOTA VENKATA NAVEEN
42	20HM1A0546	VADDE BHARGAVA
43	20HM1A0547	VALLEPU MAHALAKSHMI
44	20HM1A0548	VELPULA CHANDIRKA
45	20HM1A0549	VENNAPUSA LOKESWAR REDDY
46	20HM1A0550	YAKKANTI SAI TEJA
47	20HM1A0551	YARRA NAGAPA GARI GIRISH
48	20HM1A0552	YARRAMREDDY AARTHI REDDY
49	20HM1A0553	YATAM MUTYALU
50	20HM1A0554	YATHAM MUTYALU
51	20HM1A0555	YERIKALA ASHOK
52	21HM5A0501	KOSURI LAKSHMANA RAO


 A.M. REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 P. E. T. L. U. V. A. R. I. P. A. L. E. M
 Narasaraopeta (M.D.), Guntur (Dt)

A
C
D
B
B
D
B
B
D
A
B
B
C
B
D
A
C
A
D
D

1. The entries in the access matrix represents

- A. Access rights
- B. segment
- C. Program
- D. Process

2. Which of the following defines the modern language of an SNMP MIB document

- A. SNMPv3
- B. SSL
- C. SMIv2
- D. SET

3. SOCKS service is located on


- A. TCP port 1081
- B. TCP port 1088
- C. TCP port 1082
- D. TCP port 1080

4. In a screened host firewall, single-homed bastion, the bastion host performs which of the following functions

- A. integration
- B. authentication
- C. non repudiation
- D. segregation

5. Trojan horse browser is a threat to

- A. Confidentiality
- B. Integrity
- C. Privacy
- D. Authentication


Principal
A.M REDDY MEMORIAL COLLEGE OF
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur (Dt)

12. SSL sessions are created by which of the following

- A. Cipher spec protocol
- B. Handshake protocol
- C. TCP
- D. IP

13. Line tapping can be countered using

- A. Antivirus software
- B. Access control
- C. Link encryption techniques
- D. Spyware

14. Oakley is based on which of the following algorithms

- A. RC5
- B. Diffie-Hellman
- C. RSA
- D. 3DES

15. Anti-replay mechanism uses the window size of

- A. $w-1$
- B. $2w$
- C. $w+1$
- D. w

16. Which among the following are default policies of a packet filtering router

- A. discard, forward
- B. delete, forward
- C. discard, retrieve
- D. delete, retrieve

17. Which of the following systems are Integrated Mailsystems

- A. Java
- B. Active X
- C. Lotus notes
- D. C++

12. SSL sessions are created by which of the following

- A. Cipher spec protocol
- B. Handshake protocol
- C. TCP
- D. IP

13. Line tapping can be countered using

- A. Antivirus software
- B. Access control
- C. Link encryption techniques
- D. Spyware

14. Oakley is based on which of the following algorithms

- A. RC5
- B. Diffie-Hellman
- C. RSA
- D. 3DES

15. Anti-replay mechanism uses the window size of

- A. $w-1$
- B. $2w$
- C. $w+1$
- D. w

16. Which among the following are default policies of a packet filtering router

- A. discard, forward
- B. delete, forward
- C. discard, retrieve
- D. delete, retrieve

17. Which of the following systems are Integrated Mailsystems

- A. Java
- B. Active X
- C. Lotus notes
- D. C++

D
C
C
C
B
B
C
B
D
D
C
D
B
B
B
C
D
C
A
B
C
A

1. Which of the following systems are Integrated Mailsystems
 - A. Active X
 - B. C++
 - C. Java
 - D. Lotus notes

2. Which is a virus that mutates with every infection
 - A. Memory-resident virus
 - B. Parasitic virus
 - C. Polymorphic virus
 - D. Stealth Virus

3. Which of the systems objective is to provide rapid response time so that viruses can be stamped out almost as soon as they are introduced.
 - A. Virus signature scanner
 - B. Integrated mail system
 - C. Digital immune system
 - D. Mobile program systems

4. Who among the following is an individual who seizes supervisory control of the system and uses this control to evade auditing and access controls.
 - A. Masquerader
 - B. Misfeasor
 - C. Clandestine user
 - D. Casual user

5. SOCKS service is located on
 - A. TCP port 1082
 - B. TCP port 1080
 - C. TCP port 1081
 - D. TCP port 1088

13. Which among the following mechanisms prevents either sender or receiver from denying a transmitted message
- A. Integrity
 - B. Non-repudiation
 - C. Confidentiality
 - D. Authentication
14. In which model, a subject's access to an object depends on whether its identity is on a list associated with the object; access is conveyed by editing the list.
- A. In a capability-based model
 - B. RCL-based model
 - C. Access Control List-based model
 - D. DSS
15. Which of the following mechanisms is employed by Oakley algorithm to thwart clogging attacks
- A. Poppups
 - B. Nonces
 - C. Goggles
 - D. Cookies
16. The version field in the IPv4 header has a size of
- A. 8 bits
 - B. 6 bits
 - C. 4 bits
 - D. 16 bits
17. Which one of the following looks at system logs for evidence of malicious or suspicious application activity in real time
- A. host monitor
 - B. security kernel database
 - C. network monitor
 - D. reference monitor

1. Which of the following is most useful when detecting network intrusions?
 - A. Audit trails
 - B. Audit policies
 - C. Audit practices
 - D. Access control policies

2. 'No read up' is referred to as
 - A. *- property
 - B. Strict security property
 - C. Simple security property
 - D. #property

3. Which of the following documents provides the description of a packet encryption extension to IPv4 and IPv6
 - A. RFC 2408
 - B. RFC 2401
 - C. RFC 2406
 - D. RFC 2402

4. Which of the following is a code embedded in some legitimate program that is set to "explode" when certain conditions are met
 - A. Logic bomb
 - B. Trap door
 - C. Worms
 - D. Bacteria

5. A way of protecting password file is through
 - A. Check method
 - B. Access control
 - C. Non repudiation
 - D. Assessment control

6. Discarding packets with an inside source address if the packet arrived on an external interface is a counter measure to which of the following attacks
 - A. IP sniffing
 - B. Tiny fragment attack
 - C. IP address spoofing
 - D. Source routing attack

A
C
C
A
B
C
B
A
C
C
B
B
C
D
B
D
D
D
A

12. Ephemeral Diffie-Hellman involves signing the Diffie- Hellman parameter with
- A. IDEA
 - B. RSA
 - C. triple DES
 - D. DES
13. Oakley is based on which of the following algorithms
- A. 3DES
 - B. RSA
 - C. Diffie-Hellman
 - D. RC5
14. Tunnel mode provides authentication to
- A. TCP
 - B. ICMP
 - C. UDP
 - D. Entire original IP packet
15. TLS includes all of the symmetric encryption algorithms found in SSLv3, with the exception of .
- A. IDEA
 - B. Fortezza
 - C. DES
 - D. Triple DES
16. Which of the following viruses infects a master boot record
- A. Memory-resident virus
 - B. Stealth Virus
 - C. Parasitic virus
 - D. Boot sector Virus
17. Which among the following indicates whether the Security association is an AH or ESP security association
- A. Security Parameters index
 - B. Network address
 - C. IP destination address
 - D. Security Protocol identifier

IV B.Tech I Semester Regular Examinations, November – 2022
CRYPTOGRAPHY AND NETWORK SECURITY(COMMON TO CSE & IT)
(Computer Science and Engineering)

Time: 3 hours

Max. Marks: 75

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks

UNIT-I

- 1 a) Draw a matrix that shows the relationship between security mechanisms and attacks. [7]
 b) Make comparisons between the monoalphabetic ciphers and polyalphabetic ciphers. [8]
- (OR)
- 2 a) Consider an Automated Teller Machine (ATM) in which users provide a Personal Identification Number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement. [7]
 b) Discuss the Symmetric Cipher Model. [8]

UNIT-II

- 3 a) Explain the Block Cipher Modes of Operations. [7]
 b) Discuss the Blowfish algorithm with a neat diagram. [8]
- (OR)
- 4 a) How encryption and decryption are done in DES? Explain [7]
 b) What are relative prime numbers? Describe their role in fermat's theorem and Euler's theorem. [8]

UNIT-III

- 5 a) Briefly explain the Public key Cryptography Principles in detail. [7]
 b) Explain the Secure Hash Function Algorithm in detail. [8]
- (OR)
- 6 a) For SHA-512, show the equations for the values of $W_{16}, W_{17}, W_{18}, W_{19}$ and Calculate the hash function for the 48 letter message " I leave 20 million dollars to my friendly cousin bill". [7]
 b) Mention three variations of digital signatures and briefly state the purpose of each. [8]

UNIT-IV

- 7 a) Why Kerberos is needed? What problem was Kerberos designed to address? [5]
 b) List and explain the PGP services and explain how PGP message generation is done with a neat diagram. [10]



Code No: R1941051

R19

Set No. 2

IV B.Tech I Semester Regular Examinations, November – 2022
CRYPTOGRAPHY AND NETWORK SECURITY(COMMON TO CSE & IT)
(Computer Science and Engineering)

Time: 3 hours

Max. Marks: 75

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks

UNIT-I

- 1 Consider a desktop publishing system used to produce documents for various organizations. [15]
a. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.
b. Give an example of a type of publication in which data integrity is the most important requirement.
c. Give an example in which system availability is the most important requirement.

(OR)

- 2 a) Discuss the Buffer Overflow & Format String Vulnerabilities. [8]
b) Explain the TCP session hijacking with a neat diagram. [7]

UNIT-II

- 3 a) If n is composite and passes the Miller-Rabin test for base a , then n is called a strong pseudo prime to base a . Show that 2047 is a strong pseudo prime to the base 2. [7]
b) Do you agree with the statement that an increase in the key size of 1 bit doubles the security of DES? Justify your answer. [8]

(OR)

- 4 a) List and explain the strengths of DES. [7]
b) AES consists of four functions in three layers. Which of the functions are primarily for confusion and which are primarily for diffusion? Which of the layers are for confusion and which are for diffusion? Justify your answers. [8]

UNIT-III

- 5 a) How keys are exchanged in the Diffie-Hellman algorithm? Explain [7]
b) List the Application of Cryptographic Hash Functions. [8]

(OR)

- 6 a) Discuss the Message Authentication Functions. [7]
b) Explain the steps involved in SHA-512. [8]

UNIT-IV

- 7 a) Give the architecture of IP Security [7]
b) What are the main three parts of Kerberos? Give their significance. [8]



Code No: R1941051

R19

Set No. 3

IV B.Tech I Semester Regular Examinations, November – 2022
CRYPTOGRAPHY AND NETWORK SECURITY(COMMON TO CSE & IT)
(Computer Science and Engineering)

Time: 3 hours

Max. Marks: 75

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks

UNIT-I

- 1 a) Describe the Block Cipher Design Principles. [7]
b) List and explain the Web Based Attacks. [8]
(OR)
- 2 a) Describe the components of Symmetric cipher model with a neat diagram [7]
b) Give the classification of security attacks. How security services are related to security mechanisms? [8]

UNIT-II

- 3 a) What is the purpose of the Extended Euclidean algorithm? Illustrate with an example. [7]
b) Explain the Chinese remainders theorem. [8]
(OR)
- 4 a) Use Euler's Theorem to find a number "a" between 0 and 9 such that a is congruent to 7^{1000} modulo 13. [7]
b) Compare the rounds of DES algorithm with that of AES algorithm. [8]

UNIT-III

- 5 Perform encryption and decryption using the RSA algorithm for the following: [15]
a. $p = 3; q = 11, e = 7; M = 5$
b. $p = 5; q = 11, e = 3; M = 9$
c. $p = 7; q = 11, e = 17; M = 8$

(OR)

- 6 a) Explain the essential characteristics of public key cryptography. [7]
b) Discuss the Elliptic Curve Cryptography is used for data encryption. [8]

UNIT-IV

- 7 a) With the help of a neat diagram, explain the IP security architecture. [7]
b) Discuss the encapsulating security payload. [8]



Code No: R1941051

R19

Set No. 4

IV B.Tech I Semester Regular Examinations, November – 2022
CRYPTOGRAPHY AND NETWORK SECURITY (COMMON TO CSE & IT)
(Computer Science and Engineering)

Time: 3 hours

Max. Marks: 75

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks

UNIT-I

- 1 a) List and briefly define categories of Security Services & Mechanisms. [7]
b) Discuss the UDP Session Hijacking. [8]
(OR)
- 2 a) Compare TCP session Hijacking with UDP session Hijacking. [7]
b) Draw and explain the common attacks and vulnerabilities. [8]

UNIT-II

- 3 a) Use Fermat's Theorem to find a number x between 0 and 28 with x^{85} congruent to 6 modulo 29. [7]
b) What are the integer arithmetic operations related to security? Explain. [8]
(OR)
- 4 a) How do you find the relative prime of a number? Discuss [7]
b) Let $K = (k_0, k_1, k_2, \dots, k_{55})$ be a 56-bit DES key. List the 48 bits of each DES subkey K_1, K_2, \dots, K_{16} . Make a table that contains the number of subkeys in which each bit k_i is used. Can you design a DES key schedule algorithm in which each key bit is used an equal number of times? [8]

UNIT-III

- 5 a) Explain Message Authentication Requirements and What are the attacks related to message communication? [7]
b) Consider a Diffie- Hellman key with a common prime $q=11$ and primitive root $\alpha = 2$. If the user has a public key $Y_a= 9$ what is A's private key X_A ? [8]

(OR)

- 6 a) List and explain the applications of public key cryptography. [7]
b) Explain the weakness of Hash and MAC functions. [8]

UNIT-IV

- 7 What are the benefits of IPSec? Describe the three protocols used in IP Security. [15]



A.M.REDDY MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY
III B.TECH II Semester(R20) - MID Examination Marks- ACADEMIC YEAR -2022-2023

SUBJECT NAME : CNS

SUBJECT CODE: R903203

BRANCH: CSE

S.No	Hall Ticket No	MID-1				MID-2				BEST1
		Desc-15M	Online-10 M	Ass-1-5M	SUM1	Desc-15M	Online-10 M	ASS-2-5M	SUM2	BEST1(80from 20)
1	20HM1A0501	15	05	05	25	12	03	05	20	
2	20HM1A0502	14	05	05	24	12	02	05	19	
3	20HM1A0503	13	05	05	23	12	08	05	25	
4	20HM1A0504	14	04	05	23	13	03	05	21	
5	20HM1A0505	12	06	05	23	13	03	05	21	
6	20HM1A0506	12	04	05	21	15	08	05	05	
7	20HM1A0507	14	04	05	23	12	02	05	19	
8	20HM1A0508	14	03	05	22	12	05	05	22	
9	20HM1A0509	12	04	05	21	10	04	05	19	
10	20HM1A0510	14	04	05	23	12	04	05	21	
11	20HM1A0512	13	02	05	20	11	02	05	18	
12	20HM1A0513	AB	AB	AB	AB	AB	AB	AB	AB	
13	20HM1A0515	15	02	05	23	14	03	05	22	
14	20HM1A0516	AB	AB	AB	AB	AB	AB	AB	AB	
15	20HM1A0517	14	04	05	23	13	03	05	21	
16	20HM1A0518	10	03	05	18	4	04	05	20	
17	20HM1A0519	10	04	05	19	09	04	05	18	
18	20HM1A0520	09	03	05	17	AB	AB	05	05	
19	20HM1A0521	AB	AB	05	05	AB	AB	05	05	
20	20HM1A0522	14	03	05	22	13	05	05	23	
21	20HM1A0523	AB	AB	05	05	11	01	05	17	
22	20HM1A0524	12	05	05	22	13	04	05	22	
23	20HM1A0525	08	01	05	14	09	04	05	18	


A.M.REDDY MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY
 PETLURVAARTI
 Narasaraopeta, Guntur District

24	20HM1A0526	13	03	05	21	12	03	05	22
25	20HM1A0527	13	03	05	21	15	05	05	25
26	20HM1A0528	06	04	05	15	09	04	05	18
27	20HM1A0529	09	03	05	17	10	04	05	19
28	20HM1A0530	14	04	05	23	15	04	05	24
29	20HM1A0531	12	02	05	19	12	04	05	21
30	20HM1A0532	08	04	05	17	12	04	05	21
31	20HM1A0533	14	03	05	22	13	02	05	20
32	20HM1A0534	12	03	05	20	10	03	05	18
33	20HM1A0535	15	15	05	05	07	04	05	16
34	20HM1A0536	15	04	05	24	11	03	05	19
35	20HM1A0537	11	02	05	18	13	02	05	20
36	20HM1A0538	11	02	05	18	10	02	05	17
37	20HM1A0539	15	15	05	05	12	04	05	21
38	20HM1A0540	14	02	05	21	14	05	05	26
39	20HM1A0542	10	04	05	19	09	06	05	20
40	20HM1A0543	08	02	05	15	11	05	05	21
41	20HM1A0545	13	05	05	23	12	07	05	26
42	20HM1A0546	09	04	05	18	10	06	05	21
43	20HM1A0547	13	02	05	20	12	03	05	20
44	20HM1A0548	15	04	05	24	14	04	05	27
45	20HM1A0549	06	01	05	12	08	02	05	15
46	20HM1A0550	14	03	05	22	12	03	05	20
47	20HM1A0551	05	04	05	14	11	02	05	18
48	20HM1A0552	12	02	05	19	13	03	05	21
49	20HM1A0553	10	02	05	17	11	01	05	17
50	20HM1A0554	09	02	05	16	09	04	05	18
51	20HM1A0555	07	04	05	16	09	05	05	19
52	21HM5A0501	14	03	05	22	13	04	05	22

	<h2 style="margin:0;">A.M. REDDY</h2> <p style="margin:0;">Memorial College of Engineering and Technology Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada SPONSORED BY ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003</p>	<p style="margin:0;">An ISO 9001:2015 Certified Institution Web : www.amreddyengineering.ac.in E.mail: principal.amreddyengineering@gmail.com VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM, NARASARAOPET PALNADU (DIST) - 522601, CONTACT : 08647-247190.</p>
---	---	--

II-MID Examination Question Paper, MAY - 2023

Year / Sem: III/ II	Programme: B.Tech. -CS	Course Code: 05	Regulation : R19	
Course Name: CNS	Duration: 90 Min.	Total Marks: 15	Min.Passing Mark.: 06	
Q.No	Answer All Questions	Marks	Levels of Bloom's taxonomy	CO
1	Explain the PGP and S/MIME.	5	Understanding	CO-3
2	What are the differences between SSL and SSH	5	Understanding	CO-4
3	Explain the ISAKMP	5	Understanding	CO-5

	<h2 style="margin:0;">A.M. REDDY</h2> <p style="margin:0;">Memorial College of Engineering and Technology Approved by AICTE, New Delhi, Affiliated to JNTUK-Kakinada SPONSORED BY ATLURI MASTAN REDDY EDUCATIONAL SOCIETY, REG. NO. 450/2003</p>	<p style="margin:0;">An ISO 9001:2015 Certified Institution Web : www.amreddyengineering.ac.in E.mail: principal.amreddyengineering@gmail.com VINUKONDA ROAD, MASTAN REDDY NAGAR, PETLURIVARIPALEM, NARASARAOPET PALNADU (DIST) - 522601, CONTACT : 08647-247190.</p>
---	---	--

II-MID Examination Question Paper, MAY - 2023

Year / Sem: III/ II	Programme: B.Tech. -CS	Course Code: 05	Regulation : R20	
Course Name: CNS	Duration: 90 Min.	Total Marks: 15	Min.Passing Mark.: 06	
Q.No	Answer All Questions	Marks	Levels of Bloom's taxonomy	CO
1	Give the structure of CMAC. What is the difference between CMAC and HMAC?	5	Understanding	CO-3
2	What are the differences between SSL and SSH	5	Understanding	CO-4
3	Briefly explain Encapsulating IP Security Payload?	5	Understanding	CO-5

PETLURIVARI PALEM
 NARASARAOPET (Midi), Guntur(Dr.

COURSE PLAN

Subject code	Name of the subject	Class /Sem	Name of the faculty & Designation	No. of students	Total periods per Sem/Year	
					Lectures	Tutorials
R20 32053	CNS	BT/II	V.veerabrahmachari	52	75	

Week No.	Lecture No.	Topic	Date on which Completed*
01	1	Introduction to Cyber Security	
	2	Cyber security goals	
	3	Security attacks	
	4	Security active attacks	
	5	Security passive attacks	
02	1	Security services	
	2	Security services	
	3	Security Mechanizes	
	4	Security Mechanizes	
	5	Security Basic rules	
03	1	Security Basic rules	
	2	Basic rules of Cryptographics	
	3	Basic Concepts of Cryptographics	
	4	Mathematics of Cryptography	
	5	Mathematics of Cryptography	
04	1	At the Crypt, plaintext, Near text	
	2	Introduction to unit-11	
	3	Introduction of cryption of Cryptions	
	4	At mathematics of symmetric	
	5	Key Cryptography	

Signature of the HOD

Date:

* This column has to be filled-up in the copy kept with faculty members after completing the lecture/tutorial.

Note: One period should be allocated for revision and indicated as such at the end of each month(4 weeks)

Signature of the Faculty

Date:

Principal
AMRITA ENGINEERING COLLEGE OF
TECHNOLOGY
PETALAJAYAM, TAMIL NADU
605 006

COURSE PLAN

Subject code	Name of the subject	Class /Sem	Name of the faculty & Designation	No. of students	Total periods per Sem/Year	
					Lectures	Tutorials

Week No.	Lecture No.	Topic	Date on which Completed*
05	1	Key cryptography	
	2	Cryptography Concept	
	3	Introduction to Modern Symantic key	
	4	Cipher Data encryption	
	5	Cipher Data encryption	
06	1	DES	
	2	DES	
	3	DES	
	4	Advanced encryption stands	
	5	Advanced encryption stands.	
07	1	Advanced encryption Stands	
	2	IDEA	
	3	Blow Fish	
	4	Introduction to Unit-III	
	5	Introduction to Asymantic	
08	1	Basic rules of Asymantic	
	2	Encryption standards	
	3	Encryption Standards	
	4	Maths of Asymantic	
	5	Chinese algorithms.	


Signature of the HOD

Date: _____


Signature of the Faculty

Date: _____

* This column has to be filled-up in the copy kept with faculty members after completing the lecture/tutorial.

Note: One period should be allocated for revision and indicated as such at the end of each month(4 weeks).


COURSE PLAN

Subject code	Name of the subject	Class /Sem	Name of the faculty & Designation	No. of students	Total periods per Sem/Year	
					Lectures	Tutorials

Week No.	Lecture No.	Topic	Date on which Completed*
09	1	Chinese Algorithms	
	2	Prime number algorithms	
	3	RSA Algorithms	
	4	RSA algorithms	
	5	PSS Algorithms	
10	1	PSS Algorithms	
	2	Asymmetric Key Cryptography	
	3	Asymmetric Key Cryptography	
	4	Asymmetric Key Cryptography	
	5	Introduction to Unit - IV	
11	1	Data Integrity	
	2	Data Integrity	
	3	Data Integrity	
	4	Digital signature	
	5	Key management of Security	
12	1	Key management of Security	
	2	Message Integrity	
	3	Message Authentication	
	4	Cryptography hash - strings	
	5	CMAC.	


Signature of the HOD

Date: _____


Signature of the Faculty

Date: _____

* This column has to be filled-up in the copy kept with faculty members after completing the lecture/tutorial.

Note: One period should be allocated for revision and indicated as such at the end of each month (4 weeks)



COURSE PLAN

One copy to be submitted to the HOD one week before the commencement of the Semester

Subject code	Name of the subject	Class /Sem	Name of the faculty & Designation	No. of students	Total periods per Sem/Year	
					Lectures	Tutorials

Week No.	Lecture No.	Topic	Date on which Completed*
13	1	HMAC	
	2	Digital signature	
	3	Types of digital signature	
	4	Key management of cryptography	
	5	Key management of cryptography	
14	1	Introduction to unit IV	
	2	Network Security.	
	3	security at application layer	
	4	Security at application layer	
	5	PGP	
15	1	S/MINE	
	2	MINE	
	3	Security at the transport layer	
	4	SSL and TLS	
	5	SSL and TLS	

Principal
 A.M. REDDY MEMORIAL COLLEGE OF
 ENGINEERING AND TECHNOLOGY
 PETLURIVARIPALEM
 NARASARAOPET, GUNTUR (D.T)

Signature of the HOD

Date: _____

Signature of the Faculty

Date: _____

* This column has to be filled-up in the copy kept with faculty members after completing the lecture/tutorial.

Note :One period should be allocated for revision and indicated as such at the end of each month(4 weeks)



A.M. REDDY MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY
(Approved by AICTE, New Delhi & Affiliated To JNTU, Kakinada)
Petlurivaripalem, Narasaraopet, Guntur (D.T)

LESSON PLAN

S.No	Date & Day of the Week	Time		Topic(s) Covered	E.T Gadgets used. If any(LCD/OHP/Charts/Models)
		From	To		
1	19/1/23	11:20	12:10	Introduction to Cyber security	C/B
2	20/1/23	12:10	1:00	Cyber Security Goals	C/B
3	21/1/23	11:20	12:10	Security attacks	C/B
4	23/1/23	11:20	12:10	Security active attacks	PPT
5	24/1/23	10:20	11:10	Security passive attacks	PPT
6	25/1/23	11:20	12:10	Security Services	C/B
7	27/1/23	10:20	11:10	Security Services	C/B
8	28/1/23	12:10	1:00	Security Machines	C/B
9	30/1/23	11:20	12:10	Security machines	PPT
10	31/1/23	12:10	1:00	Security Basic rules	C/B


Signature of the Faculty Member


Signature of the Head of the Dept.

A.M. REDDY MEMORIAL COLLEGE
ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
Narasaraopet (Mdl), Guntur(Dr)

A.M. REDDY MEMORIAL COLLEGE OF ENGINEERING & TECHNOLOGY
PETLURIVARI PALEM
NARASARAOPET (M.D.), GUNTUR (D.T)


S.No	Date & Day of the Week	Time		Topic(s) Covered	E.T Gadgets used. If any(LCD/OHP/Charts/Models)
		From	To		
11	1/2/23	11:20	12:10	Security basic rules.	CB
12	2/2/23	11:20	12:10	Basic rules of Cryptographics	PPT
13	3/2/23	12:10	1:00	Basic Concepts of Cryptographics.	CB
14	4/2/23	10:20	11:10	Mathematics of Cryptography	CB
15	6/2/23	11:20	12:10	Mathematics of Cryptography	CB
16	7/2/23	12:10	1:00	at the Crypto, plaintext, Near text.	CB
17	8/2/23	12:10	1:00	Introduction to unit-2	CB
18	9/2/23	11:20	12:10	Introduction of Cryption of Cryption.	CB
19	10/2/23	12:10	1:00	at Mathematics of Symmetric	CB
20	11/2/23	10:20	11:10	Key Cryptography	CB
21	13/2/23	11:20	12:10	Key Cryptography	CB
22	14/2/23	12:10	1:00	Crypto graphy Concept	CB
23	15/2/23	10:20	11:10	Induction to modern Symantic Key	CB
24	16/2/23	12:10	1:00	Cipher Data encryption	CB
25	20/2/23	11:10	12:10	Cipher Data Encryption	PPT

Signature of the Faculty Member

Signature of the Head of the Dept.

S.No	Date & Day of the Week	Time		Topic(s) Covered	E.T Gadgets used. If any(LCD/OHP/Charts/Models)
		From	To		
26	21/2/23	11:20	12:10	DES	C/R
27	22/2/23	11:20	12:10	DES	C/R
28	23/2/23	10:20	11:10	DES	PPT
29	24/2/23	12:10	1:00	Advanced encryption Standards	C/R
30	25/2/23	1:50	2:40	Advanced encryption Standards	C/R
31	27/2/23	11:20	12:10	Advanced encryption Standards	C/R - PPT
32	28/2/23	12:10	1:00	IDEA	C/R
33	1/3/23	12:10	1:00	Blow Fish	C/R
34	2/3/23	12:10	1:00	Introduction to unit - III	C/R
35	3/3/23	9:30	10:20	Introduction to Asymmetric	C/R
36	4/3/23	10:20	11:10	Basic rules of Asymmetric	C/R
37	15/3/23	11:20	12:10	Encryption standards.	C/R
38	16/3/23	12:10	1:00	Encryption standards.	C/R
39	17/3/23	12:10	1:00	Maths of Asymmetric	C/R
40	18/3/23	11:20	12:10	Chinese Algorithms.	C/R


 Signature of the Faculty Member


 Signature of the Head of the Dept
 PETURUVAIPALEM
 ANNAMMA MEMORIAL COLLEGE OF ENGINEERING
 AND TECHNOLOGY
 HEAD OF THE DEPARTMENT

S.No	Date & Day of the Week	Time		Topic(s) Covered	E.T Gadgets used. If any(LCD/OHP/Charts/Models)
		From	To		
41	20/3/23	11:10	12:10	Chinese Algorithms.	PPT
42	21/3/23	12:10	1:00	Prime member Algorithms.	PPT
43	23/3/23	2:40	3:30	RSA Algorithms	CB
44	25/3/23	11:20	12:10	RSA Algorithms	CB
45	27/3/23	10:20	11:10	PSS Algorithms.	CB
46	28/3/23	11:20	12:10	PSS Algorithms.	CB
47	29/3/23	12:10	1:00	Asymmetric Key Cryptography	CB
48	31/3/23	1:50	2:40	Asymmetric Key Cryptography	PPT
49	1/4/23	12:10	1:00	Asymmetric Key Cryptography.	PPT
50	3/4/23	11:20	12:10	Introduction to Unit-IV	CB
51	5/4/23	11:20	12:10	Data Integrity	CB
52	6/4/23	11:20	12:10	Data Integrity	CB
53	10/4/23	11:20	12:10	Data Integrity	CB
54	11/4/23	12:10	1:00	Digital Signature	PPT
55	12/4/23	12:10	1:00	Key management of Security	CB

Signature of the Faculty Member

Signature of the Head of the Dept

PALEM
 ABRETT NATIONAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 ETURIVARI PALEM
 Narasaraopet (Mdl), Guntur Dt

PALEM
 ABRETT NATIONAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 ETURIVARI PALEM
 Narasaraopet (Mdl), Guntur Dt

S.No	Date & Day of the Week	Time		Topic(s) Covered	E.T Gadgets used. If any(LCD/OHP/Charts/Models)
		From	To		
56	13/4/23	12:10	11:00	Key management of Security	CB
57	15/4/23	11:20	12:10	Message Integrity	CB
58	17/4/23	12:10	1:00	Message Authentication	CB
59	18/4/23	11:20	11:10	Cryptography Hash -oring	PPT
60	19/4/23	11:20	12:10	CMAC	PPT
61	20/4/23	12:10	1:00	HMAC	PPT
62	21/4/23	11:20	12:10	Digital Signature	CB
63	24/4/23	12:10	1:00	Types of Digital Signature	CB
64	25/4/23	12:10	1:00	Key management of Cryptography	CB
65	26/4/23	11:20	12:10	Key management of Cryptography	CB
66	27/4/23	10:20	11:10	Introduction to Unit-IV	CB
67	28/4/23	11:20	12:10	Network Security	CB
68	29/4/23	11:20	12:10	Security at application layer	CB
69	1/5/23	11:20	12:10	Security of application layer	CB
70	1/5/23	12:10	1:00	PGP	PPT


Signature of the Faculty Member

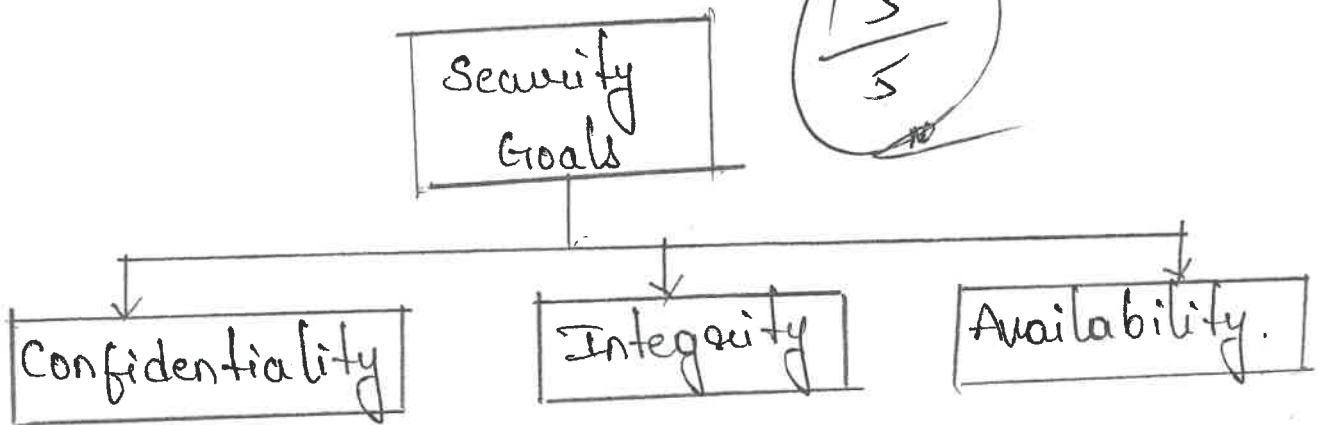

Signature of the Head of the Dept

DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING
MADRAS INSTITUTE OF TECHNOLOGY
CHENNAI - 600 076

S.No	Date & Day of the Week	Time		Topic(s) Covered	E.T Gadgets used. If any(LCD/OHP/Charts/Models)
		From	To		
71	2/5/23	11:20	12:10	S/MIME	CB
72	3/5/23	11:20	12:10	MIME	PPT
73	4/5/23	11:20	12:10	Security at the transport layer	PPT
74	5/5/23	11:20	12:10	SSL and TLS	CB
75	6/5/23	12:10	1:00	SSL and TLS	CB
76					
77					
78					
79					
80					
81					
82					
83					
84					
85					
86					
87					
88					

Explain about security goals and threads services and mechanisms?

Let us first discuss the three security goals: confidentiality, integrity, and availability.



1) Confidentiality:

→ It is the most common aspect of information security. we need to protect our confidential information.

→ An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

→ In the military, concealment of sensitive information is the major concern.

→ Confidentiality not only appears in military, but also in industry for hiding some information from the computers.

Integrity:

- Information needs to be changed constantly. In a bank, when a depositor withdraws money, the balance of her account needs to be changed.
- Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.
- Integrity violation is not necessarily the result of a malicious act.

Availability:

- The third component of information security is availability.
- The information created and stored by an organization needs to be available to authorized entities.
- The unavailability of information is just as harmful for an organization as the lack of confidentiality (or) integrity.

(ii) Security Threats:

- A threat is a possible danger to breach security.
- It may be either intentional or accidental.

Types:

1) Interruption: An asset of system is destroyed or becomes unavailable or unusable.

→ It is an attack on availability

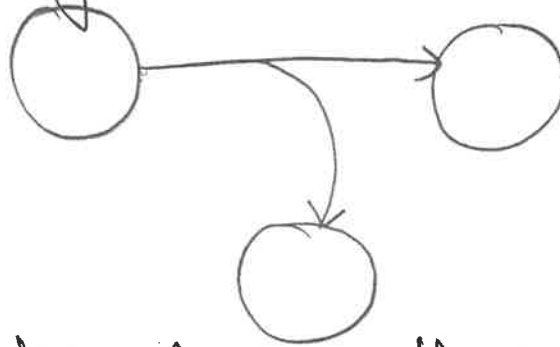
eg: Destruction of a piece of blu



2) Interception: An ~~unauthorized~~ party gains access to an asset.

→ It is an attack on confidentiality.

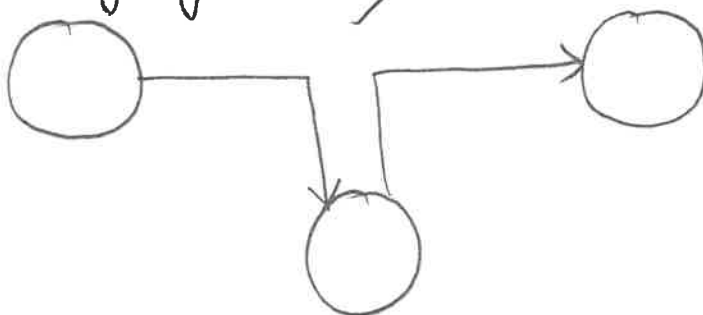
eg: wiretapping



3. modification: An unauthorized party not only gains access to but to tampers with an asset.

→ It is an attack on integrity.

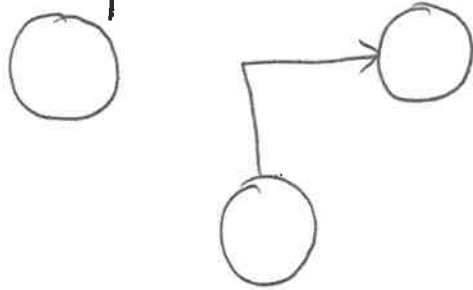
eg:- changing values in data file.



4. fabrications: An unauthorized party inserts counterfeit objects into the system.

→ It is an attack on authenticity.

eg: Insertion of spurious message in a network



(iii) Security Services: A service enhances the security of data processing systems and the information transfer of an organization.

1) Authentication: The authentication service is concerned with assuring that communication is authentic.

→ Peer Entity Authentication: used in association with a logical connection to provide confidentiality in the identity of connected devices.

→ Data Origin Authentication: It is a connectionless transfer, provides assurance of received data.

2) Access control: It means prevention of unauthorized use of resource. To achieve this, each entity trying to gain access must be authenticated.

3. Data confidentiality: It is the protection of transmitted data from passive attacks.

4. Data integrity: It means that assurance the data received is exactly as sent by authorized entity.

5. Non-repudiation: It provides the protection against denial by one of entities involved in communication.

(iv) Security mechanisms: A mechanism is designed to detect, prevent or recover from a security attack.

Types:

1) Encipherment: The use of mathematical algorithms to transform data into a form is not readily intelligible.

2) Digital signature: Data appended to, or cryptographic transformation of data until that allows a recipient of data unit to prove integrity.

3) Access control: A variety of mechanisms that enforce access rights to resources.

4) Data integrity: A variety of mechanisms used to assure the integrity of data unit.

5. Authentication exchange: It is used to ensure the identity of an entity by means of information-exchange.

6. Traffic Padding: Insertion of bits into gaps in a datastream to frustrate traffic analysis attempts.

7. Routing control: enables selection of physically secured routes from certain data and allows routing changing.

8. Notarization: It means the use of trusted third party to assure certain properties of data exchange.

2. Explain any three transposition techniques:

→ In transposition encryption techniques, the cipher text is obtained by performing some sort of permutation on plaintext letters.

(i) The Rail fence: Here, the plaintext is written downwards on successive 'rails' of an imaginary fence, then moving up when we get

we get to bottom.

→ The message is read off in rows.

Eg: WE ARE DISCOVERED FLEE AT ONCE

W	.	.	.	E	C	.	.	.	R	.	.	.	L	.	.	.	T	.	.	E					
.	E	.	.	R	.	.	D	.	.	S	.	.	O	.	.	E	.	.	E	.	F	.	E	.	A	.	O	.	C
.	.	A	I	V	.	.	.	D	.	.	.	E	.	.	.	N	

Ciphertext: WECRL TEEFD SOEET EAOCA IVDEN

(ii) Route cipher: The plaintext is first written out in a grid of given dimensions, then read off in a pattern, given in the key

W	R	I	O	R	F	E	O	E
E	E	S	V	E	L	A	N	J
A	D	C	E	D	E	T	C	K

Ciphertext: WRIDREEOE EESVELANJADCEDE TCK

(iii) Columnar Transposition:

The message is written off in rows of a fixed length, and then read out again column by column.

eg: W E A R E D
 I S C O V E
 R E D F L E
 E A T O N C
 E

Ciphertext: EVLNI ACDT ESEA ROFO DEEC WIREE

3) What is meant by block cipher? Explain DES algorithm?

Block cipher: - It is a method of encrypting text in which a cryptographic key and algorithm are applied to a block of data at one bit of time.

→ The general blocksize may be 64 (or) 128 bits.

eg: DES, AES, IDEA, Blowfish.

Data encryption standard: - It is a block cipher was selected by the national bureau of standard as an official FIPS for the US in 1976.

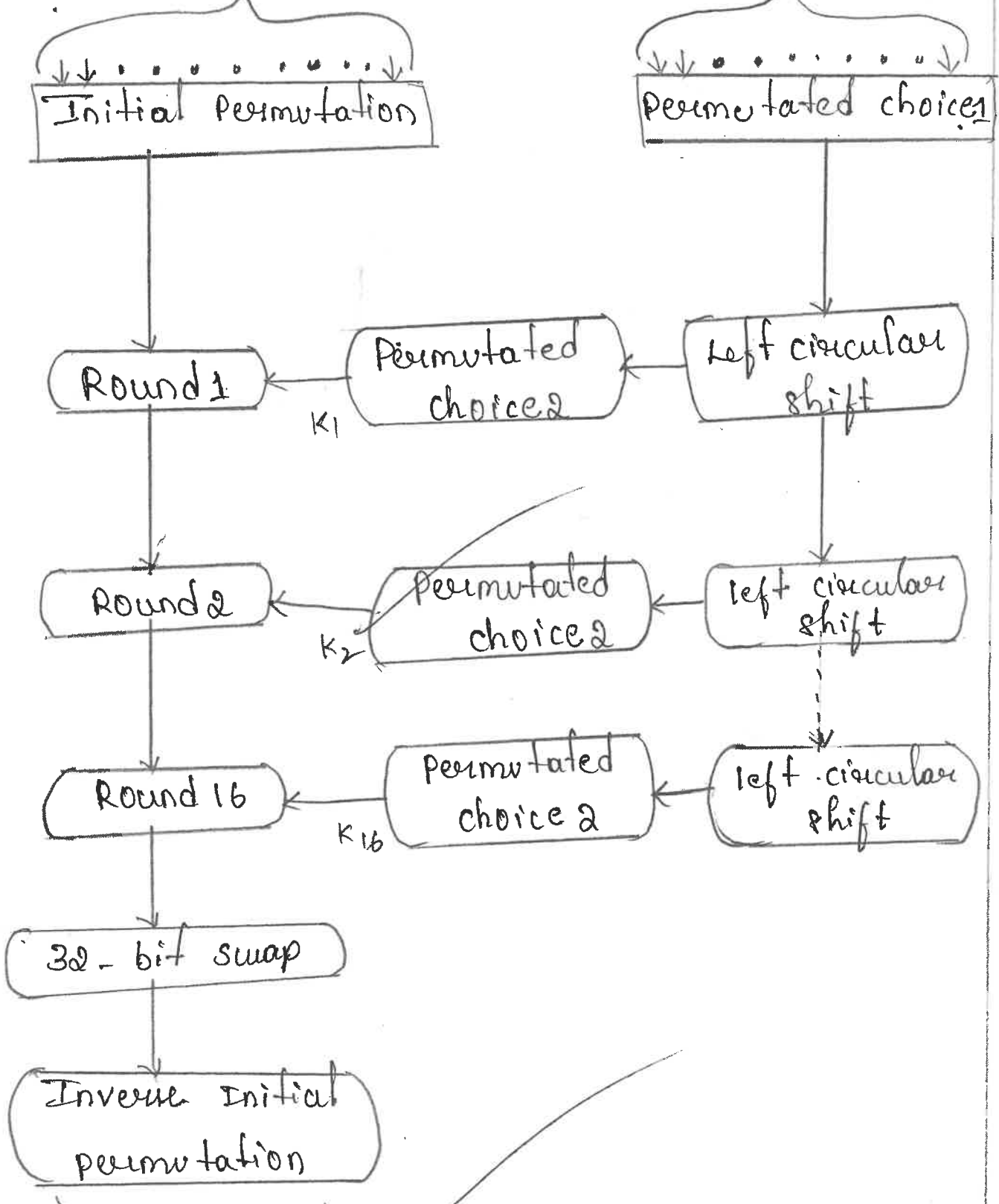
→ It is based on a symmetric key algorithm that uses 56-bit key.

→ It takes fixed string of plaintext bits and transforms it through a complicated operations.

→ In case of DES, the blocksize is 64 bits.

Structure: 64 bit plaintext

64-bit key



64-bit ciphertext

- Left side: the plain text passes through initial permutation which produced permuted output and it undergoes 16 rounds. last round have 64 bits.
- Right side: It shows subkey generation key process.

Details of single Round:

→ The left and right halves of each 64-bit intermediate values are treated as separate 32-bit quantities labeled as left (L) and Right (R).

$$L_i = R_{i-1}$$

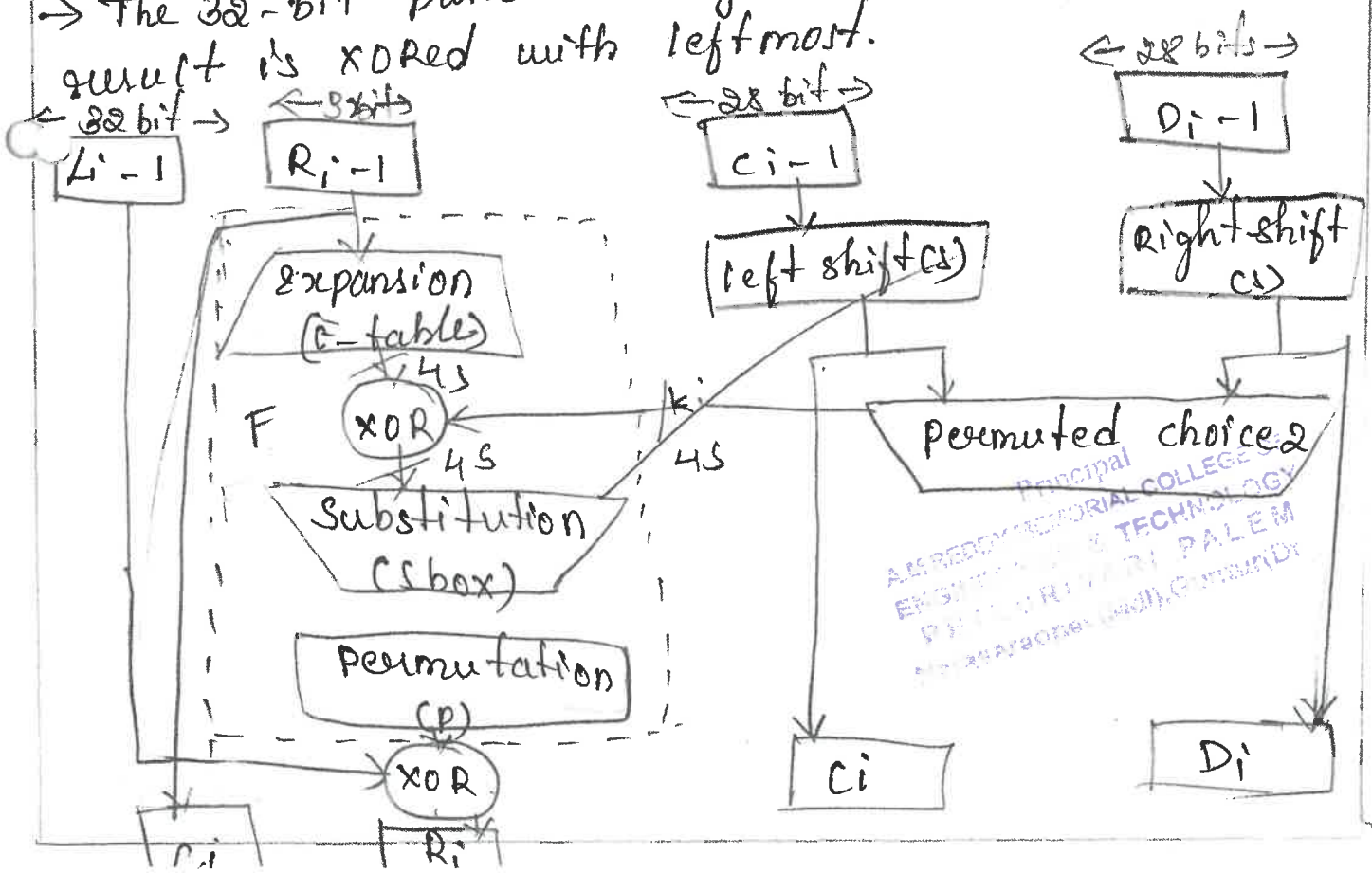
$$R_i = L_{i-1} \text{ (or) } F(R_{i-1}, k_i)$$

→ The round key k_i is 48 bits. The R input is 32 bit.

→ This R input is first expanded to 48 bits using a table that defines a permutation plus and expansion that involves duplication of 16 and R bits.

→ The 48 bits passes through a substitution function with 32 bit o/p.

→ The 32-bit passes through permutation box and result is XORed with leftmost.



4) Explain AES algorithm.

→ AES is a symmetric block cipher intended to replace DES for commercial applications.

→ It uses 128 bit block size and key size of 128, 192 or 256 bits.

→ It was published by National Institute of Standards and Technology in 2001.

AES Cipher:

→ AES is having following parameters.

key size (word / bytes / bit)	4 / 16 / 128	6 / 24 / 192	8 / 32 / 256
plaintext block size	4 / 16 / 128	4 / 16 / 128	4 / 16 / 128
No. of rounds	10	12	14
Round key size	4 / 16 / 128	4 / 16 / 128	4 / 16 / 128
Expanded key size	44 / 176	52 / 208	60 / 240

AES Encryption & Decryption structure:-

→ This structure does not follow Feistel structure.

→ Data block size is 128 bits.

→ key size is 128 bits or 192 bits or 256 bits

→ No. of rounds is 10, 12, 14.

key (16 bytes)
Expand key

plain-text (16 bytes)

plaintext (16 bytes)

Round 1

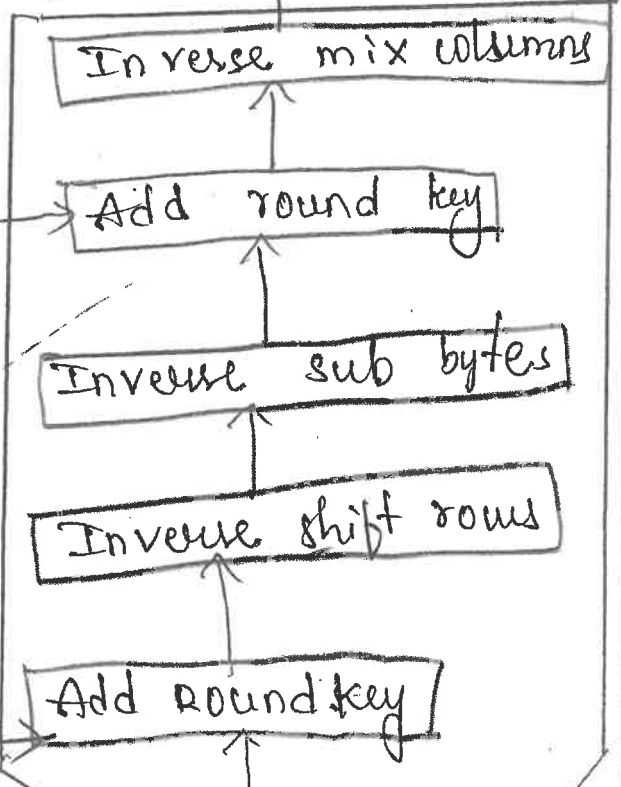
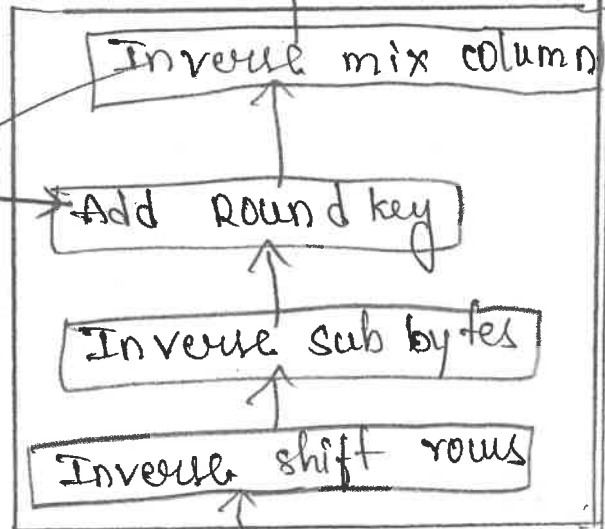
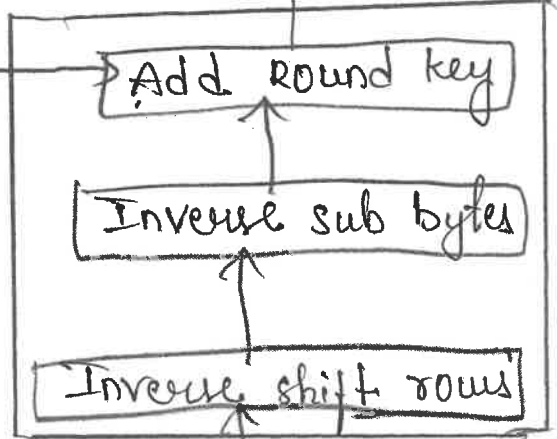
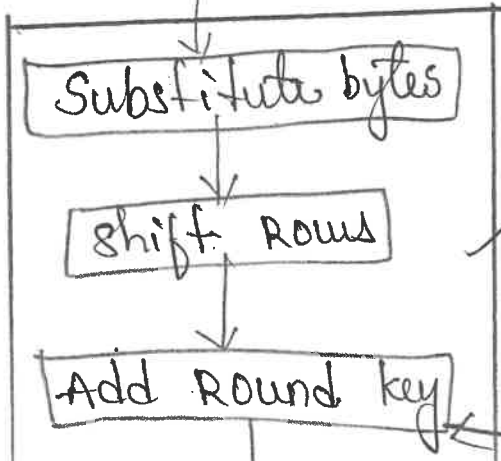
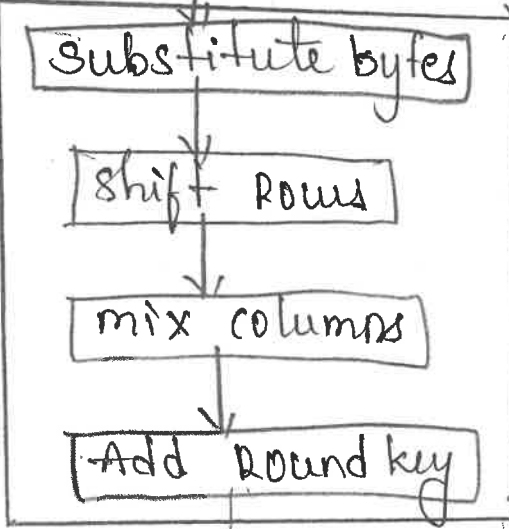
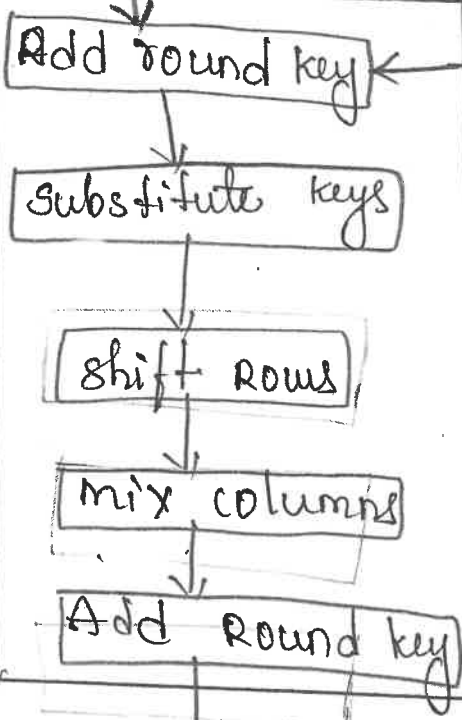
Round 9

Round 10

Round 10

Round 9

Round 1



ciphertext (16 bytes)

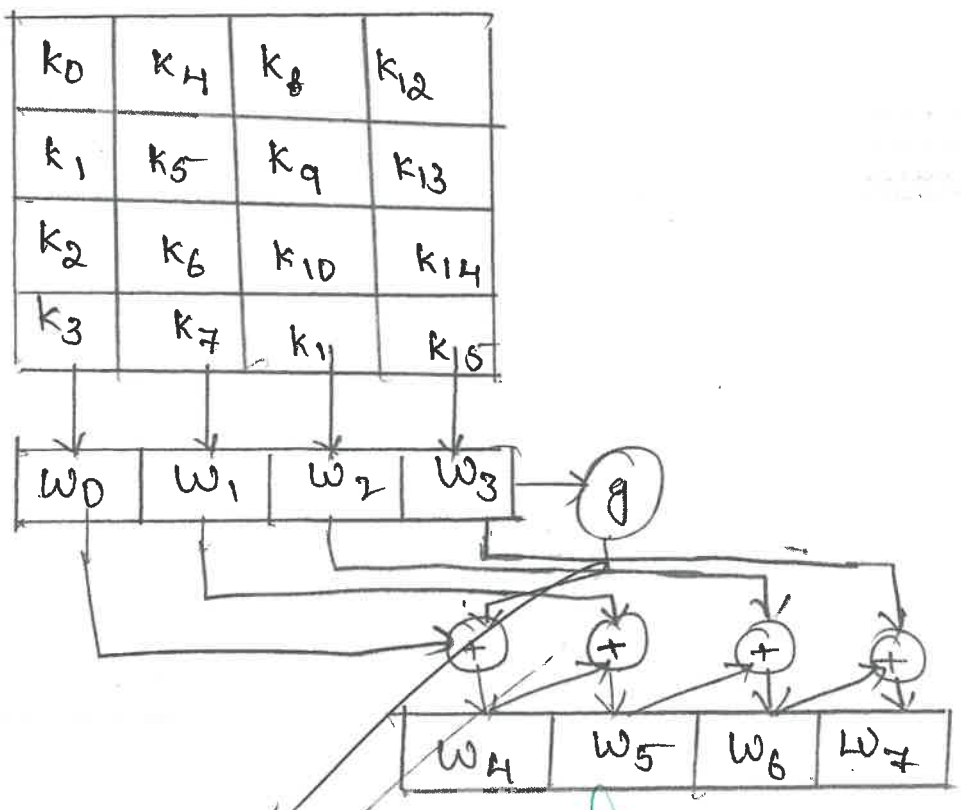
ciphertext (16 byte)

→ AES consists of four separate functions in each round.

- They are (i) byte substitution
- (ii) permutation / shifting of rows.
- (iii) mixing of columns
- (iv) XOR with a key / Add Round key

AES key expansion:

→ It will take 128 bit key and expands into array of 44/52/60/32 bit-words.

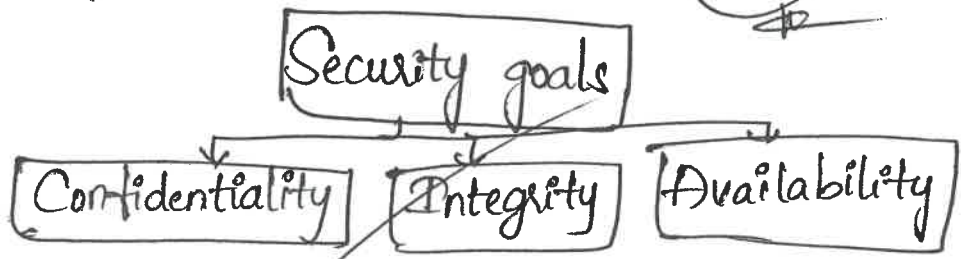


1) Explain about security goals, threats, services & mechanisms

Security goals:-

→ Majorly there are 3 security goals. They are confidentiality, Integrity and availability.

5/5



Confidentiality:

- It is the most common aspect of information security. We need to protect our confidential information
- An organization needs to guard against those malicious actions that endanger the confidentiality of its information.
- In the military, concealment of sensitive information is the major concern.
- Confidentiality not only appears in military, but also in industry for hiding some information from the competitors.
- It applies to the storage of the information, is also applies to the transmission of information.

Integrity:

- Information needs to be changed constantly. In a bank, when a depositor withdraws money, the balance of her account needs to be changed.
- Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.
- Integrity violation is not necessarily the result of malicious act.

Availability:

- The third component of information security is availability.
- The information created and stored by an organization needs to be available to authorized entities.
- The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity.

(ii) Security Threats:

- A threat is a possible danger to breach security.
- It may be either intentional & accidental.

Types

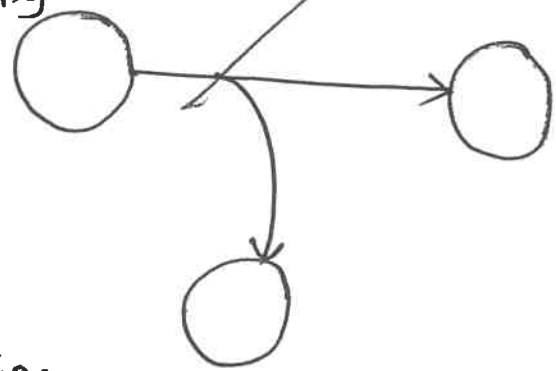
1. Interruption:-- An asset of system is destroyed or becomes unavailable or unusable.

→ It is an attack on availability.
eg: Destruction of a piece of hardware



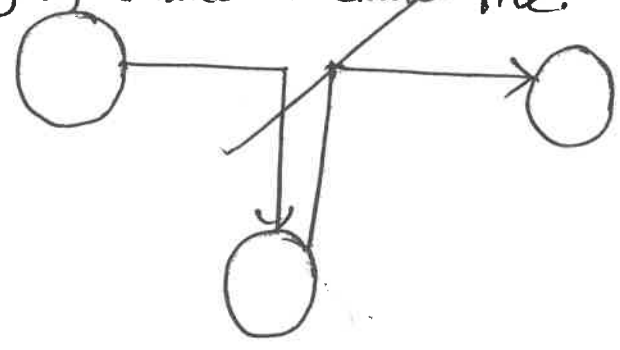
2. Interception: An unauthorized party gains access to an asset.

→ It is an attack on confidentiality.
eg: Wiretapping



3. Modification: An unauthorized party not only gains access to but to tamper with an asset.

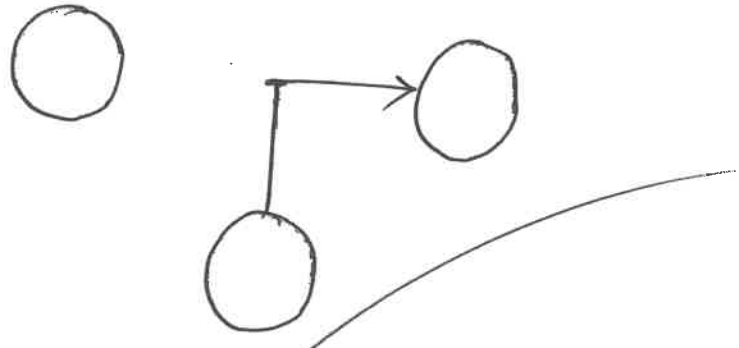
→ It is an attack on integrity.
eg: changing values in data file.



iv) Fabrication: - An unauthorized party inserts counterfeit objects into the system.

→ It is an attack on authenticity.

eg: Insertion of spurious messages in a network.



iii) Security Services: A service enhances the security of data processing systems and the information transfers of an organization.

cb) Authentication: - The authentication service is concerned with assuring that a communication is authentic.

→ Peer Entity Authentication: used in association with a logical connection to provide confidentiality in the identity of connected devices.

→ Data origin Authentication: It is a connectionless transfer, provides assurance of received data.

2) Access Control: - It means prevention of unauthorized use of resource. To achieve this, each entity trying to gain access must be authenticated.

3) Data Confidentiality:- It is the protection of transmitted data from passive attacks.

4) Data Integrity:- It means that assurance the data received is exactly as sent by authorized entity,

5) Non-repudiation: It provides the protection against denial by one of entities involved in communication.

6) Availability:- It requires that computer system assets be available to authorized parties when needed.

iv) Security Mechanisms:- A mechanism is designed to detect, prevent or recover from a security attack,

Types:-

1) Encipherments:- The use of mathematical algorithms to transform data into a form that is not readily intelligible.

2) Digital Signature: Data appended to, or cryptographic transformation of data until that allows a receipt of data unit, to prove integrity.

3) Access Control: - A variety of mechanisms that enforce access rights to resources.

4) Data Integrity: A variety of mechanisms used to assure the integrity of data unit.

5) Authentication Exchange: It is used to ensure the identity of an entity by means of information exchange.

6) Traffic Padding: Insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

7) Routing Control: Enables selection of physically secured routes from certain data and allows routing changing.

8) Notarization: - It means the use of trusted third party to assure certain properties of data exchange.

2) Explain any three transposition techniques:-

→ In transposition encryption techniques, the cipher text is obtained by performing some sort of permutation on plaintext letters.

i) The Rail Fence :- Here, the plaintext is written downwards on successive 'rails' of an imaginary fence, then moving up when we get to bottom.

→ The message is read off in rows.

Eg: WE ARE DISCOVERED FLEE AT ONCE

W	.	.	.	E	C	.	.	.	R	L	.	.	.	T	.	.	E
.	E	.	R	.	D	.	S	.	O	.	E	.	E	.	F	.	E	.	A	.	O	.	.	G	
.	.	A	.	.	.	I	V	.	.	.	D	.	.	.	E	N	

Cipher Text: WEERL TEERD SOEEF EAACA IDEN

ii) Route Cipher: The plaintext is first written out in a grid of given dimensions, then read off in a pattern, given in the key

W	R	I	O	R	F	E	O	E
E	E	S	V	E	L	A	N	J
A	D	C	E	D	E	T	C	X

Cipher Text: WRIOREFE EESVELANJ ADCED
TCX

iii) Columnar Transposition: The message is written off in rows of a fixed length, and then read out again column by column

eg: 6 3 2 4 1 5
 W E A R E D
 I S C O V E
 R E D F L E
 E A T O N C
 E

Cipher Text: - EVLN ACDT ESEA ROFO DEEC WIRE E

3) What is meant by block cipher? Explain DES Algorithm.

Block Cipher: - It is a method of encrypting text in which a cryptographic key and algorithm are applied to a block of data at one bit of time.

→ The general block size may be 64 or 128 bits.

eg: DES, AES, IDEA, Blowfish.

DES - Data Encryption Standard: -

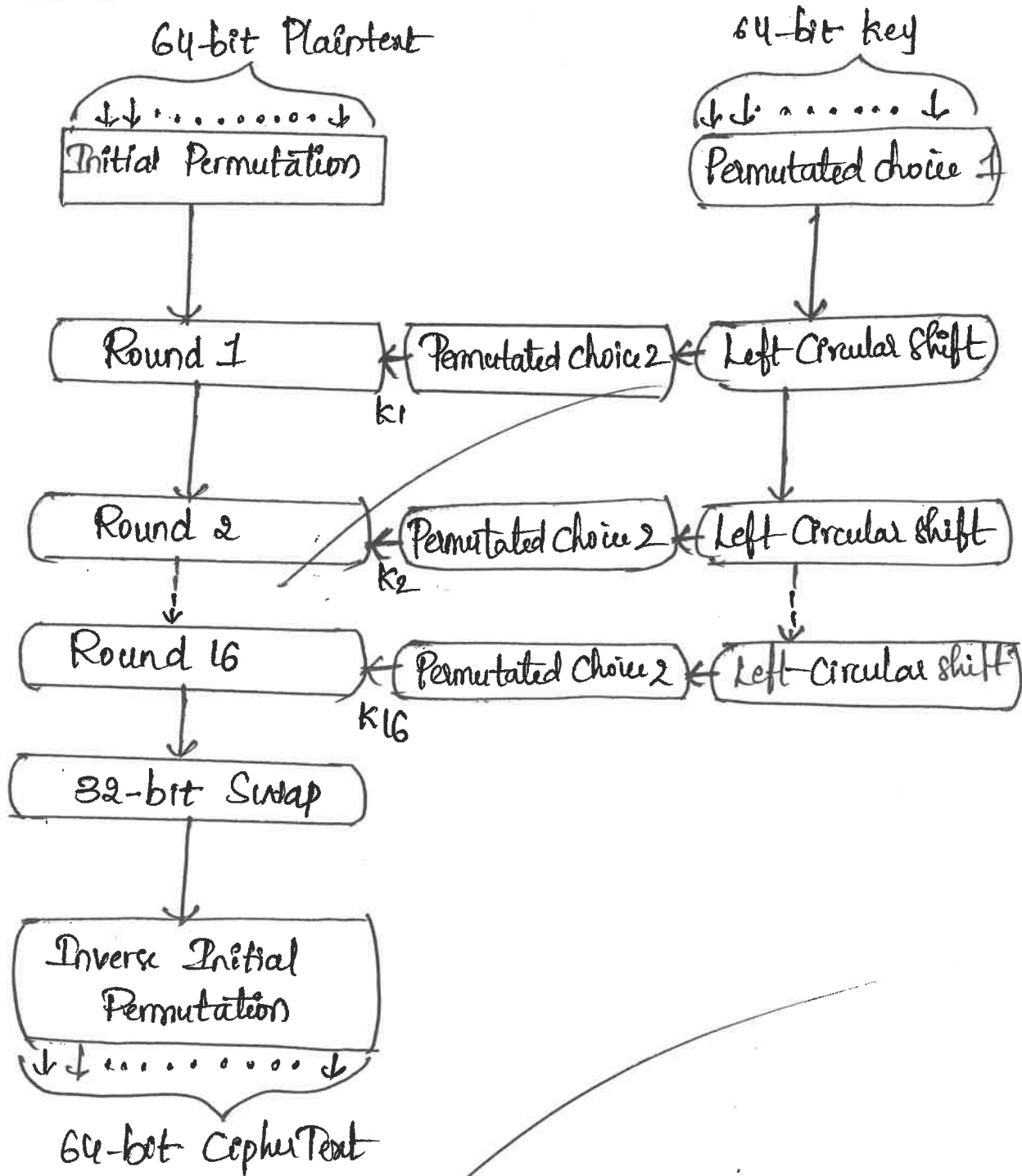
→ It is a block cipher was selected by the National Bureau of standards as an official FIPS for the US in 1976.

→ It is based on a symmetric key algorithm that uses 56-bit key.

→ It takes fixed string of plaintext bits and transforms it through a complicated operations

→ In case of DES, the blocksize is 64 bits.

Structure:-



Left side - The plaintext passes through initial permutation which produced permuted output and it undergoes 16 rounds. Last round output have 64-bits.

Right side - It shows subkey generation. Key process.

→ Details of Single Round:-

→ The left and right halves of each 64-bit intermediate values are treated as separate 32-bit quantities labeled as Left (L) and Right (R).

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, k_i)$$

→ The round key k_i is 48 bits. The R input is 32 bit

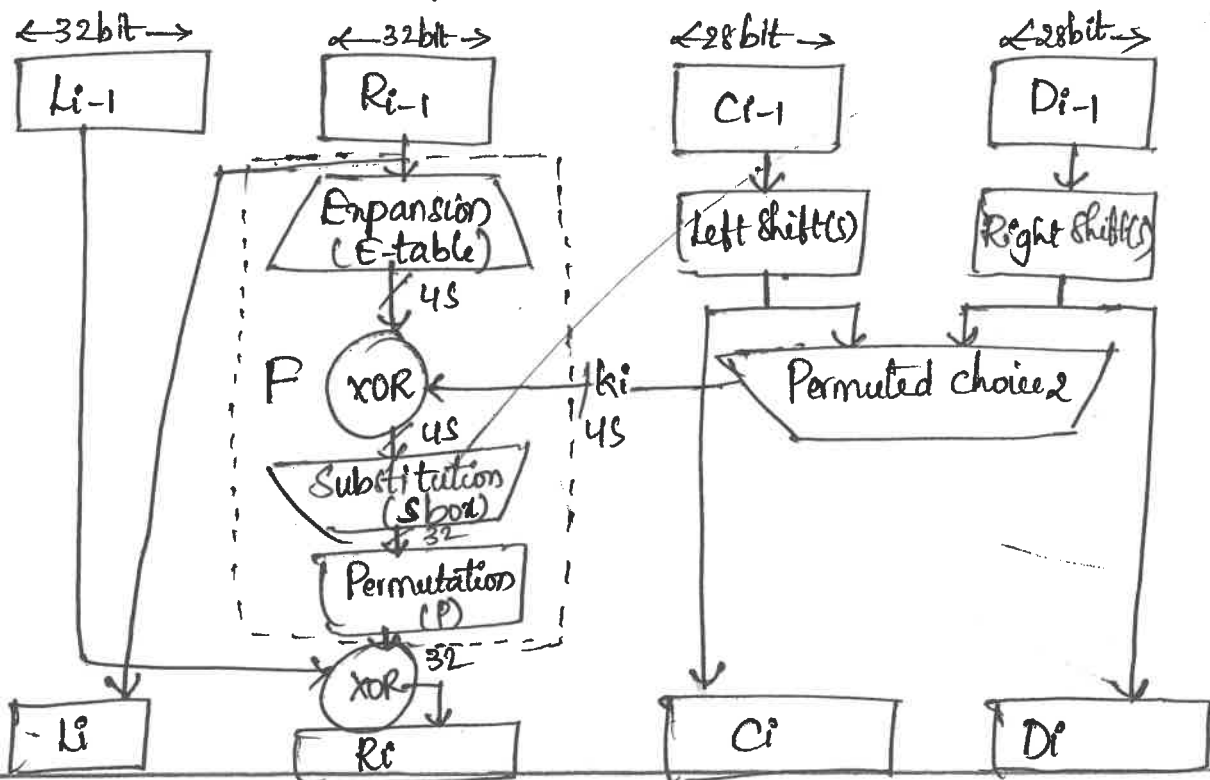
→ This R input is first expanded to 48 bits using a table that defines a permutation plus and expansion that involves duplication of 16 and R bits.

→ The resulting 48 bits are XORed with k_i .

→ The 48 bits passes through a substitution function with 32 bit o/p.

→ The role of s-boxes consists of set of 8 s boxes, each of accept 6-bits as I/p and 4-bits as o/p.

→ The 32-bit passes through permutation box and result is XORed with leftmost.



4) Explain AES Algorithm

- AES is a symmetric block cipher intended to replace DES for commercial applications.
- It uses 128 bit block size and a key size of 128, 192 or 256 bits.
- It was published by National Institute of Standards and Technology in 2001.

AES Cipher:-

→ AES is having following parameters.

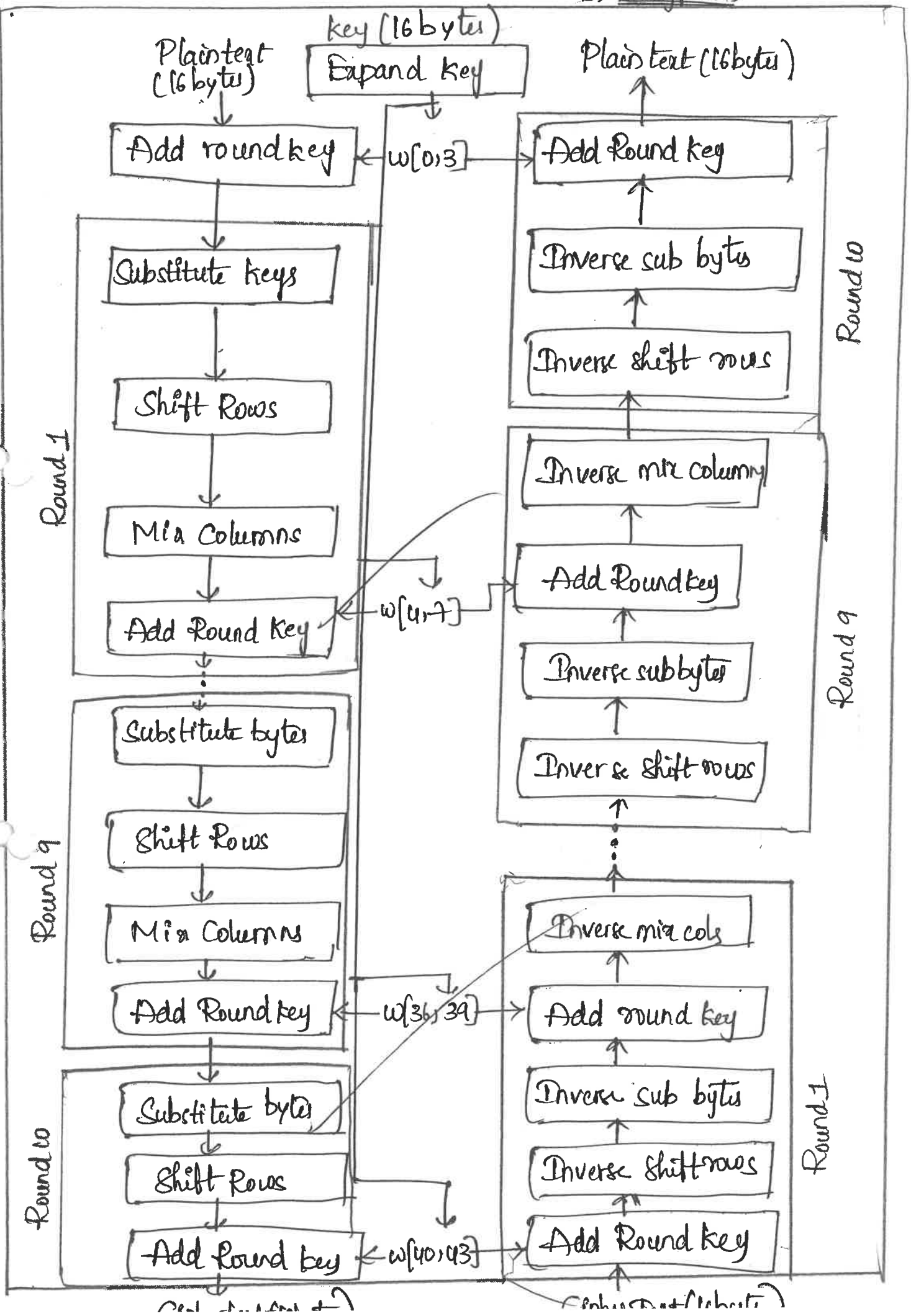
key size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block size	4/16/128	4/16/128	4/16/128
No. of Rounds	10	12	14
Round key size	4/16/128	4/16/128	4/16/128
Expanded key size	44/176	52/208	60/240

AES Encryption & Decryption Structure:-

- This structure doesn't follow Feistel Structure
- Data block size is 128 bits
- key size is 128 bits or 192 bits or 256 bits
- No. of rounds is 10, 12, 14

a) Encryption

b) Decryption

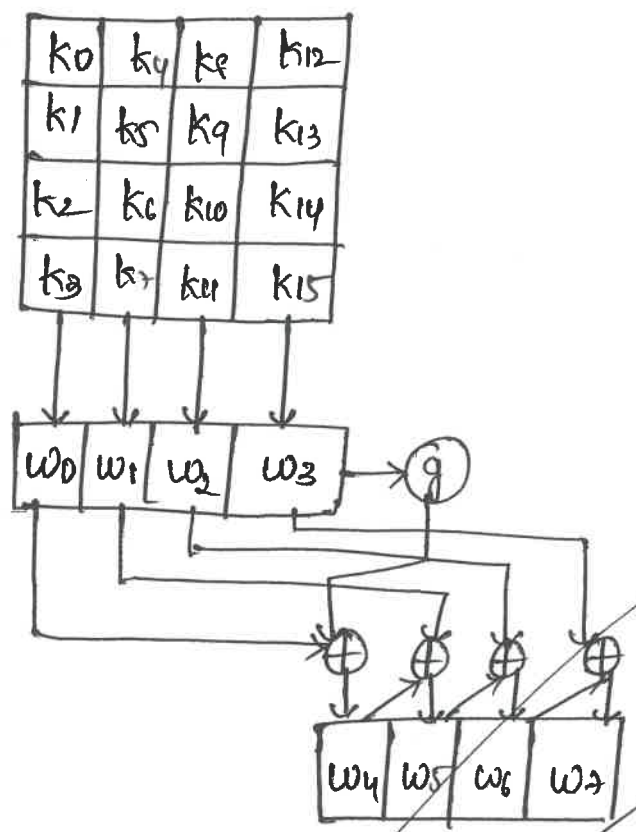



→ AES consists of four separate functions in each round.

- They are
 - i) Byte Substitution
 - ii) Permutation / Shifting of rows
 - iii) Mixing of columns
 - iv) XOR with a key / Add Round Key

AES key Expansion:

→ It will take 128 bit key and expands into array of 44/52/60 32 bit words.




 Principal
 A.M REDDY MEMORIAL COLLEGE OF
 ENGINEERING & TECHNOLOGY
 PETLURIVARI PALEM
 Narasaraopet (Mdl), Guntur(Dr)

UNIT – I

INTRODUCTION: SECURITY ATTACKS, SECURITY SERVICES & SYMMETRIC CIPHER MODEL, SUBSTITUTION TECHNIQUES, TRANSPOSITION TECHNIQUES, CYBER THREATS AND THEIR DEFENSE (PHISHING DEFENSIVE MEASURES, WEB BASED ATTACKS, SQL INJECTION & DEFENSE TECHNIQUES) (TEXT BOOK 2), BUFFER OVERFLOW & FORMAT STRING VULNERABILITIES, TCP SESSION HIJACKING (ARP ATTACKS, ROUTE TABLE MODIFICATION) , UDP HIJACKING (MAN-IN-MIDDLE ATTACKS) (TEXT BOOK 3)

WHAT IS MEANT BY SECURITY ATTACK? WHAT ARE VARIOUS TYPES OF SECURITY ATTACKS?

Security attack refers to a process whereby a person compromises the security of information. Security attacks can be divided into two types. They are,

Passive Attacks: Passive attacks are the attempts to make use of information from the system but they do not affect system resources. Passive attacks are very difficult to detect because they do not involve any alteration of data.

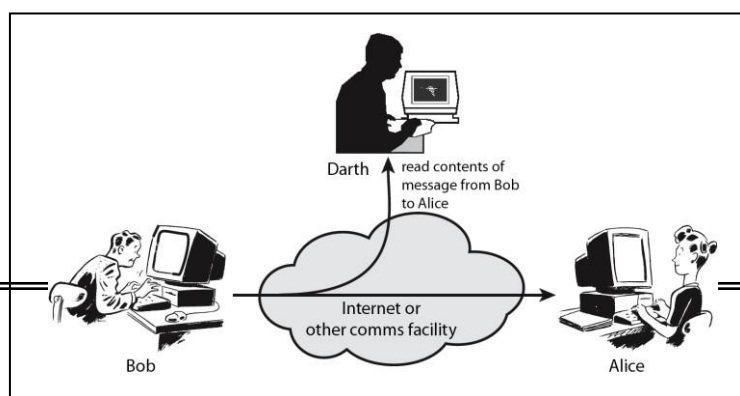
Types:

Release of Message Contents:

It means to obtain the message contents during transmit and they release the same to another persons.

Traffic Analysis:

Traffic analysis is done by the opponents, even if they captured the message, could not extract the information from the message. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.



Active Attack:

An active attack is an attack that alters system resources or affects their operation.

Types:

Masquerade:

In this one entity pretends as another entity.

Replay:

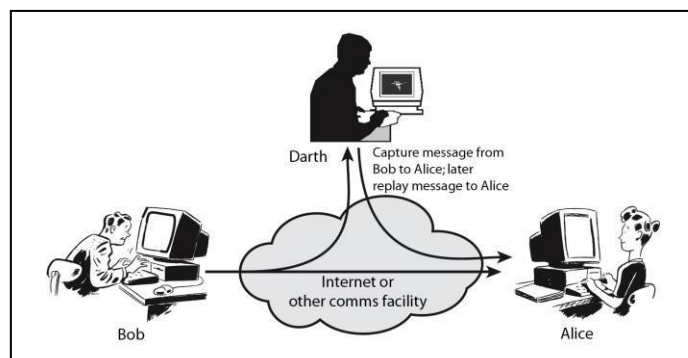
It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Modification of messages:

It means that some portion of a legitimate message is altered or that messages are delayed or recorded to produce an unauthorized effect.

Denial of service:

It prevents or inhibits the normal use or management of communication facilities. This attack may have a specific target.



WHAT IS MEANT BY SECURITY THREAT? WHAT ARE VARIOUS TYPES OF SECURITY THREATS?

A threat is a possible danger to breach security. A Threat may be either intentional or accidental.

Types:

1. Interruption:

An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on *availability*.

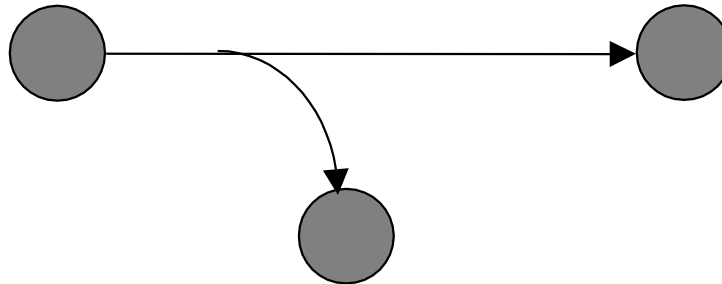
Ex: Destruction of a piece of hardware, cutting of communication line, etc.



2. Interception:

An unauthorized party gains access to an asset. This is an attack on *confidentiality*. An unauthorized party could be a person, a program or a computer.

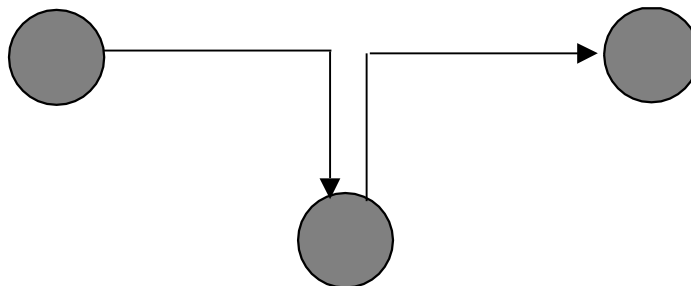
EX: Wiretapping to capture data in a network and illegal copying of files or programs.



3. Modification:

An unauthorized party not only gains access to but to tampers with an asset. This is an attack on *integrity*.

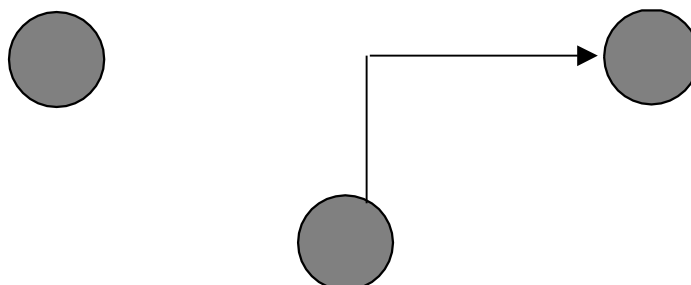
Ex: changing values in a data file, altering a program so that it performs differently, modifying the content of the messages while transmitted in a network.



4. Fabrication:

An unauthorized party inserts counterfeit objects into the system. This is an attack on *authenticity*.

Ex: Insertion of spurious messages in a network, addition of records to a file, etc.



WHAT IS MEANT BY SECURITY SERVICE? WHAT ARE VARIOUS TYPES OF SECURITY SERVICES?

A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

1. Authentication

The authentication service is concerned with assuring that a communication is authentic. Authentication Services:

- *Peer Entity Authentication:* It is used in association with a logical connection to provide confidentiality in the identity of the connected entities.
- *Data Origin Authentication:* In a connectionless transfer, provides assurance that the source of received data is as authentic. It does not provide protection against the duplication or modification of data units.

2. Access control

It means prevention of unauthorized use of a resource. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

3. Data confidentiality

Confidentiality is the protection of transmitted data from passive attacks. While transmitting the data several levels of protection may be needed.

4. Data integrity

It means the assurance that data received are exactly as sent by an authorized entity.

- **Connection integrity with recovery**
Provides for integrity of all user data on a connection and detects any modification, insertion, deletion or replay of any data within an entire data sequence, with recovery attempted.
- **Connection integrity without recovery**
Provides for integrity of all user data on a connection and detects any modification, insertion, deletion or replay of any data within an entire data sequence, without recovery attempted.
- **Selective field connection integrity**
Provides for the integrity of selected fields within the user data or a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted or replayed.

➤ Connectionless integrity

Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

➤ Selective field connection less integrity

Provides for the integrity or selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

5. **Nonrepudiation**

It provides protection against denial by one of the entities involved in a communication or part of the communication.

➤ Nonrepudiation, Origin

It is a proof that the message was sent by the specified party.

➤ Nonrepudiation, Destination

It is a proof that the message was received by the specified party.

6. **Availability**

It requires that computer system assets be available to authorized parties when needed.

WHAT IS MEANT BY SECURITY MECHANISM? WHAT ARE VARIOUS TYPES OF SECURITY MECHANISMS?

A mechanism that is designed to detect, prevent or recover from a security attack is called as security mechanism. The various types of security mechanisms are;

➤ Encipherment

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

➤ Digital Signature

Data appended to, or cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

➤ Access Control

A variety of mechanisms that enforce access rights to resources.

➤ Data Integrity

A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

7 Authentication Exchange

A mechanism intended to ensure the identity of an entity by means of information exchange.

7 Traffic Padding

The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

7 Routing Control

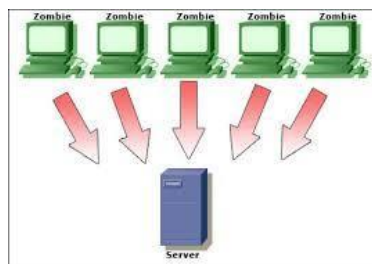
Enables selection of physically secured routes for certain data and allows routing changes, especially when a breach of security is suspected.

7 Notarization

It means the use of a trusted third party to assure certain properties of a data exchange.

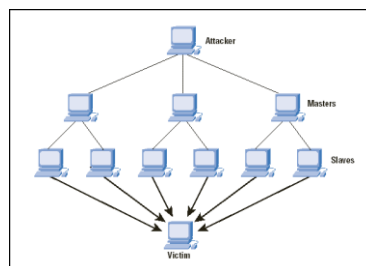
WRITE ABOUT DOS.

DOS stands Denial of Service Attack. It is an attack that denies the use of resources to the legitimate users. In this the attacker sends large number of requests is sent to the target. So many requests to the target may overload the target and cannot respond to the legitimate users.



WRITE ABOUT DDOS.

DDoS stands for Distributed Denial of Service. It is a type of DoS attack where multiple compromised systems are used to target a single system causing DoS attack. The compromised machines are called as zombie. A zombie is a computer that is connected to the Internet that has been compromised by the hacker, virus or Trojan horse and can be used to perform some malicious action or one sort or another under remote direction.



What are the basics of cryptography? Explain about symmetric cipher model with a neat diagram.

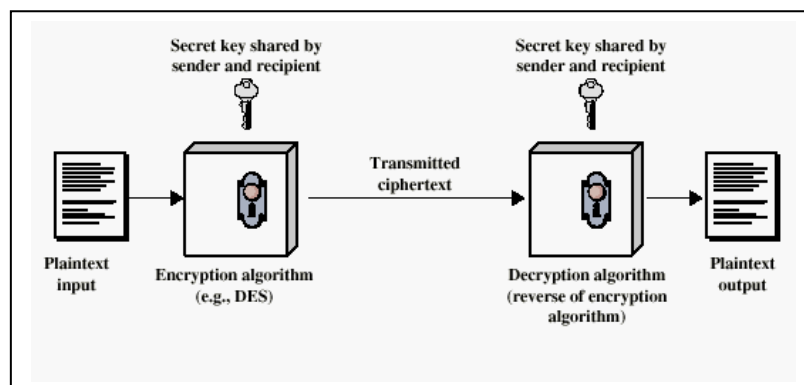
Conventional Encryption Principles: (Secret Key Cryptography)

It is also referred as symmetric encryption or single-key encryption. The original message is referred as plain text, is converted into some coded message is referred as cipher text. The encryption process consists of an algorithm and a key. The key is a value independent of the plain text. Changing the key changes the output of the algorithm. A conventional encryption scheme has five ingredients. They are;

- **Plain Text:** This is the original message or data that is fed into the algorithm as input.
- **Encryption Algorithm:** The encryption algorithm is used to transform the plain text into cipher text.
- **Secret Key:** The secret key is also input the encryption algorithm. The key value is independent of the plain text. The algorithm will produce different outputs for different keys used.
- **Cipher Text:** This is the scrambled message produced as output. It depends on the plain text and the secret key. For a given plaintext, two different keys will produce two different cipher texts.
- **Decryption Algorithm:** The encryption algorithm is used to transform the Cipher text into Plaintext text.

Requirements for secure use of conventional encryption:

- a. Strong encryption algorithm
- b. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.



The security of symmetric encryption depends on secrecy of the key not the secrecy of the algorithm.

Cryptographic systems are characterized along three independent dimensions.

1. **The type of operations used for transforming plain text to cipher text:** All encryption algorithms are based on two general principles;
 - a. Substitution: In this technique each element in the plain text is mapped into another element.
 - b. Transposition: In this technique each element in the plain text is rearranged.
2. **The number of keys used:** If both sender and receiver use the same key, the system is referred to as **symmetric, single-key, secret-key or conventional encryption**. If the sender and receiver uses a different key, the system referred to as **asymmetric, two-key or public key encryption**.
3. **The way in which the plain text is processed:** A ***block cipher*** processes the input one block of elements at a time, producing an output block for each input block. A ***stream cipher*** processes the input elements continuously, producing output one element at a time, as it goes along.

What are the basic building blocks of encryption techniques? Explain.

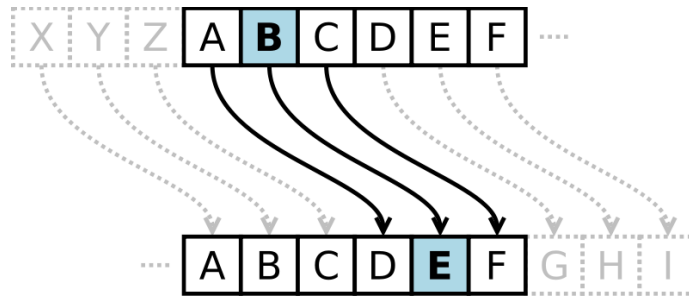
Write about substitution and transposition techniques with examples.

Write about various substitution encryption techniques.

In substitution technique the letters of plaintext are replaced with other letters or numbers or symbols. Some of substitution techniques are as follows;

1. Caesar Cipher

The Caesar cipher is named after [Julius Caesar](#), is used with a shift of three to protect messages of military significance. Caesar Cipher is also called as Shift Cipher. It is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plain text is replaced by a letter with some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on.



The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions. For instance, here is a Caesar cipher using a left rotation of three places (the shift parameter, here 3, is used as the [key](#)):

Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ
 Cipher : DEFGHIJKLMNOPQRSTUVWXYZABC

When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line. Deciphering is done in reverse.

Plaintext: the quick brown fox jumps over the lazy dog
 Ciphertext: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

2. Monoalphabetic Cipher

A Monoalphabetic cipher uses fixed substitution over the entire message. The ciphers in this substitution section replace each letter with another letter according to the cipher alphabet. Ciphers in which the cipher alphabet remains unchanged throughout the message are called Monoalphabetic substitution ciphers.

Ex:

Plain Text Alphabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ
 Cipher Text Alphabet : IWLZUQPEGKBXCYHRFVANTDOSJM

Ex: Plain Text : RAMA

Cipher Text : VICI

Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet. A countermeasure is to provide multiple substitutes, known as homophones for a single letter.

3. Playfair Cipher

The Playfair cipher or Playfair square is a manual symmetric encryption technique and was the first literal digraph substitution cipher. This scheme was invented in 1854 by

CRYPTOGRAPHY AND NETWORK SECURITY :: UNIT I

Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of cipher. The technique encrypts pairs of letters instead of single letters as in the simple substitution cipher and rather more complex vigenere cipher systems then in use.

The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword. To generate the key table we must follow the rules;

- First fill the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order. (generally "Q" is omitted)
- The key can be written in the top rows of the table from left to right or in some other pattern.
- The keyword together with the conventions for filling in the 5 x 5 table constitute the cipher key.

Ex: Keyword : playfair example

Table:

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
J	K	N	O	S
T	U	V	W	Z

Plain Text : HIDE THE GOLD IN THE TREE STUMP

HI DE TH EG OL DI IT HE TR EX ES TU MP

- The pair HI forms a rectangle, replace it with BM
- The pair DE is in a column, replace it with ND
- The pair TH forms a rectangle, replace it with ZB
- The pair EG forms a rectangle, replace it with XD
- The pair OL forms a rectangle, replace it with KY
- The pair DI forms a rectangle, replace it with BE
- The pair IT forms a rectangle, replace it with JV
- The pair HE forms a rectangle, replace it with DM
- The pair TR forms a rectangle, replace it with UI
- The pair EX (X is inserted to split EE) in a row, replace it with XM
- The pair ES forms a rectangle, replace it with MN
- The pair TU is in a row, replace it with UV
- The pair MP forms a rectangle, replace it with IF

Cipher Text:

BM ND ZB XD KY BE JV DM UI XM MN UV IF

4. Polyalphabetic Cipher

A Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The vigenere cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

For example, if the keyword is *deceptive*, the message is "we are discovered save yourself" is encrypted as follows;

Key : deceptivedeceptivedeceptive
 Plain Text : wearediscoveredsaveyourself
 Cipher Text : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

1. Given plain text 'w' and key 'd' : see in vigenere Table 'w' row and 'd' column : Z
2. Given plain text 'e' and key 'e' : see in vigenere Table 'e' row and 'e' column : a

Decryption: The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plain text letter is at the top of that column.

Key : deceptivedeceptivedeceptive

Cipher Text : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Plain Text : wearediscoveredsaveyourself

1. Given cipher text 'Z' and key 'd' : see in vigenere Table 'd' row and 'z' letter : w (column)
2. Given cipher text 'a' and key 'e' : see in vigenere Table 'I' row and 'e' letter : e (column)

A vigenere cipher is suspected, then progress depends on determining the length of the keyword length can be determined. If the keyword length is N, then the cipher in effect, consists of N Monoalphabetic substitution ciphers. For example, with the keyword DECEPTIVE, the letters in positions 1, 10, 19 and so on are all encrypted with the same Monoalphabetic cipher. Thus, we can use the known frequency characteristics of the plain text language to attack each of the Monoalphabetic ciphers separately.

The periodic nature of the keyword can be eliminated by using a nonrepeating keyword that is as long as the message itself. Vigenere proposed what is referred to as an auto key system, in which a keyword is concatenated with the plain text itself to provide a running key.

Ex:

Key : deceptivewarediscoveredsav

Plain Text : wearediscoveredsaveyourself

Cipher Text : ZICVTWQNGKZEIIGASXSTSLVWLA

$$C_i = P_i \text{ XOR } K_i$$

Where,

P_i = ith binary digit of plain text

K_i = ith binary digit of key

C_i = ith binary digit of cipher text

Thus, the cipher text is generated by performing the bitwise XOR of the plain text and the key. Because of the properties of the XOR, decryption simply involves the same bitwise operation.

$$P_i = C_i \text{ XOR } K_i$$

5. One-time Pad

In cryptography, the one time pad is an encryption algorithm in which the plain text is combined with a secret random key or pad as long as the plain text and used only once.

The Vernam one-time pad was recognized early on as difficult to break.

Drawbacks:

- ⑦ It requires perfectly random one-time pads
- ⑦ Secure generation and exchange of the one-time pad material, which must be as long as the message
- ⑦ Careful treatment to make sure that it continues to remain secret from any adversary and is disposed of correctly preventing any reuse in whole or part hence "one time"
- ⑦ The one-time pad does not provide a mechanism to ensure message integrity

Ex:

KEY : XMCKL

Plain Text : HELLO

Encryption :

7 (H) 4 (E) 11 (L) 11 (L) 14 (O) message
 + 23 (X) 12 (M) 2 (C) 10 (K) 11 (L) key
 = 30 16 13 21 25 message + key
 = 4 (E) 16 (Q) 13 (N) 21 (V) 25 (Z) message + key (mod 26)
 >> ciphertext

Similar to the above, if a number is negative then 26 is added to make the number positive.

Write about various transposition encryption techniques.

In this cipher text is obtained by performing some sort of permutation on the plain text letters.

1. **The Rail Fence (Row Transposition Technique)** cipher is a form of transposition cipher that gets its name from the way in which it is encoded. In the rail fence cipher, the plain text is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom. The message is then read off in rows.

Ex: WE ARE DISCOVERED FLEE AT ONCE

W . . . E . . . C . . . R . . . L . . . T . . . E
 . E . R . D . S . O . E . E . F . E . A . O . C .
 . . A . . . I . . . V . . . D . . . E . . . N . .

Cipher Text : WECRL TEERD SOEEF EAOCA IVDEN

2. In a **Route Cipher**, the plain text is first written out in a grid of given dimensions, then read off in a pattern, given in the key

W	R	I	O	R	F	E	O	E
E	E	S	V	E	L	A	N	J
A	D	C	E	D	E	T	C	X

Cipher Text: WRIORFEOEEESVELANJADCEDETCX

3. In a **Columnar Transposition**, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a key word. For example the word ZEBRAS is of length 6 and the permutation is defined by the alphabetic order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

Plain Text : WE ARE DISCOVERED FLEE AT ONE

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E					

Cipher Text: EVLN ACDT ESEA ROFO DEEC WIREE

To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length. Then he can write the message out in columns again, and then re-order the columns by reforming the key word.

4. In **Double Transposition** was often used to make columnar transposition make it stronger. This is simply a columnar transposition applied twice. The same key can be used for both transpositions or two different keys may be used.

As an example, we can take the result of the irregular columnar transposition in the previous section, and perform a second encryption with a different keyword, STRIPE, which gives the permutation "564231":

5	6	4	2	3	1
E	V	L	N	A	C
D	T	E	S	E	A
R	O	F	O	D	E
E	C	W	I	R	E
E					

As before, this is read off column wise to get the cipher text:

Cipher Text: CAEEN SOIAE DRLEF WEDRE EVTOC

5. In ***Myszkowski Transposition*** requires a keyword with recurrent letters. In usual practice, subsequent occurrences of a keyword letter are treated as if the next letter in alphabetical order.

Ex: TOMOTA yields key string of "532164"

In Myszkowski transposition, recurrent keyword letters are numbered identically. TOMOTO yielding a key string of "432143".

```

4 3 2 1 4 3
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E
    
```

Plaintext columns with unique numbers are transcribed downward; those with recurring numbers are transcribed left to right:

Cipher Text: ROFOA CDTED SEEEA CWEIV RLENE

6. In ***Disrupted Transposition***, certain positions in a grid are blanked out, and not used when filling in the plain text. This breaks up regular patterns and makes the cryptanalyst's job more difficult.

WHAT IS MEANY BY CYTER THREATS? WHAT ARE ITS TYPES?

Cyber threat is an attack on digital systems originating malicious act of an anonymous source. Cyber attack allows illegal access to the digital system, while gaining access of the digital system.

Types:

Backdoor:

A backdoor is also known as trapdoor. It is a secret entry point into a program that allows someone to gain access without going through the usual security access procedures.

Denial of Service Attack:

Dos stand Denial of Service Attack. It is an attack that denies the use of resources to the legitimate users. In this the attacker sends large number of requests is sent to the target. So

many requests to the target may overload the target and cannot respond to the legitimate users.

Distributed Denial of Service:

DDoS stands for Distributed Denial of Service. It is a type of DoS attack where multiple compromised systems are used to target a single system causing DoS attack. The compromised machines are called as zombie.

Direct access Attack:

A direct access attack means gaining physical access to the computer and performing various functions or installing various types of devices to compromise security. The attacker can install software loaded with worms or download important data using portable devices.

Logic Bomb:

A logic bomb is a piece of code intentionally inserted into a software system which will perform a malicious function when specified conditions are met.

Trojan Horses

A Trojan horse seems to be useful program or command procedure which contains hidden code that, when invoked, performs some unwanted or harmful function. The common motivation for the Trojan horse is data destruction.

Tampering:

Tampering is a web based attack where certain parameters in the URL are changed without the customer's knowledge. Tampering is basically done by hackers to steal the identity and obtain illegal access to information.

Information Disclosure:

Information disclosure breach means that the information which is thought to be secured is released.

Mobile Code

Mobile code is software, which is transformed between systems and executed on a local system without explicit installation by the recipient. Mobile code is transmitted from a remote system to a local system and then executed on the local system without the user's explicit instruction.

Eavesdropping:

It means secretly listening to a conversation between the hosts on a network.

Spoofing:

Spoofing is a cyber attack where a person or a program impersonates as another by creating false data in order to gain illegal access to a system.

Virus:

A computer virus is a computer program that can replicate itself and spread from one computer to another. Computer viruses first appeared in the early 1980s, and the term itself is attributed to Fred Cohen in 1983.

Multiple-Threat Malware:

It is capable of infection multiple types of files. A blended attack uses multiple methods of infection or transmission to maximize the speed of infection and the severity of the attack.

DEFINE PHISHING. EXPLAIN ABOUT VARIOUS DEFENSIVE MEASURES FOR PHISHING.

Phishing is an act of acquiring sensitive information, such as usernames, passwords, credit card numbers, and SSNs, by masquerading as a trustworthy entity in an electronic communication. Phishing technique was described in the year of 1987.

Types:

SPEAR PHISHING: A spear phisher sends a message that appears to be from an employer, a colleague or other legitimate correspondent. This attack targets a certain product or a website.

CLONE PHISHING: This technique could be used indirectly from a previously infected machine and gain a foothold on another machine.

WHALING: These attacks have been directed specifically at senior executive and other high profile targets within the business.

Defensive Measures:

1. Safe browsing tool

Since the web is the most frequently used attack vector, it is important to have protection for browsers, especially when a search is used.

2. Uniform resource locator (URL) filtering

Internet Explorer (IE), Chrome, and Firefox provides phishing filters. Phishing and malware protection is accomplished by checking the site that is being visited against lists of reported phishing and malware sites. These lists are automatically downloaded and updated by browsers. Whenever the Phishing and Malware Protection features are enabled, browsers can provide warnings.

3. The obfuscated URL and the redirection technique

Two of the most common techniques employed in phishing are the confusing/obfuscated URL and the redirection technique

EXPLAIN ABOUT WEB-BASED ATTACKS:

The vulnerabilities in web-based attacks are manifested in a variety of ways. For example, the inadequate validation of user input may occur in one of the following attacks: Cross-Site Scripting (XSS or CSS) [27], HTTP Response Splitting or SQL Injection and so on.

1. Web Service Protection:

Web services based on the eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), and related open standards that are deployed in Service Oriented Architectures (SOAs) allow data and applications to interact without human intervention through dynamic and ad hoc connections.

2. Attack Kits:

Unfortunately, there are a number of attack kits that although illegal, can be purchased on the Black market. Some of them are;

- Botnet
- Autodoor
- SQL injection tools
- Shopadmin Exploiter
- RFI Scanner
- LFI Scanner
- XSS Scanner

3. Http Response Splitting Attacks:

HTTP response splitting attacks may happen where the server script embeds user data in HTTP response headers without appropriate sanitation. This typically happens when the script embeds user data in the redirection URL of a redirection response.

4. Cross-Site Request Forgery (CSRF OR XSRF):

A Cross-Site Request Forgery attack [28] tricks the victim's browser into issuing a command to a vulnerable web application. Vulnerability is caused by browsers automatically including user authentication data, session ID, IP address, Windows domain credentials, etc. with each request. For example, a single browser runs two scripts simultaneously: a script from a high-value site and a malicious script from a malicious/contaminated site.

5. Cross-Site Scripting (XSS) Attacks:

Cross-site scripting (XSS) is not a new vulnerability for AJAX. It is common, especially if an application allows state data to be manipulated with JavaScript. In such situations, the attacker is able to execute some code on the user's machine. Thus, the attacker inserts malicious JavaScript into a Web page or HTML email, and when the script is executed, it steals the user's information and forwards it to attacker's site.

6. Non-Persistent Xss Attacks:

A non-persistent XSS attack is also known as a reflected XSS vulnerability because the vulnerable server need not store a malicious script and the server is simply echoing back the input fields sent by the user's browser.

7. Persistent XSS Attacks:

A website may store malicious script if it is compromised by other attacks such as SQL injection.

8. Document Object Model (DOM) XSS Attacks:

The Document Object Model (DOM) XSS first published by Amit Kleinand. An application HTML page containing JavaScript code parses the URI line, by accessing either document.URL or document.location, and performs some client side script execution accordingly in its normal mode.

EXPLAIN ABOUT SQL INJECTION AND THEIR DEFENSE TECHNIQUES.

SQL injection is also known as SQLI, is a common attack that uses malicious SQL code for backend database manipulation to access the information that was not intended to be displayed. The successful attack may result in the unauthorized views of data relates to an organization.

Ex:

Select itemname from item where itemnumber = 999;

It will displays the itemname for itemnumber 999.

An attacker wishing to execute SQL injection manipulates a standard SQL query to exploit non-validated input vulnerabilities in a database. For example the attacker wishes to see the all the item details then the query is modified as follows;

Select itemname from item where itemnumber = 999 or 1=1;

Since the statement 1=1 is always true, the query returns all the product names, even those may not be eligible to access.

Defensive Measures:

- (a) Input validation using analysis tools like Microsoft SQL Source Code Analysis Tool
- (b) Web application firewall
- (b) Scan the URL using e.g., Microsoft UrlScan,
- (c) Scan the whole site using e.g., HP Scrawlr, and
- (d) Sanitize user input forms through secure programming.

EXPLAIN ABOUT BUFFER OVERFLOW.

A Buffer is a temporary storage area for data. When more data gets placed by a program or system process, the extra data overflows. It causes some of that data to leak out into other buffers, which can corrupt or overwrite whatever data they were holding.

In a **buffer-overflow attack**, the hacker tries to place extra data which may damages files, changes data or unveils private information.

Attacker would use a buffer-overflow exploit to take advantage of a program that is waiting on a user's input. There are two types of buffer overflows:

- Stack-based: Stack-based buffer overflows, which are more common among attackers, exploit applications and programs by using what is known as a stack. memory space used to store user input
- Heap-based: Heap-based, which are difficult to execute and is an attack on application by flooding the memory space reserved for a program.

Basic example:

```
# include <stdio.h>
int main(int argc, char *argv[])
{
    char buff[4];
    printf("\n Some Input:");
    gets(buff);
    puts(buff);
}
```

Output:

Some Input: ABC

ABC

If the user inputs more than 3 characters, will generate an error and the program terminates.

EXPLAIN ABOUT FORMAT STRING VULNERABILITIES.

A format string is an ASCII string that contains text and format parameters. Format string vulnerability attacks are divided into three categories.

Denial of service: Format strings require valid memory addresses as corresponding variables. For example %s requires a pointer to a NULL terminated string. If an attacker supplies a malicious format string and no valid memory address exists where the corresponding variable is expected. In such case the process will fail. This may cause a denial of service.

Reading attacks: Reading attacks are a serious problem and can lead to disclosure of sensitive information. For example, if a program accepts authentication information from clients and does not clear it immediately after use, format string vulnerabilities can be used to read it.

Writing attacks: The existence of such a format specifier has serious security implications: it can allow for writes to memory. This is the key to exploiting format string vulnerabilities to accomplish goals such as executing shell code.

EXPLAIN ABOUT TCP SESSION HIJACKING, ARP ATTACKS AND ROUTE TABLE MODIFICATION.

TCP SESSION HIJACKING:

- TCP session hijacking occurs when a hacker takes over a TCP session between two machines. Since most authentications only occur at the start of a TCP session, this allows the hacker to gain access to a machine.
- A popular method is using source-routed ip packets. This allows a hacker at point a on the network to participate in a conversation between b and c by encouraging the ip packets to pass through its machine.
- A hacker can also be "inline" between b and c using a sniffing program to watch the conversation. This is known as a "man-in-the-middle attack".
- A common component of such an attack is to execute a denial-of-service attack against one end-point to stop it from responding. This attack can be either against the machine to force it to crash, or against the network connection to force heavy packet loss.
- TCP session hijacking is a much more complex and difficult attack. The purpose of the attack is not to deny service, but to pretend to be an authorized user in order to gain access to a system.

ARP ATTACKS:

- ARP(address resolution protocol) spoofing, also known as ARP poisoning, is a technique used to attack an Ethernet network which may allow an attacker to sniff data frames on a switched local area network (LAN) or stop the traffic altogether.
- The principle of ARP spoofing is to send fake, or 'spoofed', ARP messages to an Ethernet LAN. These frames contain false MAC addresses, confusing network devices, such as network switches. As a result frames intended for one machine can be mistakenly sent to another or an unreachable host.
- ARP spoofing can also be used in a man-in-the-middle attack in which all traffic is forwarded through a host with the use of ARP spoofing and analyzed for passwords and other information.

ROUTE TABLE MODIFICATION:

Routers use routing tables to send packets in the network. The router moves the packets by looking into the routing table. The routing table is formed by exchanging routing information between routers. Route table modification means the unwanted change in the routing table of the router. This attack can cause severe damage in the network by entering wrong routing table entries in the routing table.

EXPLAIN ABOUT UDP SESSION HIJACKING AND MAN-IN-MIDDLE ATTACKS.

- Hijacking a session over a UDP is exactly the same as over TCP, except that UDP attackers do not have to worry about the overhead of managing sequence numbers and other TCP mechanisms.
- Since UDP is connectionless, injecting data into a session without being detected is extremely easy.

Methods to prevent session hijacking:

- ➔ Session key will be a long random number or string
- ➔ Session ID should be regenerated after a successful login
- ➔ Change the value of the cookie with each and every request
- ➔ Users should logout of websites after finished using them

MAN-IN-MIDDLE-ATTACK:

A Man-in-the-Middle Attack is a type of cyber attack where a malicious actor (attacker) inserts himself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allow a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM OR MIM.

IMPORTANT QUESTIONS

1. WHAT IS MEANT BY SECURITY ATTACK? WHAT ARE VARIOUS TYPES OF SECURITY ATTACKS?
2. WRITE ABOUT SECURITY MECHANISMS.
3. EXPLAIN ABOUT SECURITY SERVICES.
4. EXPLAIN ABOUT NETWORK SECURITY MODEL WITH A NEAT DIAGRAM.
5. WHAT ARE THE BASICS OF CRYPTOGRAPHY? EXPLAIN ABOUT SYMMETRIC CIPHER MODEL WITH A NEAT DIAGRAM.
6. WHAT ARE THE BASIC BUILDING BLOCKS OF ENCRYPTION TECHNIQUES? EXPLAIN.
7. WHAT ARE THE PRINCIPLES OF BLOCK CIPHER.

UNIT –II

Block Ciphers & Symmetric Key Cryptography:

Objectives: The Objectives of this unit is to understand the difference between stream ciphers & block ciphers, present an overview of the Feistel Cipher and explain the encryption and decryption, present an overview of DES, Triple DES, Blowfish, IDEA.

Traditional Block Cipher Structure, DES, Block Cipher Design Principles, AES-Structure, Transformation functions, Key Expansion, Blowfish, CAST-128, IDEA, Block Cipher Modes of Operations

WRITE ABOUT SECRET KEY CRYPTOGRAPHY.

It is also called as private key encryption or symmetric encryption. In this same key is used for both encryption and decryption. Encryption involves applying an algorithm to the data to be encrypted using the private key to make them unintelligible.

The main disadvantage of secret key algorithm is exchange of keys. This encryption is based on the exchange of the secret keys.

EXPLAIN ABOUT BLOCK CIPHER DESIGN PRINCIPLES.

Block ciphers treat a block of plaintext as a whole. In general a block size is 64 or 128 bits. These are more popular than stream ciphers and mostly based on Feistel cipher structure.

Block Cipher: A block cipher is a method of encrypting text in which a cryptographic key and algorithm are applied to a block of data at one rather than to one bit at a time. In general a block size may be 64 or 128 bits.

Ex: DES, AES, IDEA, BlowFish,

Stream Cipher: A stream cipher is a method of encrypting text in which cryptographic key and algorithm are applied to each binary digits in a data stream, one bit at a time. This method is not much used in modern cryptography.

Ex: Onetime pad, autokeyed Vigenere, Vernam cipher

Feistel Cipher Structure:

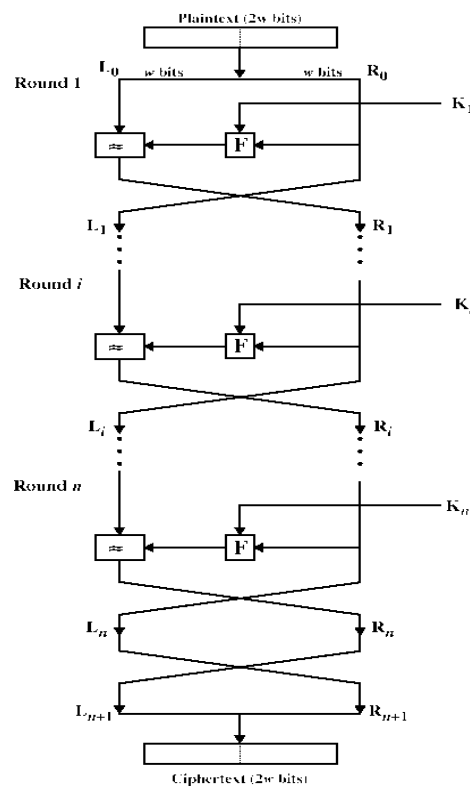
In cryptography, a Feistel cipher is a symmetric structure used in the construction of block ciphers named after the German born physicist and cryptographer Horst Feistel. A large proportion of block ciphers uses the scheme, including the DES. The Feistel structure has the

advantage that encryption and decryption operations are very similar even identical in some cases, requiring only a reversal of the key schedule.

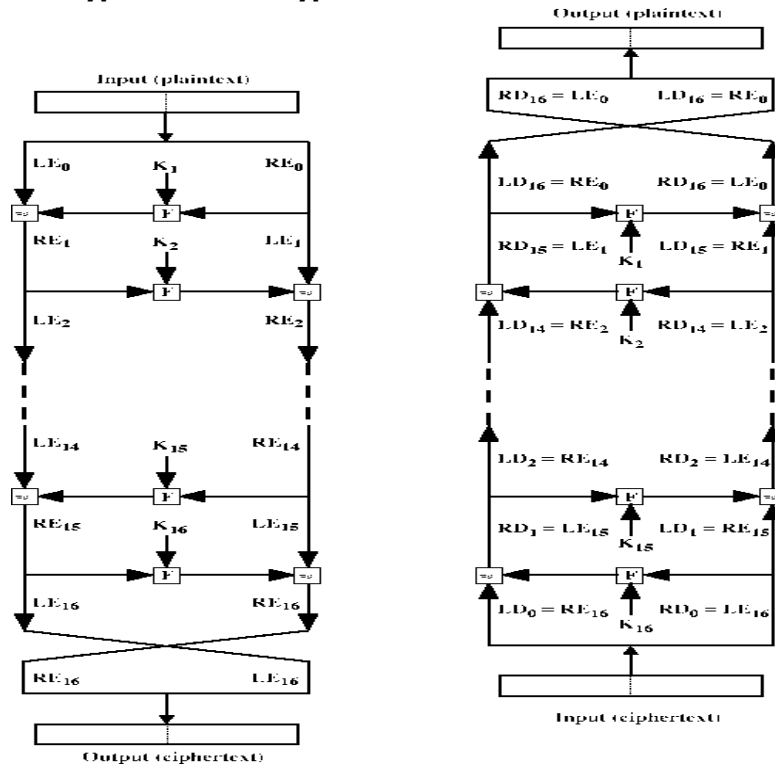
Design Features:

- **Block size:** Larger block size means greater security, but it reduces encryption/decryption speed. The reasonable block size is 64 bits.
- **Key size:** Larger key size means greater security but it may decrease encryption/decryption speed. The common key size is 128 bits.
- **Number of rounds:** A typical size is 16 rounds.
- **Subkey generation algorithm:** Is used to generate the subkey.
- **Round function:** Greater complexity of round function having greater resistance to cryptanalysis. It is the process of encryption and decryption in each round.

Fiestel Cipher Structure:



Fiestel Cipher Encryption and Decryption:



Construction Details:

F - RoundFunction

K_0, K_1, \dots, K_n - Subkeys for the rounds $0, 1, \dots, n$

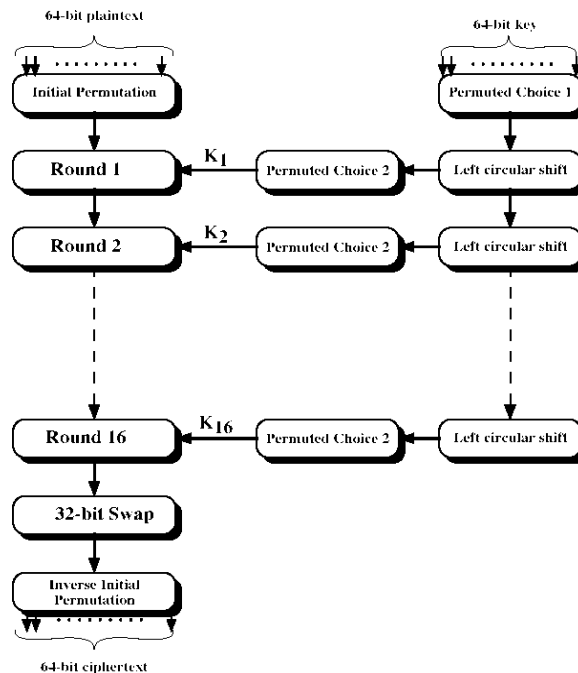
Basic Operations: All rounds have the same structure.

- The plain text is split into to equal size blocks (L_0, R_0).
- A substitution is performed on the left half of the data by applying a round function F to the right half of the data and then taking the XOR of the output of that function and the left half of the data.
- After final round, a permutation is performed that consists of the interchange of **te** two halves of the data.

Explain about DES. (Data Encryption Standard)

The **Data Encryption Standard (DES)** is a block cipher that was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976. It is based on a symmetric-key algorithm that uses a 56-bit key. It takes a fixed length string of plain text bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In case of DES the block size is 64 bits.

Structure:



Left Side:

First the plain text passes through initial permutation (IP) which rearranges the bits and produces the permuted output. Then it is followed by a phase consisting of 16 rounds of the same function, which involves both permutation and substitution. The output of the last round consists of 64 bits. After 6 rounds the left and right halves of the output are swapped to produce the preoutput. Finally the preoutput is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation to produce the 64-bit cipher text.

Right Side:

It shows the subkey generation process. Initially the key is passed through a permutation function. The permutation function is same for all the 16 rounds, but it produces different subkeys because of the repeated shifts of the key bits.

Details of Single Round:

Left Side Diagram:

The left and right halves of each 64-bit intermediate values are treated as separate 32-bit quantities labeled as L (left) and R (right).

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \text{ xor } F(R_{i-1}, K_i)$$

The round key K_i is 48 bits. The R input is 32 bits.

- This R input is first expanded to 48 bits using a table that defines a permutation plus an expansion that involves a duplication of 16 of the R bits.
- The resulting 48 bits are XORed with K_i .
- These 48 bits pass through a substitution function that produces 32 bit output.
- The role of S-boxes consists of a set of 8 S-boxes, each of which accepts 6-bits as input and produces 4 – bits as output.
- These 32 bits pass through permutation box and the result is XORed with the leftmost

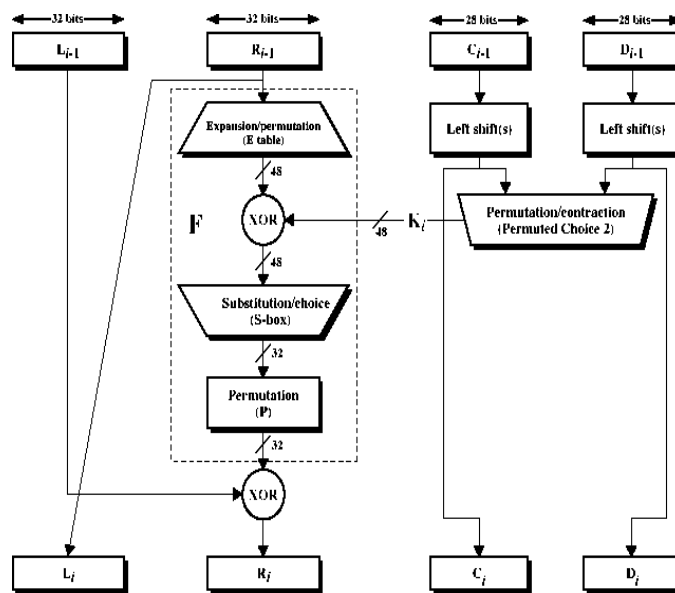


Figure 3.8 Single Round of DES Algorithm

bits of the corresponding round.

Key Generation:

- 56-bit key is used as input to the algorithm is first subjected to a permutation governed by initial permuted choice one.
- The resulting 56-bit key is then treated as two 28-bit quantities labeled as C_0 and D_0 .
- At each round C_{i-1} and D_{i-1} are subjected to a circular left shift or rotation of 1 or 2 bits as governed by the DES Key schedule calculation.
- These shifted values serve as input to the next round.

- Apply Permuted Choice 2 to produce 48-bit output that serves the input to the function.

Table 3.2 Permutation Tables for DES

(a) Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP⁻¹)

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

(c) Expansion Permutation (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(d) Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

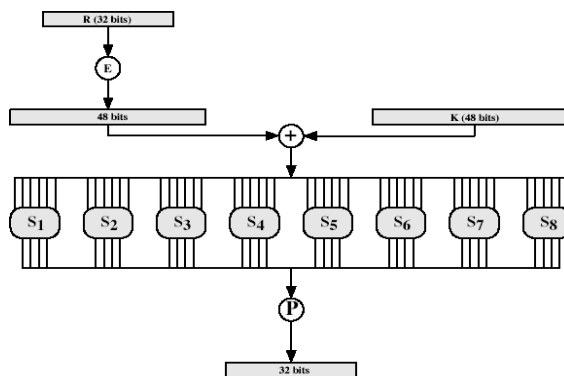


Figure 3.9 Calculation of F(R, K)

Table 3.3 Definition of DES S-Boxes

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Table 3.4 DES Key Schedule Calculation

(a) Input Key

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(b) Permuted Choice One (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

(c) Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

(d) Schedule of Left Shifts

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

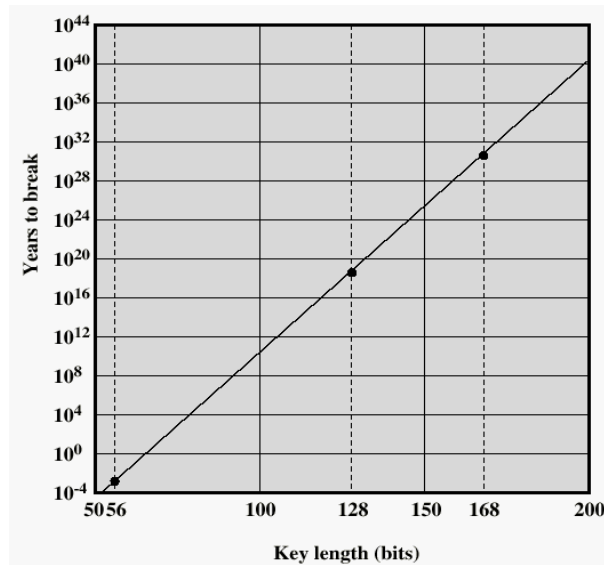
What is the strength of DES?

1. The use of 56-bit keys:

- 56-bit keys have $2^{56} = 7.2 \times 10^{16}$ values
- Brute force search looks hard
- In 1999 Plain text is achieved in 22 hours.
- Still must be able to recognize plaintext
- Now considering alternatives to DES.

2. The nature of the DES algorithm: DES algorithm focuses on the eight substitution boxes that are used in each iteration. The design criteria for these boxes are indeed for the entire algorithm were not made public, there is a suspicion that the boxes were constructed in such a way that cryptanalysis is possible for an opponent who knows the weaknesses in the S-boxes.

3. Timing Attacks: A timing attack is an example of an attack that exploits the implementation of an algorithm rather than the algorithm itself.



EXPLAIN ABOUT AES-STRUCTURE.

AES is a symmetric block cipher intended to replace DES for commercial applications. It uses 128 bit block size and a key size of 128, 192 or 256 bits. AES was published by National Institute of Standards and Technology (NIST) in 2001.

Evolution Criteria:

- **Security:** It refers the effort that is required to cryptanalyze the algorithm. Because of the key size for AES is 128 bits, brute-force attacks with current and projected technology was impractical.
- **Efficiency:** The intension of NIST is to design AES is to be practical in a wide range of applications and must have high computational efficiency.
- **Algorithm and Implementation Characteristics:** It includes the flexibility, suitability for various hardware and software implementations, simplicity and security. The following criteria is used for final evaluation.
 - **General Security:** Compared to DES, the amount of time and the number of cryptographers devoted to analysis are quite limited. So AES provides more security than the DES.
 - **Software Implementations:** The concern is execution speed, performance across a variety of platforms and variation of speed with key size.

- **Restricted Space Environments:** Representation of S-boxes will be stored in RAM or ROM and subkey storage in RAM is required.
- **Hardware Implementations:** Like software, hardware implementations can be optimized for size and speed. In the case of hardware size translates directly into cost that is usually in the case for software implementations.
- **Attacks on Implementations:** It deals with the various types of attacks that exploit the mathematical properties of the algorithms.
- **Encryption versus Decryption:** It deals with the issues related to the considerations of both encryption and decryption.
- **Key agility:** It refers to change of the keys quickly with a minimum of resources.
- **Other Versatility and Flexibility:** It refers to the possibility of optimizing cipher elements.
- **Potential for Instruction Level Parallelism:** It refers to the ability of ILP feature implementations in current and future processors.

AES Cipher:

AES is having following parameters.

Table 5.1 AES Parameters

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

AES Encryption and Decryption Structure:

1. This structure does not follow the Feistel Structure.
2. Data block size is 128 bits.
3. Key size is 128 bits or 192 bits or 256 bits.
4. Number of rounds is 10, 12 or 14.

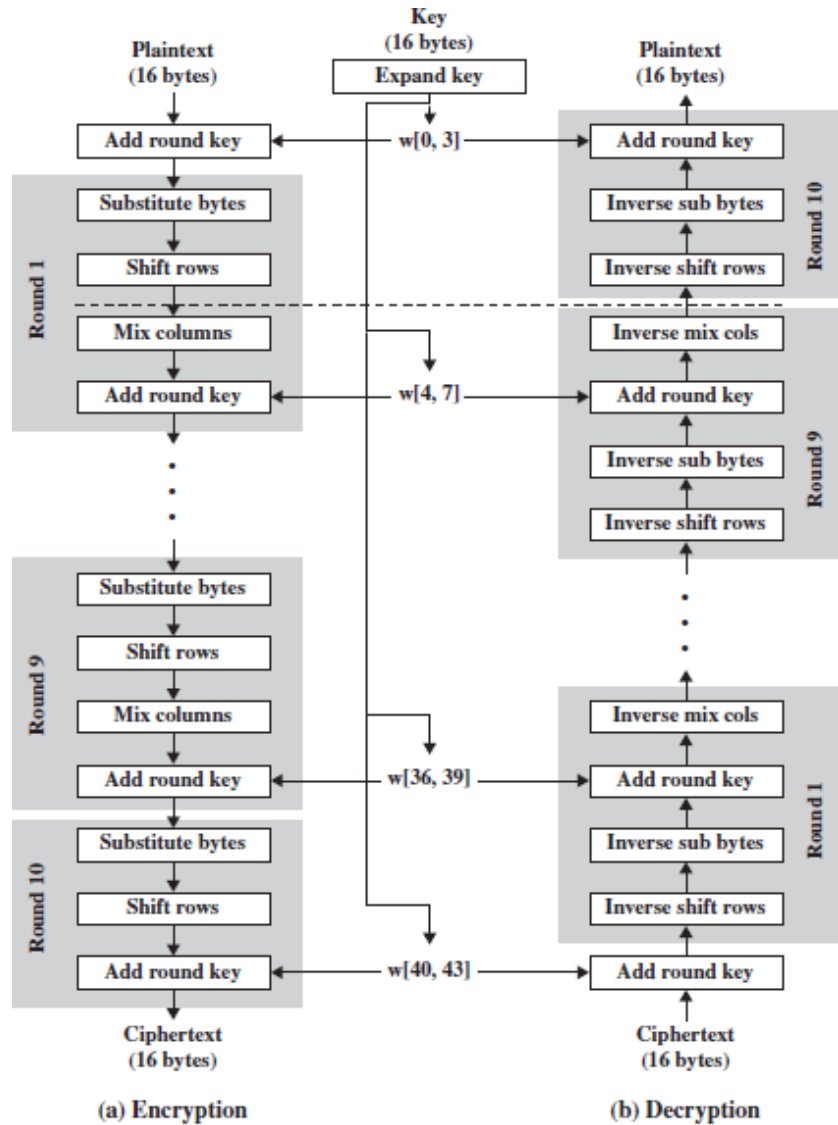


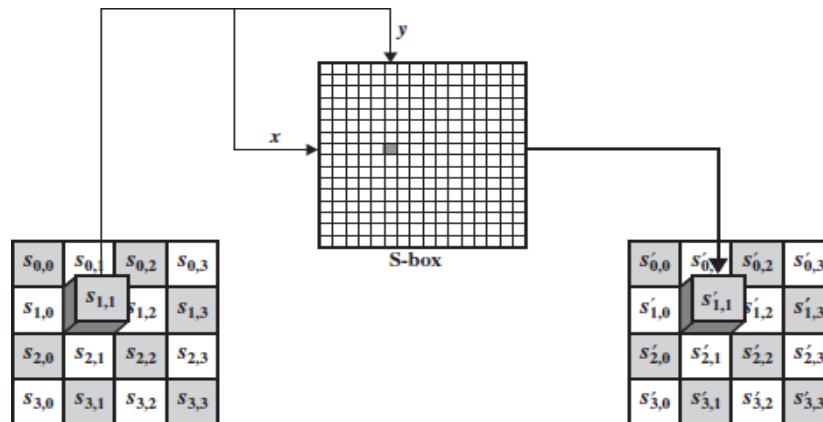
Figure 5.3 AES Encryption and Decryption

AES consists of four separate functions in each round. They are;

- ➔ Byte Substitution
- ➔ Permutation / shifting of rows
- ➔ Mixing of columns
- ➔ XOR with a key / Add round key

Byte Substitution:

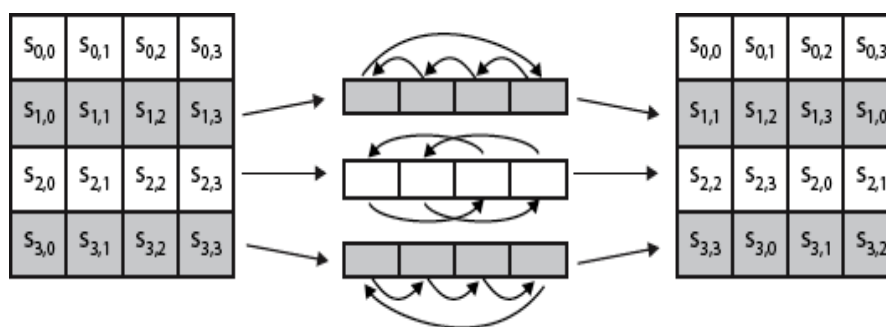
By using S-boxes byte-by-byte substitution is done. AES defines a 16×16 matrix of byte values, called an S-box that contains a permutation of all possible 256 8-bit values.



Permutation/Shifting of rows:

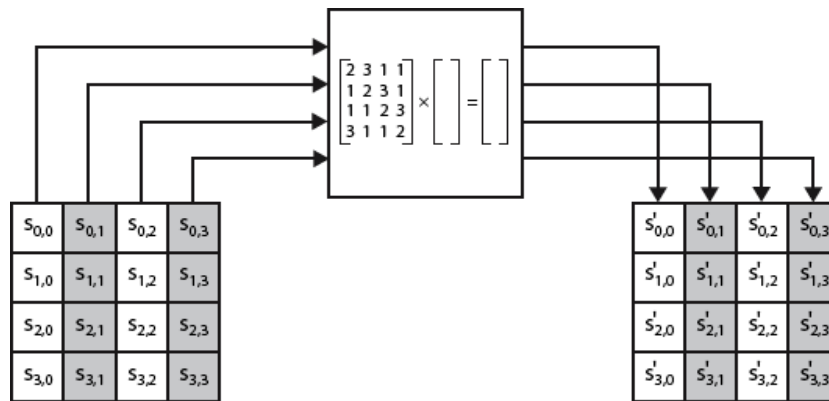
In permutation shifting rows will be performed. In encryption the transformation is called as shiftrows. In decryption the transformation is called as Invshiftwors and the shifting is to the right.

- A circular byte shift in each each
 - 1st row is unchanged
 - 2nd row does 1 byte circular shift to left
 - 3rd row does 2 byte circular shift to left
 - 4th row does 3 byte circular shift to left
- Decrypt inverts using shifts to right



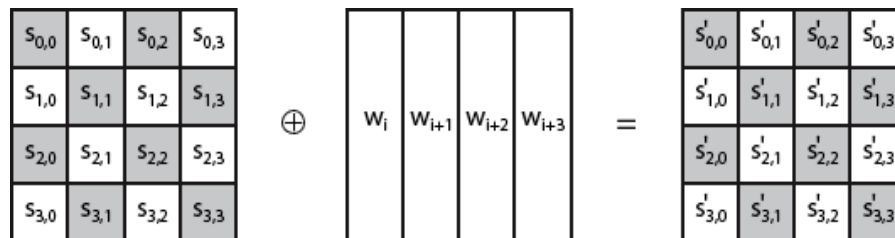
Mixing:

It means interbyte transformation that changes bits inside a byte, based on the bits inside to neighboring bytes. We need mix bytes to provide diffusion at the bit level. The mix columns transformation operates at the column level. It transforms each column of the state to a new column.



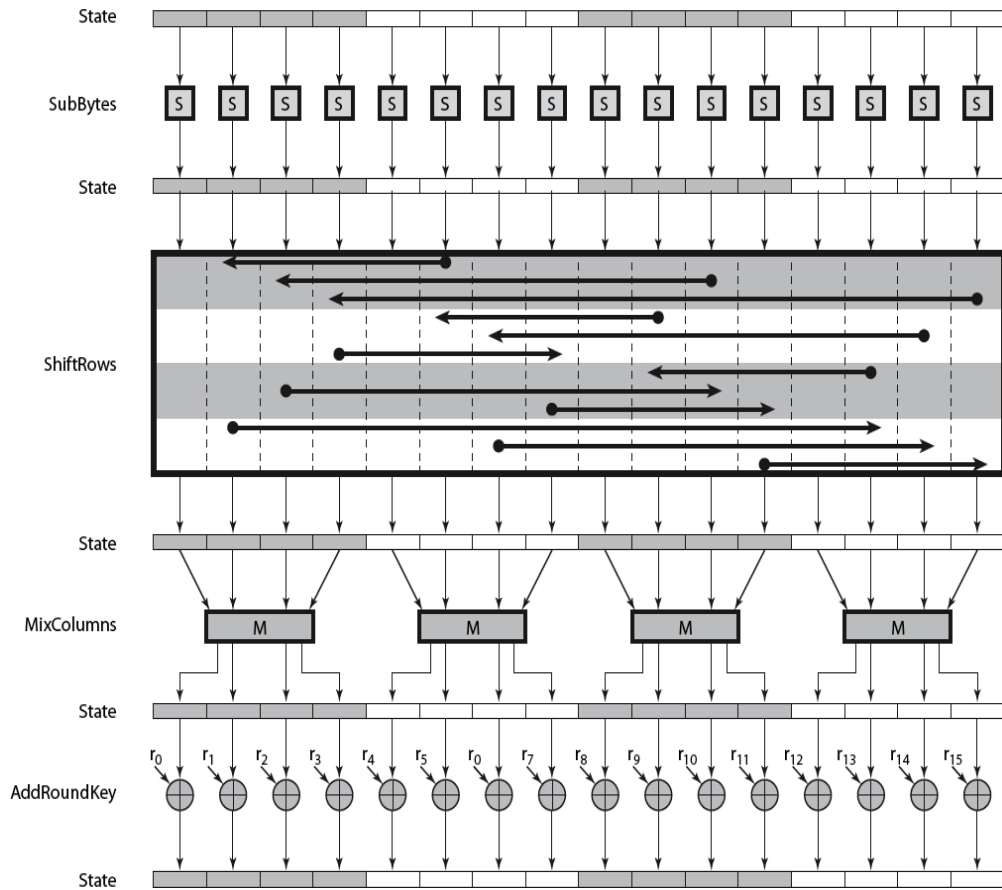
XOR with a key:

This operation uses a simple bitwise XOR of the current block with a portion of the expanded key.



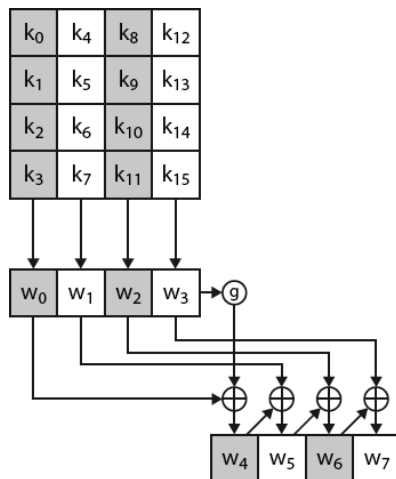
The input to the encryption and decryption algorithm is 128 bit block. This block is copied into a state array. The state array is modified at each stage of encryption or decryption. After the final stage the output is copied into output matrix. 128 bit key is also depicted as a square matrix of bytes. This key is then expanded into the array of key scheduled words. Each word is 4 bytes and the total key schedule is 44 words for the 128 bit key. The ordering of bytes within a matrix is by column. For example first 4 bytes of a 128 bit plaintext input to the encryption cipher occupies the first column of the in matrix, the second four bytes occupy the second column and so on. Similarly the first four bytes of the expanded key which forms a word, occupy the first column of the w matrix.

AES Round:



AES Key Expansion:

It takes 128 bit key and expands into array of 44/52/60 32-bit words.



Explain about Triple DES.

Triple DES was first proposed by Tuchman and first standardized for the use in financial applications. In cryptography, **Triple DES (3DES)** is the common name for the Triple Data Encryption Algorithm (TDEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Because of the availability of increasing computational power, the key size of the original DES cipher was becoming subject to brute force attacks; Triple DES was designed to provide a relatively simple method of increasing the key size of DES to protect against such attacks, without designing a completely new block cipher algorithm.

$$\text{Ciphertext} = E_{K_3}(D_{K_2}(E_{K_1}(\text{Plaintext})))$$

Where,

$E_x[X]$ = encryption of X using key K

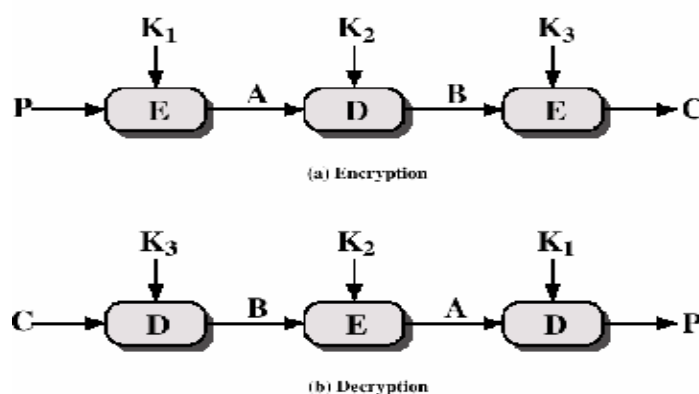
$D_x[Y]$ = decryption of Y using key K

Decryption is simply the same operation with the keys reversed.

$$\text{Plaintext} = D_{K_1}(E_{K_2}(D_{K_3}(\text{Ciphertext})))$$

With three distinct keys, TDES has an effective key length of 168 bits. FIPS (Federal Information Processing Standards) also allows for the use of two keys with $K_1=K_3$. This provides a length of 112 bits. FIPS includes the following guidelines for TDES.

1. TDES is the FIPS approved conventional encryption algorithm.
2. Govt. organizations with DES systems are encouraged to transit to TDES.
3. It is anticipated that TDES and AES will coexist as FIPS approved algorithms allowing for a gradual transition to AES.



Explain about INTERNATIONAL DATA ENCRYPTION ALGORITHM. (IDEA)

1. IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM) is a symmetric block cipher algorithm.
2. IDEA is developed by Lai and James of Swiss Federal Institute of Technology in 1991.
3. IDEA uses 128 bit key and is divided into 52 subkeys.
4. IDES uses 64 bit plain text block.
5. Number of identical rounds are 8 where in each round 6 keys are used ($6 \times 8 = 48$ keys).
6. In last round the remaining 4 keys are used in both encryption and decryption process.
7. It was meant to be a replacement for DES algorithm.

Design Issues:

1. IDEA does not use S-boxes.
2. IDEA relies on three different mathematical operations:
 - XOR
 - Binary Addition of 16-bit integers,
 - Binary Multiplication of 16-bit integers.
3. These functions are combines to produce a complex transformation and are very difficult to cryptanalyze.

Key Generation Process:

1. 128 bit key is divided into 8 subparts of 16 bits each.
2. Then 128 bit key is left shifted to 25th position which will generate a new 128 bit key.
3. Then it is divided into 8 subparts and will be used to next round.
4. The same process is performed 9 times.

Sequence of operations in one round:

1. Multiply P1 and K1
2. Add P2 and K2
3. Add P3 and K3
4. Multiply P4 and K4
5. Step 1 XORed with Step 3
6. Step 2 XORed with Step 4
7. Multiply Step 5 with K5
8. Add Step 6 and Step 7
9. Multiply result of Step 8 with K6
10. Add Step 7 and Step 9
11. XOR Step 7 and Step 9.
12. XOR Step 1 and Step 9.

13. XOR Step 3 and Step 9.
 14. XOR Step 2 and Step 10.
 15. XOR Step 4 and Step 10.
- Same operations are performed in 8 rounds

Sequence of operation in last round:

1. Multiply P1 with K49.
2. Add P2 and K50.
3. Add P3 and K51.
4. Multiply P4 and K52.

Encryption:

1. 64 bit plain text is divided into 4 16-bit blocks and they are taken as input in first round.
2. The first round output is taken as input for second round.
3. The same process is repeated for all the subsequent 8 encryption rounds.
4. The 9th round uses 4 keys and performs different operations.

Decryption:

1. The process of decryption is same as the process used for encryption.
2. The difference is the keys used for decryption is the inverse of the keys used during encryption.

Applications:

1. Financial and commercial data
2. E-Mail
3. Smart Cards, etc.

Explain about Blowfish.

1. It is a symmetric block cipher encryption algorithm designed by Bruce in 1993.
2. It is one of the fastest block ciphers in public use.
3. It is a general purpose algorithm intended as replacement for the DES algorithm.
4. Block size is 64 bits and key size is from 32 bits to 448 bits and number of rounds is 16.
5. It is designed to be easy to implement and to have a high execution speed.
6. It uses S-boxes and XOR function. Blowfish uses dynamic S-boxes are generated by repeated application of Blowfish algorithm. A total of 521 executions are required to produce the subkeys and S-boxes.

Description of the Algorithm:

Blowfish is a symmetric block cipher algorithm which encrypts 64 bits at a time. It follows feistel network.

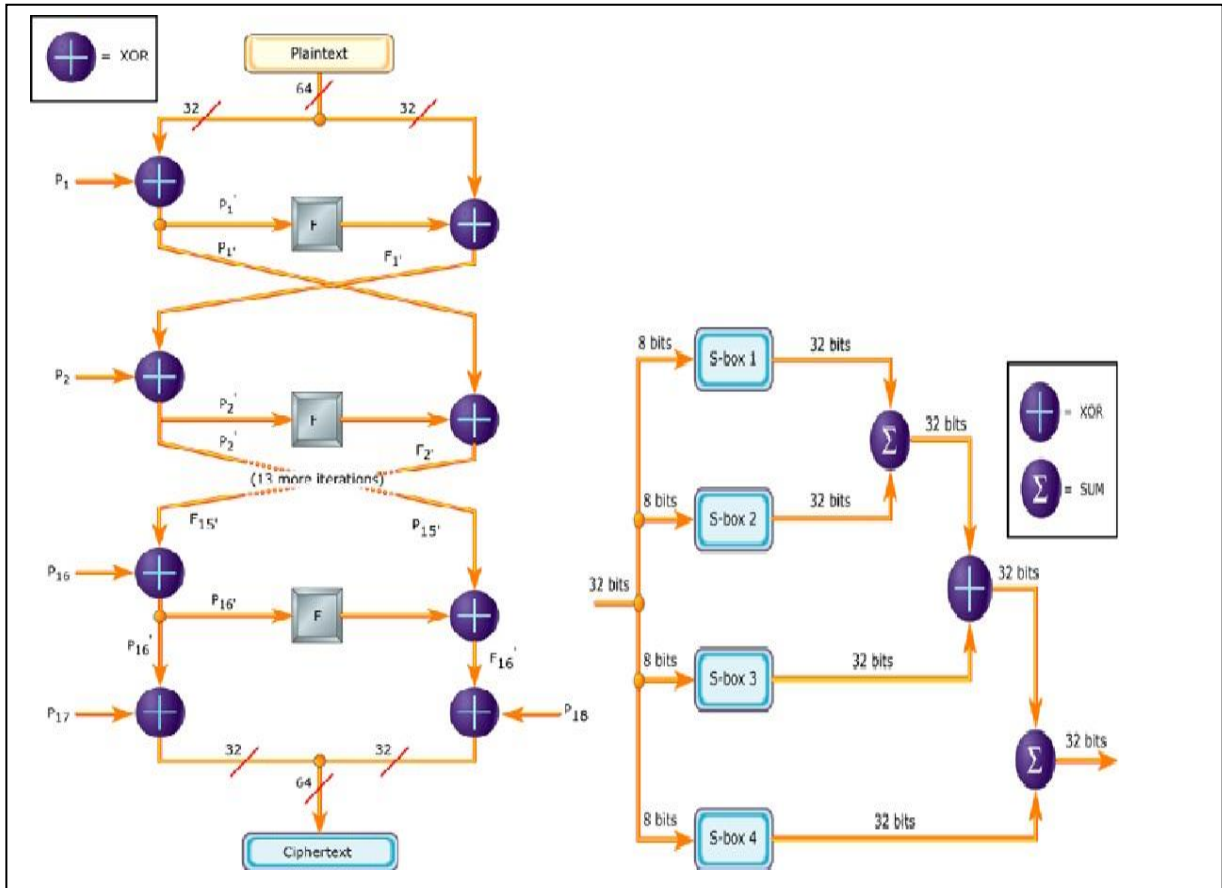
Key expansion:

- The p-array consists of 18, 32 bit sub-keys (576), i.e., P1,P2, ...,P18.
 - Four 32 bit S-boxes consist of 256 entries each (S1, S2, S3, S4).
1. Initialize the P-array and four S-boxes with a fixed string, which contains hexadecimal digits.
 2. XOR P1 with first 32 bits of the key, XOR P2 with second 32 bits of the key, XOR P3 with third 32 bits of the key and so on until the entire P-array has been XORed with the key bits.
 3. Encrypt all zero string with blowfish algorithm using the subkeys which are generated in step 1 and 2.
 4. Replace P1 and P2 with the output obtained in step 3.
 5. Encrypt the output of step 3 using Blowfish algorithm with the modified sub keys.
 6. Replace P3 and P4 with the output of step 5.
 7. Continue the same process until all the entries in the P array are replaced and then all the S-boxes with the output of the continuously changing Blowfish algorithm.

Total of 521 iterations are required to generate all required sub-keys.

Encryption:

It has 16 rounds and each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words.

**Algorithm:**

1. Blowfish Encryption Divides the plaintext into two 32-bit halves: x_L, x_R
2. For $i = 1$ to 16:
3. $x_L = x_L \text{ XOR } P_i$
4. $x_R = F(x_L) \text{ XOR } x_R$
5. Swap x_L and x_R
6. Swap x_L and x_R (Undo the last swap.)
7. $x_R = x_R \text{ XOR } P_{17}$
8. $x_L = x_L \text{ XOR } P_{18}$
9. Recombine x_L and x_R

Decryption:

Decryption is exactly same as encryption, except that P_1, P_2, \dots, P_{18} are used in the reverse order.

Explain about CAST 128.

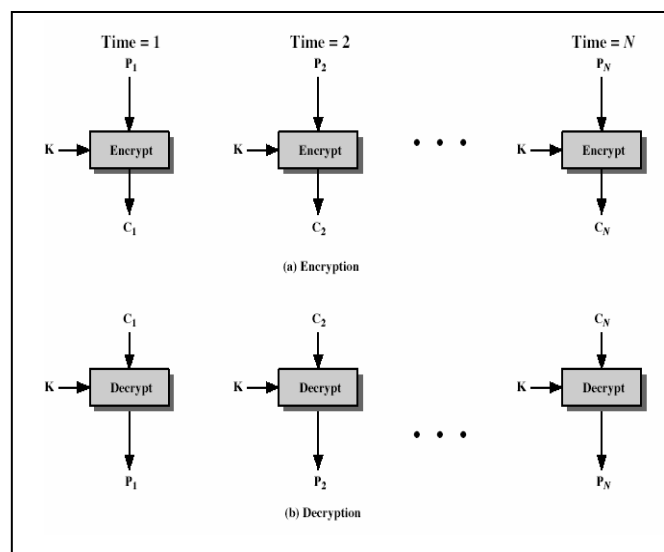
1. CAST-128 is a symmetric key block cipher and also been approved for Government of Canada use by Communications Security Establishment.
2. CAST-128 is a 12 or 16-round Feistel network with a 64-bit block size and a key size of between 40 to 128 bits (but only in 8-bit increments).
3. The full 16 rounds are used when the key size is longer than 80 bits. Components include large 8×32 -bit S-boxes based on bent functions (special type of Boolean functions), key-dependent rotations, modular addition, subtraction and XOR operations. There are three alternating types of round function, but they are similar in structure and differ only in the choice of the exact operation (addition, subtraction or XOR) at various points.

EXPLAIN ABOUT VARIOUS MODES OF OPERATIONS WITH NEAT DIAGRAMS.

The DES algorithm is a basic building block for providing data security. To apply DES in a variety of applications, four "modes of operation" have been defined. These four modes are intended to cover virtually all the possible applications of encryption for which DES could be used.

Electronic Codebook Mode

1. The simplest mode is the electronic codebook (ECB) mode, in which plaintext is handled 64 bits at a time and each block of plaintext is encrypted using the same key.
2. The term *codebook* is used because, for a given key, there is a unique ciphertext for every 64-bit block of plaintext.

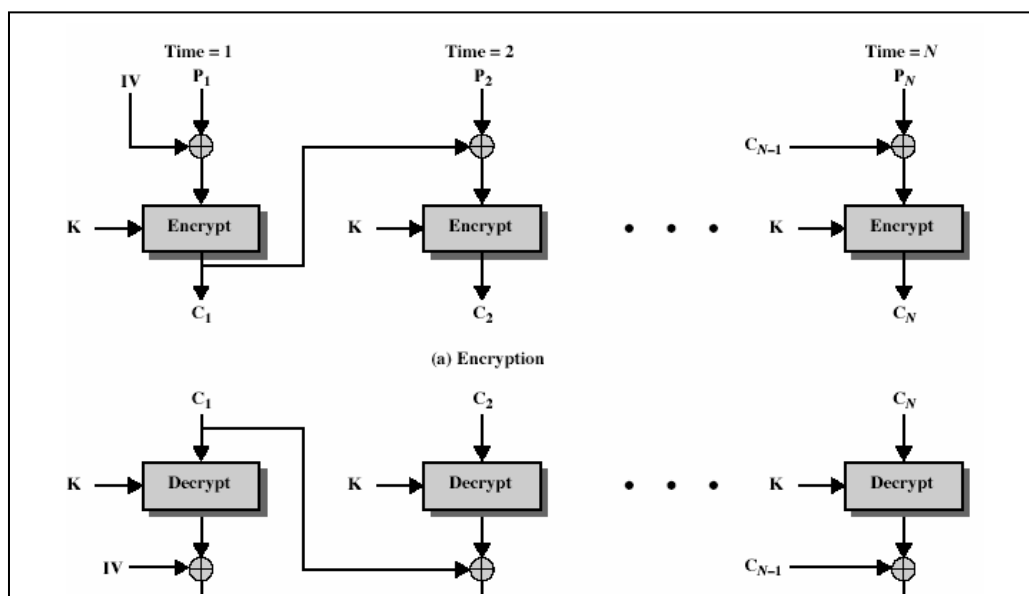


3. For a message longer than 64 bits, the procedure is simply break the message into 64-bit blocks, padding the last block if necessary.

4. Decryption is performed one block at a time, always using the same key.
5. In the above [Figure](#), the plaintext (padded as necessary) consists of a sequence of 64-bit blocks, P_1, P_2, \dots, P_N ; the corresponding sequence of ciphertext blocks is C_1, C_2, \dots, C_N .
6. The ECB method is ideal for a short amount of data, such as an encryption key, thus, if you want to transmit a DES key securely, ECB is the appropriate mode to use.
7. The most significant characteristic of ECB is that the same 64-bit block of plaintext, if it appears more than once in the message, always produces the same ciphertext.
8. For lengthy messages, the ECB mode may not be secure.

Cipher Block Chaining Mode

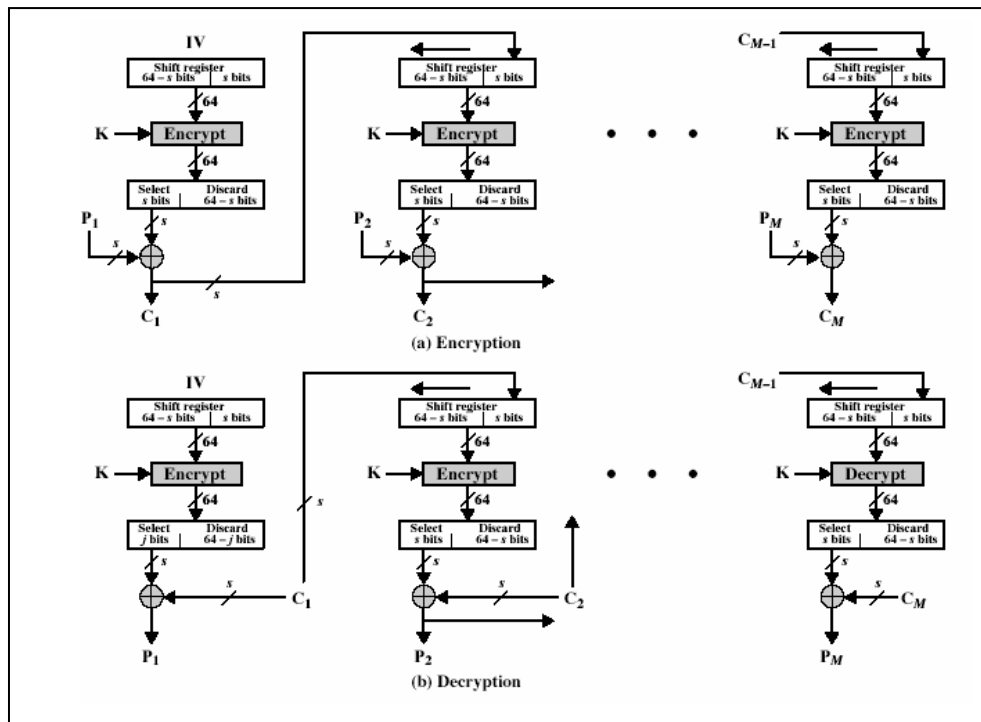
1. To overcome the security deficiencies of ECB, we would like a technique in which the same plaintext block, if repeated, produces different ciphertext blocks.
2. A simple way to satisfy this requirement is the cipher block chaining (CBC) MODE. In this scheme, the input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block; the same key is used for each block.



3. For decryption, each cipher block is passed through the decryption algorithm. The result is XORed with the preceding ciphertext block to produce the plaintext block.
4. To produce the first block of ciphertext, an initialization vector (IV) is XORed with the first block of plaintext.
5. The IV must be known to both the sender and receiver. For maximum security, the IV should be protected as well as the key.

Cipher Feedback Mode

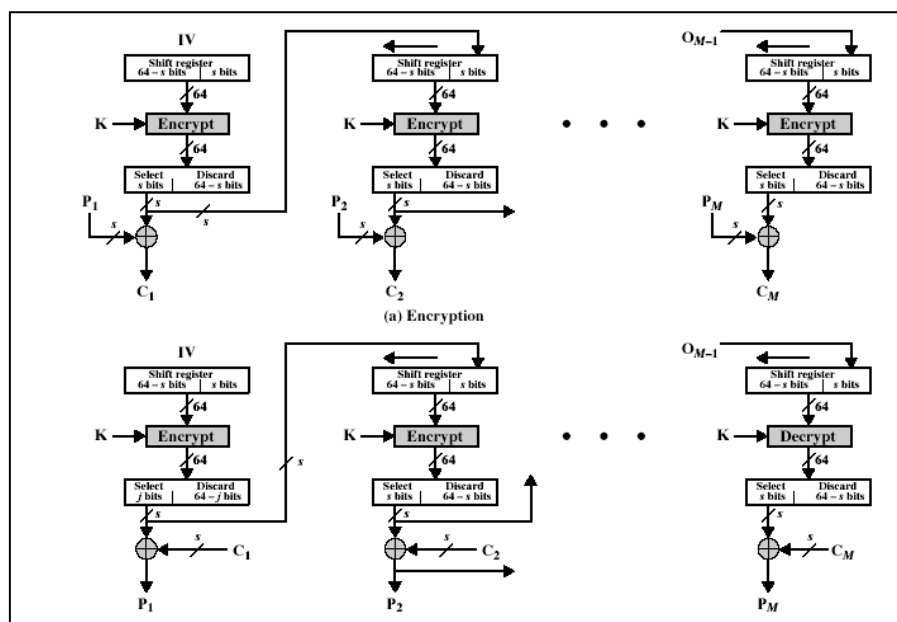
1. The DES scheme is essentially a block cipher technique that uses 64-bit blocks. However, it is possible to convert DES into a stream cipher, using either the cipher feedback (CFB) or the output feedback mode.
2. A stream cipher eliminates the need to pad a message to be an integral number of blocks. It also can operate in real time. If a character stream is being transmitted, each character can be encrypted and transmitted immediately using a character-oriented stream cipher.



3. In the [Figure](#), it is assumed that the unit of transmission is s bits; a common value of S is 8. In CBC the units of plaintext are chained together but in CFB rather than units of 64 bits of the plaintext it is divided into *segment* of s bits.
4. The input to encryption function is a 64-bit shift register that is initially set to some initialization vector (IV). The leftmost s bits in the output of the encryption function are XORed with the first segment of plaintext P_1 to produce the first unit of ciphertext C_1 , which is then transmitted. In addition, the contents of the shift register are shifted left by s bits and C_1 is placed in the rightmost (least significant) s bits of the shift register, this process continues until all plaintext units have been encrypted.
5. For decryption, the same scheme is used, except that the received ciphertext unit is XORed with the output of the encryption function to produce the plaintext unit. Note that it is the encryption function that is used, not the decryption function.

Output Feedback Mode

1. The output feedback (OFB) mode is similar in structure to that of CFB. As can be seen, it is the output of the encryption function that is fed back to the shift register in OFB, whereas in CFB the ciphertext unit is fed back to the shift register.
2. One advantage of the OFB method is that bit errors in transmission do not propagate. For example, if a bit error occurs in C_1 , only the recovered value of P_1 is affected; subsequent plaintext units are not corrupted. With CFB, C_1 also serves as input to the shift register and therefore causes additional corruption downstream.
3. The disadvantage of OFB is that it is more vulnerable to a message stream modification attack than CFB. Consider that complementing a bit in the ciphertext complements the corresponding bit in the recovered plaintext. Thus, controlled changes to the recovered plaintext can be made. This may make it possible for an opponent, by making the necessary changes to the checksum portion of the message as well as to the data portion, to alter the ciphertext in such a way that it is not detected by an error-correcting code.



QUESTIONS

1. EXPLAIN ABOUT BLOCK CIPHER DESIGN PRINCIPLES.
2. EXPLAIN ABOUT DES WITH A NEAT DIAGRAM.
3. EXPLAIN ABOUT VARIOUS MODES OF OPERATIONS WITH NEAT DIAGRAMS.
4. EXPLAIN ABOUT AES.
5. EXPLAIN ABOUT IDEA AND TRIPLE DES.
6. WRITE ABOUT KEY EXPANSION IN BLOWFISH.

UNIT – III

NUMBER THEORY & ASYMMETRIC KEY CRYPTOGRAPHY:

NUMBER THEORY: PRIME AND RELATIVELY PRIME NUMBERS, MODULAR ARITHMETIC, FERMAT'S AND EULER'S THEOREMS, THE CHINESE REMAINDER THEOREM, DISCRETE LOGARITHMS.

PUBLIC KEY CRYPTOGRAPHY: PRINCIPLES, PUBLIC KEY CRYPTOGRAPHY ALGORITHMS, RSA ALGORITHM, DIFFIE-HELLMAN KEY EXCHANGE, ELGAMAL ENCRYPTION & DECRYPTION, ELLIPTIC CURVE CRYPTOGRAPHY.

NUMBER THEORY

PRIME AND RELATIVELY PRIME NUMBERS:

An integer $P > 1$ is a prime number only if its divisors are 1 and P .

Two integers are said to be **relatively prime** if the only common factor between them is 1.

Any integer can be broken down into certain multiples of prime numbers; this is called prime factorization. When you prime factorize two integers and the only common number is 1, then the two integers are said to be relatively prime.

Ex:

$$18 = 2 \times 3 \times 3$$

$$35 = 7 \times 5$$

So 18 and 35 are relatively prime numbers.

$$18 = 2 \times 3 \times 3$$

$$21 = 3 \times 7$$

3 is a common factor for both 18 and 21, so 18 and 21 are not relatively prime numbers.

MODULAR ARITHMETIC:

If n and a are any two positive integers and if we divide a by n we get an integer quotient q and an integer remainder r that obey the following condition.

$$A = qn + r \quad 0 \leq r < n \quad ; [q = \lfloor a/n \rfloor]$$

Ex:

$$A = 11 \quad n = 7$$

$$Q = 11/7 = 1 \quad r = 11 - 7 = 4$$

$$A = qn + r$$

$$= (1 \times 7) + 4$$

$$= 7 + 4$$

$$= 11$$

If n is a positive integer and a is an integer, then we define $a \bmod n$. The integer n is called the modulus.

$$A = [a/n] \times n + (a \bmod n)$$

Ex: $11 \bmod 7 = 4$ and $-11 \bmod 7 = 4$

Two integers a and b are said to be congruent modulo n if and only if

$$(a \bmod n) = (b \bmod n).$$

This will be written as $a \equiv b \pmod{n}$

$$73 \equiv 4 \pmod{23}$$

$$73 \bmod 23 = 4$$

$$4 \bmod 23 = 4$$

So 73 and 4 are congruent modulo to 23.

Modular arithmetic operations:

Properties:

Property	Expression
Commutative Laws	$(a+b) \bmod n = (b+a) \bmod n$ $(a*b) \bmod n = (b*a) \bmod n$
Associative Laws	$[(a+b)+c] \bmod n = [a+(b+c)] \bmod n$ $[(a*b)*c] \bmod n = [a*(b*c)] \bmod n$
Distributive Law	$[a*(b+c)] \bmod n = [(a+b)*(a+c)] \bmod n$
Identities	$(0+a) \bmod n = a \bmod n$ $(1*a) \bmod n = a \bmod n$

FERMAT'S THEOREM

This theorem plays an important role in public key cryptography. This theorem states that If ' p ' is a prime and ' a ' is a positive integer not divisible by p then $a^{p-1} \equiv 1 \pmod{p}$. This theorem is also known as Fermat's little theorem. This theorem is used in RSA and primality testing.

Proof:

- Consider a set of positive integers less than p .
 $P = \{1, 2, \dots, p-1\}$
- Multiply each element by a and modulo p , to get the set X .
 $X = \{a \bmod p, 2a \bmod p, \dots, (p-1)a \bmod p\}$.

None of the elements of X is equal to zero, because p does not divide a and also any two of the integers in X are not equal.

- Assume that $ja \equiv ka \pmod{p}$, here $1 \leq j < k \leq p-1$, because of 'a' is relatively prime to p , we can eliminate 'a' from both sides.

$$j \equiv k \pmod{p}$$

- So we know that this last equality is impossible, because j and k are both positive integers less than p . so $(p-1)$ elements of X are all positive integers with no two elements are equal.

$$A \times 2a \times \dots \times (p-1)a \equiv [1 \times 2 \times 3 \times \dots \times (p-1)] \pmod{p}$$

$$A^{p-1} \equiv 1 \pmod{p}$$

Ex: $p=7, p=19$

$$7^2 = 49 \equiv 11 \pmod{19}$$

$$7^4 = 121 \equiv 7 \pmod{19}$$

$$7^8 = 49 \equiv 11 \pmod{19}$$

$$7^{16} = 121 \equiv 7 \pmod{19}$$

$$A^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}$$

Euler's Totient Theorem:

Euler's totient function $\Phi(n)$ is defined as the number of positive integers less than 'n' and are relatively prime to 'n'.

$$\Phi(n) = 1$$

Ex: Determine $\Phi(35)$

To determine $\Phi(35)$ we need all the positive integers less than 35 that are relatively prime to it;

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34

$$\Phi(35) = 24$$

$$\Phi(p) = p-1$$

Suppose we have two prime numbers p and q with $p \neq q$.

$$n = pq$$

$$\Phi(n) = \Phi(pq)$$

$$= \Phi(p) \times \Phi(q)$$

$$= (p-1) \times (q-1)$$

Euler's theorem states that every a and n that are relatively prime. $a^{\Phi(n)} \equiv 1 \pmod{n}$

EX:

$$A= 3, n=10, \Phi (10)= 4$$

$$a^{\Phi (n)}= 3^4 = 81 = 1(\text{mod } 10) = 1(\text{ mod } n)$$

THE CHINESE REMAINDER THEOREM (CRT)

Let m_1, m_2, \dots, m_n be pairwise relatively prime positive integers and let b_1, b_2, \dots, b_n be any integers. Then the system of linear congruences in one variable given by;

$$X \equiv b_1 \text{ mod } m_1$$

$$X \equiv b_2 \text{ mod } m_2$$

.

.

.

$$X \equiv b_n \text{ mod } m_n$$

Has unique solution modulo m_1, m_2, \dots, m_n .

Proof:

E first construct a solution to the given system of linear congruences in one variable. Let $M = m_1, m_2, \dots, m_n$ and, for $I = 1, 2, \dots, n$, let $M_i = M/m_i$. noe $(M_i, m_i) = 1$ for each i . So $M_i x_i \equiv 1 \text{ mod } m_i$ has a solution for each i by Corollary forms

$$X = b_1 M_1 x_1 + b_2 M_2 x_2 + \dots + b_n M_n x_n$$

Note that x is a solution of the desired system since, for $i = 1, 2, \dots, n$

$$\begin{aligned} X &= b_1 M_1 x_1 + b_2 M_2 x_2 + \dots + b_i M_i x_i + \dots + b_n M_n x_n \\ &\equiv 0 + 0 + \dots + b_i + \dots + 0 \text{ mod } m_i \\ &\equiv b_i \text{ mod } m_i \end{aligned}$$

It remains to show the uniqueness of the solution modulo M . let x' be another solution of the given system of linear congruences in one variable. Then, for all I , we have that $x' \equiv b_i \text{ mod } m_i$ for all i , we have that $x \equiv x' \text{ mod } m_i$ for all i or equivalently, $m_i \mid x - x'$ for all i . then $M \mid x - x'$ from which $x \equiv x' \text{ mod } M$. The proof is complete.

Note that the proof of the CRT shows the existence and uniqueness of the claimed solution modulo M by actually constructing this solution. Such a proof is said to be constructive; the advantage of constructive proofs is that they yield a procedure or algorithm for obtaining the

desired quantity. We now use the procedure motivated in the proof of theorem to solve the system of linear congruences in one variable.

Ex:

$$X \equiv 2 \pmod{3}$$

$$X \equiv 1 \pmod{4}$$

$$X \equiv 3 \pmod{5}$$

$$M=3 \cdot 4 \cdot 5 = 60$$

$$M_1=60/3 =20$$

$$M_2=60/4 =15$$

$$M_3=60/5 =12$$

$$M_1=20, m_1 = 3$$

$$\text{Solve } 20x_1 \equiv 1 \pmod{3}$$

$$2x_1 \equiv 1 \pmod{3}$$

$$M_2=15, m_2 = 4$$

$$\text{Solve } 15x_2 \equiv 1 \pmod{4}$$

$$3x_2 \equiv 1 \pmod{4}$$

$$M_3=12, m_3 = 5$$

$$\text{Solve } 12x_3 \equiv 1 \pmod{5}$$

$$2x_3 \equiv 1 \pmod{5}$$

$$\begin{aligned} X &= b_1M_1x_1 + b_2M_2x_2 + b_3M_3x_3 \\ &= 2(20)(2) + 1(15)(3) + 3(12)(3) = 233 \pmod{60} \\ &\equiv 53 \pmod{60} \end{aligned}$$

So any positive integer congruent to 53 mod 60 is a solution to the system.

DISCRETE LOGARITHMS

Discrete logarithms are fundamental to number of public key algorithms.

The powers of Integer, modulo n:

According to Euler's theorem;

$$a^{\Phi(n)} \equiv 1 \pmod{n}$$

where $\Phi(n)$ is Euler's totient function, represents the number of positive integers less than 'n' are relatively prime to 'n'.

$$a^m \equiv 1 \pmod{n} \text{ where } m = \Phi(n)$$

The following tables shos the powers of 'a' modulo 19 for all positive a<19.

Table 8.3 Powers of Integers, Modulo 19

a	a ²	a ³	a ⁴	a ⁵	a ⁶	a ⁷	a ⁸	a ⁹	a ¹⁰	a ¹¹	a ¹²	a ¹³	a ¹⁴	a ¹⁵	a ¹⁶	a ¹⁷	a ¹⁸
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

- All sequences end with 1
- The length of a sequence divides $\Phi(19) = 18$
- Some of the sequences are of length 18. In this case, it is said that the base integer 'a' generates the set of nonzero integers modulo 19. Each such integer is called a prime root of the modulus 19.

The highest possible exponent to which a number can belong (mod n) is $\Phi(n)$. if a number is of this order, it is referred to as a primitive root of n. the importance of this solution is that if 'a' is a prime root of n, then its powers;

$$a, a^2, \dots, a^{\Phi(n)}$$

are distinct (mod n) and are all relatively prime to n. in partical for a primer number p, if a is a primitive root of p, then

$$a, a^2, \dots, a^{p-1}$$

are distinct (mod p). for othe pirme number 19, the primitive roots are 2, 3, 10, 13, 14 and 15.

Logarithms for modular arithmetic:

For ordinary positive real number, the logarithm function is the inverse of exponentiation.

Logarithm properties:

- The logarithm of a number is defined to be the poser to which some positive base except 1 must be raised in order to equal to the number. That is for base x and for a value y.

$$y = x^{\log_x(y)}$$

- $\text{Log}_x(1) = 0$
- $\text{Log}_x(x) = 1$
- $\text{Log}_x(yz) = \text{Log}_x(y) + \text{Log}_x(z)$
- $\text{Log}_x(y^r) = r \times \text{Log}_x(y)$

Consider a primitive root a for some number p, then we know that the powers of a from 1 through (p-1) produce each integer from 1 through (p-1) exactly once. We also know that any integer b satisfies;

$$b \equiv r \pmod{p} \text{ for some } r, \text{ where } 0 <= r <= (p-1)$$

by the definition of modular arithmetic it follows that for any integer b and a primitive root a of prime numbr p, we can find a unique component i such that ;

$$b \equiv a^i \pmod{p}, \text{ where } 0 <= i <= (p-1)$$

this exponent of I is referred to as the discrete logarithm of the number b for the base a (mod p). we denote this value as $\text{dlog}_{a,p}(b)$ ¹⁰.

Ex:

Here is an example using a nonprime modulus, $n = 9$. Here $\phi(n) = 6$ and $a = 2$ is a primitive root. We compute the various powers of a and find

$$2^0 = 1 \quad 2^4 \equiv 7 \pmod{9}$$

$$2^1 = 2 \quad 2^5 \equiv 5 \pmod{9}$$

$$2^2 = 4 \quad 2^6 \equiv 1 \pmod{9}$$

$$2^3 = 8$$

This gives us the following table of the numbers with given discrete logarithms (mod 9) for the root $a = 2$:

Logarithm	0	1	2	3	4	5
Number	1	2	4	8	7	5

To make it easy to obtain the discrete logarithms of a given number, we rearrange the table:

Number	1	2	4	5	7	8
Logarithm	0	1	2	5	4	3

Now consider

$$x = a^{\text{dlog}_{a,p}(x)} \pmod{p} \quad y = a^{\text{dlog}_{a,p}(y)} \pmod{p}$$

$$xy = a^{\text{dlog}_{a,p}(xy)} \pmod{p}$$

Using the rules of modular multiplication,

$$\begin{aligned} xy \pmod{p} &= [(x \pmod{p})(y \pmod{p})] \pmod{p} \\ a^{\text{dlog}_{a,p}(xy)} \pmod{p} &= [(a^{\text{dlog}_{a,p}(x)} \pmod{p})(a^{\text{dlog}_{a,p}(y)} \pmod{p})] \pmod{p} \\ &= (a^{\text{dlog}_{a,p}(x) + \text{dlog}_{a,p}(y)}) \pmod{p} \end{aligned}$$

But now consider Euler's theorem, which states that, for every a and n that are relatively prime,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Any positive integer z can be expressed in the form $z = q + k\phi(n)$, with $0 \leq q < \phi(n)$. Therefore, by Euler's theorem,

$$a^z \equiv a^q \pmod{n} \quad \text{if } z \equiv q \pmod{\phi(n)}$$

Applying this to the foregoing equality, we have

$$\text{dlog}_{a,p}(xy) \equiv [\text{dlog}_{a,p}(x) + \text{dlog}_{a,p}(y)] \pmod{\phi(p)}$$

and generalizing,

$$\text{dlog}_{a,p}(y^r) \equiv [r \times \text{dlog}_{a,p}(y)] \pmod{\phi(p)}$$

This demonstrates the analogy between true logarithms and discrete logarithms.

Keep in mind that unique discrete logarithms mod m to some base a exist only if a is a primitive root of m .

Table 8.4, which is directly derived from Table 8.3, shows the sets of discrete logarithms that can be defined for modulus 19.

Table 8.4 Tables of Discrete Logarithms, Modulo 19

(a) Discrete logarithms to the base 2, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(b) Discrete logarithms to the base 3, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

(c) Discrete logarithms to the base 10, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{10,19}(a)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

(d) Discrete logarithms to the base 13, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{13,19}(a)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

(e) Discrete logarithms to the base 14, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{14,19}(a)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9

(f) Discrete logarithms to the base 15, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{15,19}(a)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

Calculation of Discrete Logarithms

Consider the equation

$$y = g^x \bmod p$$

Given g , x , and p , it is a straightforward matter to calculate y . At the worst, we must perform x repeated multiplications, and algorithms exist for achieving greater efficiency (see Chapter 9).

However, given y , g , and p , it is, in general, very difficult to calculate x (take the discrete logarithm). The difficulty seems to be on the same order of magnitude as that of factoring primes required for RSA. At the time of this writing, the asymptotically fastest known algorithm for taking discrete logarithms modulo a prime number is on the order of [BETH91]:

$$e^{((\ln p)^{1/3}(\ln(\ln p))^{2/3})}$$

which is not feasible for large primes.

PUBLIC KEY CRYPTOGRAPHY

Public key algorithms are also called as asymmetric key algorithms. Public key cryptography refers to a cryptographic system requiring two separate keys one of which is kept as secret is known as private key and one of which is public known as public key. One key is used for encryption and other key is used for decryption.

PUBLIC KEY CRYPTOGRAPHY: PRINCIPLES, PUBLIC KEY CRYPTOGRAPHY ALGORITHMS, RSA ALGORITHM, DIFFIE-HELLMAN KEY EXCHANGE, ELGAMAL ENCRYPTION & DECRYPTION, ELLIPTIC CURVE CRYPTOGRAPHY.

WHAT ARE THE PRINCIPLES OF PUBLIC KEY CRYPTOSYSTEMS?

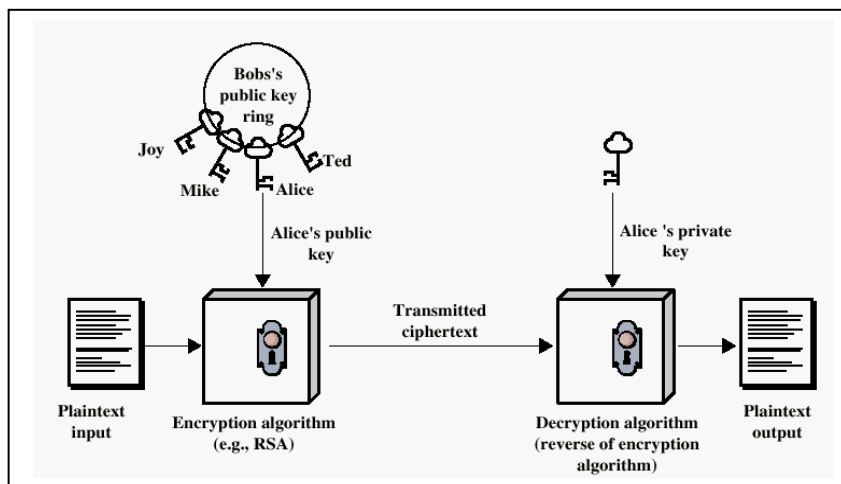
Public-key cryptography is a cryptographic approach, which involves the use of asymmetric key algorithms instead of symmetric key algorithms. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver. The asymmetric key algorithms are used to create a mathematically related key pair: a secret private key and a published public key. Use of these keys allows protection of the authenticity of a message by creating a digital signature of a message using the private key, which can be verified using the public key. It also allows protection of the confidentiality and integrity of a message, by public key encryption, encrypting the message using the public key, which can only be decrypted using the private key.

Public key encryption was first publicly proposed by Diffie and Hellman in 1976. Public algorithms are based on mathematical functions rather than simple operations on bit patterns. The distinguishing technique used in public key cryptography is the use of asymmetric key algorithms, where one key used to encrypt a message and another key is used to decrypt the message. Each user has a pair of cryptographic keys—a public key and a private key. The private key is kept secret, while the public key may be widely distributed. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. The keys are related mathematically, but the private key cannot feasibly be derived from the public key. The discovery of algorithms that could produce public/private key pairs revolutionized the practice of cryptography beginning in the middle 1970s. In fact, the security of any encryption scheme depends on 1) The length of the key and 2) The computational work involved in breaking a cipher.

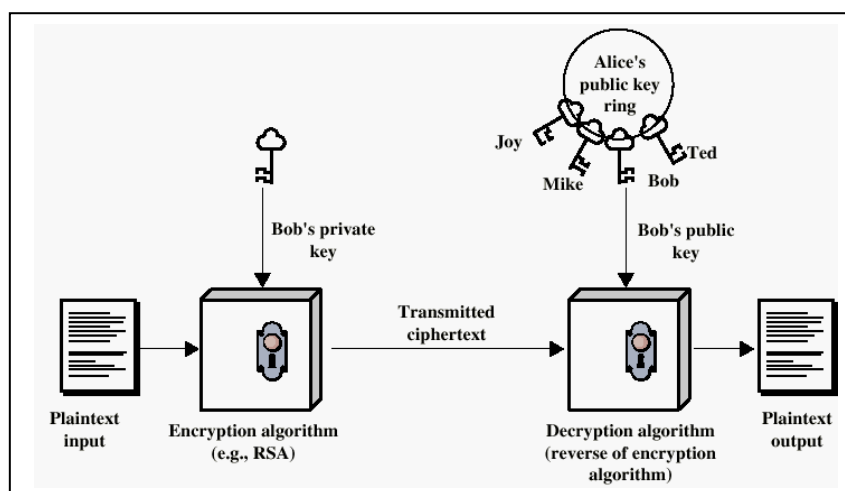
A public key encryption scheme has six ingredients. They are;

- **Plain Text:** This is the original message or data that is fed into the algorithm as input.
- **Encryption Algorithm:** The encryption algorithm performs various substitutions and transformations on the plain text.
- **Public and private key:** This is a pair of keys that have been selected so that if one is used for encryption and the other is used for decryption.
- **Cipher Text:** This is the scrambled message produced as output. It depends on the plain text and the secret key. For a given message, two different keys will produce two different cipher texts.
- **Decryption Algorithm:** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plain text.

Encryption Public Key (Confidentiality)



Encryption Private Key (Authentication)



DIFFERENTIATE BETWEEN CONVENTIONAL ENCRYPTION AND PUBLIC KEY ENCRYPTION.

The same algorithm and key is used for encryption and decryption.	Algorithm is same for both encryption and decryption but one key is used for encryption and another key is used for decryption.
The sender and receiver must share the key and algorithm.	The sender and receiver must each have one of the paired keys.
The key must be kept secret	One of the two keys must be kept secret

What are the Applications for Public-Key Cryptosystems?

Public key systems are characterized by the use of a cryptographic type of an algorithm with two keys, one held private and one available publicly. Depending on the application, the sender uses either the sender's private key or the receiver's public key or the sender uses the sender's private key and receiver's public key or both.

Categories:

- 1. Encryption/decryption:** The sender encrypts a message with the recipient's public key.
- 2. Digital signature:** The sender signs a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.
- 3. Key exchange:** To exchange a session key.

Algorithm	Encryption/decryption	Digital signature	Key exchange
RSA	Yes	Yes	Yes
Duffie-Hellman	No	No	Yes
DSS	No	Yes	No
Elliptic Curve	Yes	Yes	Yes

Requirements for Public-Key Cryptography:

The public key cryptography algorithms must fulfill the following;

1. It is computationally easy for a party B to generate a pair
2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M to generate the corresponding ciphertext.

$$C = E_{k_{ub}}(M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message.

$$M = D_{KR_b}(C) = D_{KR_b}[E_{KU_b}(M)]$$

4. It is computationally infeasible for an opponent, knowing the public key, KU_b to determine the private key KR_b .
5. It is computationally infeasible for an opponent, knowing the public key, KU_b and a cipher text C to recover the original message M .
6. Either of the two related keys can be used for encryption, with the other used for decryption.

$$M = D_{KR_b}[E_{KU_b}(M)] = D_{KU_b}[E_{KR_b}(M)]$$

Explain about RSA Public Key Algorithm with an example.

RSA algorithm is described by Ron Rivest, Adi Shamir and Adleman in 1971. RSA implements a public key cryptosystem as well as digital signatures. This algorithm involves three steps.

They are;

1. Key generation
2. Encryption
3. Decryption

Key Generation:

RSA involves a public key and a private key. The public key is known by everyone and is used for encrypting the messages. Messages encrypted with the public key can only be decrypted with the corresponding private key. The keys are generated in the following way;

1. Choose two distinct prime number p and q . for security purpose the integers p and q should be chosen at random and should be of similar bit length. Prime integers can be efficiently found using a primality testing.
2. Compute $n = pq$. N is used as modulus for both the public and private keys.
3. Compute $\phi(n) = \phi(p) \phi(q) = (p-1)(q-1)$ where ϕ is Euler's totient function.
4. Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n))=1$; i.e. e and $\phi(n)$ are coprime. e is released as public key component.
5. Determine d as $d^{-1} \equiv e \pmod{\phi(n)}$ i.e. d is the multiplicative inverse of e (modulo $\phi(n)$). d is used as private key.

Encryption:

The public key (n,e) is transmitted to the sender and the sender send the message to the receiver by encrypting using this key. The message will be decrypted only with the private key of the receiver. It provides confidentiality.

$$C = M^e \pmod{n}$$

Where,

C = Cipher text

M = Plain text message

E = Public key

Decryption:

The receiver can recover the message by using his/her private key.

$$M = C^d \pmod{n}$$

Where,

C = Cipher text

M = Plain text message

D = Private key

Ex:



Example 1: Perform encryption and decryption using the RSA algorithm, for the following

- | | | | | |
|----|--------------|--------------|--------------|-------------|
| a) | p=3; | q=11; | e=7; | M=5. |
| b) | p=5; | q=11; | e=3; | M=9. |
| c) | p=11; | q=13; | e=11; | M=7. |

Solution:

a) **p=3; q=11; e=7; M=5.**

$$n = p \cdot q = 3 \cdot 11 = 33$$

$$\Phi(n) = (p-1)(q-1) = (3-1)(11-1) = 2 \cdot 10 = 20$$

$$ed \equiv 1 \pmod{\Phi(n)}$$

$$7 \cdot d \equiv 1 \pmod{20} \Rightarrow (7 \cdot d) \pmod{20} = 1 \pmod{20}$$

$$\Rightarrow (7 \cdot 3) \pmod{20} = 1 \pmod{20}$$

$$\Rightarrow 21 \pmod{20} = 1 \pmod{20}$$

$$\Rightarrow d = 3$$

For Encryption:

$$\begin{aligned}C &= M^e \bmod n \\ &= 5^7 \bmod 33 \\ &= 78125 \bmod 33 \\ &= 14\end{aligned}$$

For Decryption

$$\begin{aligned}M &= C^d \bmod n \\ &= 14^3 \bmod 33 \\ &= 2744 \bmod 33 \\ &= 5\end{aligned}$$

b) p=5; q=11; e=3; M=9.

$$N = p \cdot q = 5 \cdot 11 = 55$$

$$\Phi(n) = (p-1) \cdot (q-1) = (5-1) \cdot (11-1) = 4 \cdot 10 = 40$$

$$ed \equiv 1 \pmod{\Phi(n)}$$

$$3 \cdot d \equiv 1 \pmod{40} \Rightarrow (3 \cdot d) \bmod 40 = 1 \pmod{40}$$

$$\Rightarrow (3 \cdot 27) \bmod 40 = 1 \pmod{40}$$

$$\Rightarrow 81 \bmod 40 = 1 \pmod{40}$$

$$\Rightarrow d = 27$$

For Encryption:

$$\begin{aligned}C &= M^e \bmod n \\ &= 9^3 \bmod 55 \\ &= 729 \bmod 55 \\ &= 14\end{aligned}$$

For Decryption

$$\begin{aligned}M &= C^d \bmod n \\ &= 14^{27} \bmod 55 \\ &= 5\end{aligned}$$

c) p=11; q=13; e=11; M=7.

$$N = p \cdot q = 11 \cdot 13 = 143$$

$$\Phi(n) = (p-1) \cdot (q-1) = (11-1) \cdot (13-1) = 10 \cdot 12 = 120$$

$$ed \equiv 1 \pmod{\Phi(n)}$$

$$11 \cdot d \equiv 1 \pmod{120} \Rightarrow (11 \cdot d) \bmod 120 = 1 \pmod{120}$$

$$\Rightarrow (11 * 11) \bmod 120 = 1 \bmod 120$$

$$\Rightarrow 121 \bmod 120 = 1 \bmod 120$$

$$\Rightarrow d = 11$$

For Encryption:

$$\begin{aligned} C &= M^e \bmod n \\ &= 7^{11} \bmod 143 \end{aligned}$$

$$7^2 \bmod 143 = 49 \bmod 143$$

$$\begin{aligned} 7^4 \bmod 143 &= (49 * 49) \bmod 143 \\ &= 113 \end{aligned}$$

$$\begin{aligned} 7^8 \bmod 143 &= (113 * 113) \bmod 143 \\ &= 12769 \bmod 143 \\ &= 42 \end{aligned}$$

$$\begin{aligned} 7^3 \bmod 143 &= (7^2 * 7) \bmod 143 \\ &= 343 \bmod 143 \\ &= 57 \end{aligned}$$

$$\begin{aligned} 7^{11} \bmod 143 &= (42 * 57) \bmod 143 \\ &= 2394 \bmod 143 \\ &= 106 \end{aligned}$$

For Decryption

$$\begin{aligned} M &= C^d \bmod n \\ &= 106^{11} \bmod 143 \\ &= 7 \end{aligned}$$

Exercise: Perform encryption and decryption using the RSA algorithm, for the following

a) p=7; q=11; e=17; M=8.

b) p=17; q=31; e=7; M=2.

WRITE ABOUT THE SECURITY OF RSA.

Five possible approaches to attacking the RSA algorithm are;

- 1. Brute Force:** This involves trying all possible private keys.
- 2. Mathematical Attacks:** There are several approaches, all equivalent in effort to factoring the product of two primes.
- 3. Timing Attacks:** These depend on the running time of the decryption algorithm.
- 4. Hardware Fault-Based Attacks:** This involves inducing hardware faults in the processor that is generation digital signatures.
- 5. Chosen Ciphertext Attacks:** This type of attacks exploits properties of the RSA algorithm.

Explain about Diffie-Hellman Key Exchange Algorithm with an example.

Diffie-Hellman key exchange is a method of exchanging cryptographic keys between two users securely. The keys are used to encrypting the messages. This algorithm itself limited to exchange of the secret values.

Algorithm:

Global Public Elements	
q	prime number
α	$\alpha < q$ and α a primitive root of q

User A Key Generation	
Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \text{ mod } q$

User B Key Generation	
Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \text{ mod } q$

Calculation of Secret Key by User A	
$K = (Y_B)^{X_A} \text{ mod } q$	

Calculation of Secret Key by User B	
$K = (Y_A)^{X_B} \text{ mod } q$	

The security of Diffie-Hellman key exchange is relatively each to calculate exponentials modulo a prime, it is very difficult to calculate discrete logarithms. For large primes the task is considered as infeasible.

ExL

- Prime number $a = 353$ and primitive roots of 353 in this case $\alpha = 3$.
- A and B are select secret keys $X_A = 97$ and $X_B = 233$ respectively. Each computes its public key as follows;

A computes $Y_A = 3^{97} \bmod 353 = 40$

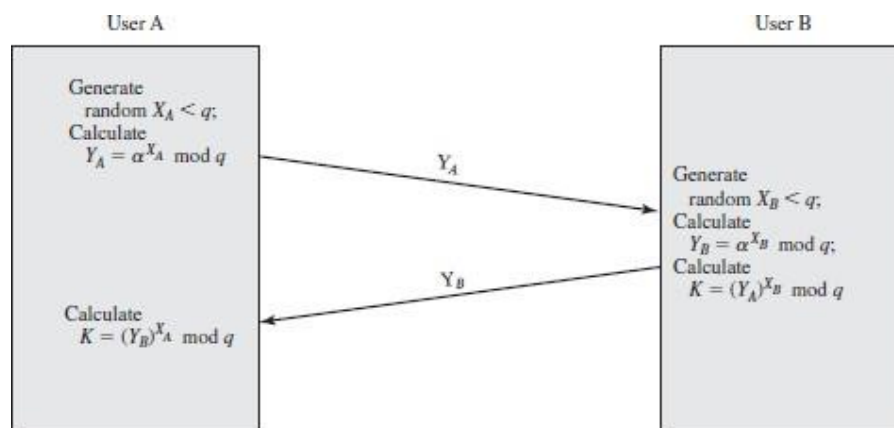
B computes $Y_B = 3^{233} \bmod 353 = 248$

- After the exchange of public keys each can compute the common secret key as follows.

A computes $K = (Y_B)^{X_A} = 248^{97} \bmod 353 = 160$

B computes $K = (Y_A)^{X_B} = 40^{233} \bmod 353 = 160$

Key Exchange Protocols:



- User A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection.
- User A can generate a one-time private key, calculate, and send that to user B.
- User B responds by generating a private value, calculating, and sending to user A. Both users can now calculate the key.
- The necessary public values and would need to be known ahead of time. Alternatively, user A could pick values for α and q and include those in the first message.

Explain about ELGAMAL ENCRYPTION & DECRYPTION Algorithm with an example.

T. ElGamal announced a public key cryptosystem based on discrete logarithms in 1984. It provides an alternative to the RSA System. Security of RSA depends on the difficulty of factoring large integers whereas security of ElGamal algorithm depends on the difficulty of computing discrete logs in a large prime modulus.

Applications:

- Key Sharing
- Encrypting Messages

Advantages:

The same plaintext gives different ciphertext.

Disadvantages:

Ciphertext is twice as long as the plaintext.

Key Generation:

1. Select a random prime number q and α which is a primitive root of q .
2. Generate a random integer X_A such that $1 < X_A < q-1$ (Private Key)
3. Calculate Public Key $Y_A = \alpha^{X_A} \bmod q$
4. A 's private key X_A and public key $[q, \alpha, X_A]$

Encryption: (Public key is used to encrypt the message)

1. Plaintext M should be in the range $0 \leq M < q-1$. Longer messages should be divided into blocks and each block size should be $< q$.
2. Choose a random integer k such that $1 \leq k \leq q-1$
3. Compute a onetime key $K = (Y_A)^k \bmod q$
4. Encrypt M as the pair of integers $(C1, C2)$ where
$$C1 = \alpha^k \bmod q \text{ and } C2 = KM \bmod q$$

Decryption:

1. Recover the key by computing $K = (C1)^{X_A} \bmod q$
2. Compute $M = (C2 \cdot K^{-1}) \bmod q$

Ex: $q=19$ $\alpha = 10$

Key Generation:

1. Generate a random integer $X_A = 5$
2. Calculate Public Key $Y_A = \alpha^{X_A} \text{ mod } q$
 $= 10^5 \text{ mod } 19$
 $= 10^2 \text{ mod } 19 * 10^2 \text{ mod } 19 * 10 \text{ mod } 19$
 $= (5*5*10) \text{ mod } 19$
 $= 250 \text{ mod } 19$
 $= 3$
3. A's private key X_A and public key $[19, 10, 3]$

Encryption:

B wants to send the message with the value $M=17$ then

1. $M=17$
2. Choose a random integer k ; $k=6$
3. Compute a onetime key $K = (3)^6 \text{ mod } 19$
 $= 27 \text{ mod } 19 * 27 \text{ mod } 19$
 $= (8*8) \text{ mod } 19$
 $= 64 \text{ mod } 19$
 $= 7$
4. Encrypt M as the pair of integers $(C1, C2)$ where
 $C1 = \alpha^k \text{ mod } q$
 $= 10^6 \text{ mod } 19$
 $= 10^2 \text{ mod } 19 * 10^2 \text{ mod } 19 * 10^2 \text{ mod } 19$
 $= (5 * 5 * 5) \text{ mod } 19$
 $= (125) \text{ mod } 19$
 $= 11$
 $C2 = KM \text{ mod } q$
 $= (7 * 17) \text{ mod } 19$
 $= 119 \text{ mod } 19$
 $= 5$
5. B sends Cipher Text as $(11,5)$

Decryption:

1. Recover the key by computing $K = (C1)^{X_A} \text{ mod } q$

$$\begin{aligned} K &= (11)^5 \text{ mod } 19 \\ &= 11^2 \text{ mod } 19 * 11^2 \text{ mod } 19 * 11 \text{ mod } 19 \\ &= (7*7*11) \text{ mod } 19 \\ &= 7 \end{aligned}$$

2. Compute $M = (C2 k^{-1}) \text{ mod } q$

$$\begin{aligned} &= (5*11) \text{ mod } 19 [K^{-1} \text{ is } 7^{-1} \text{ mod } 19] \\ &= 55 \text{ mod } 19 \\ &= 17 \end{aligned}$$

$7^{-1} \text{ mod } 19$:

$$\equiv a^{m-2} \text{ mod } m$$

$$7^{-1} = 7^{17} \text{ mod } 19$$

$$= 11$$

Explain about Elliptic Curve Cryptography (ECC) with an example.

Elliptic curve systems as applied to cryptography were first proposed in 1985. ECC is an approach to public key cryptography based on algebraic structure of elliptic curves over finite fields.

Elliptic curve on a finite set of integers:

- Consider $y^2 = x^3 + 2x + 3 \text{ (mod } 5)$
 $x = 0 \Rightarrow y^2 = 3 \Rightarrow$ no solution (mod 5)
 $x = 1 \Rightarrow y^2 = 6 = 1 \Rightarrow y = 1,4 \text{ (mod } 5)$
 $x = 2 \Rightarrow y^2 = 15 = 0 \Rightarrow y = 0 \text{ (mod } 5)$
 $x = 3 \Rightarrow y^2 = 36 = 1 \Rightarrow y = 1,4 \text{ (mod } 5)$
 $x = 4 \Rightarrow y^2 = 75 = 0 \Rightarrow y = 0 \text{ (mod } 5)$
- Then points on the elliptic curve are
(1,1) (1,4) (2,0) (3,1) (3,4) (4,0) and the point at infinity: ∞

ECC is a public key cryptosystem just like RSA. Every user has a public key and a private key. Public key is used for encryption/signature verification and private key is used for decryption/signature generation. Elliptic curves are used as an extension to other current cryptosystems. They are;

- Elliptic curve Diffie-hellman key exchange

-
- Elliptic curve Digital signature algorithm

The central part of any cryptosystem involving elliptic curves is the **elliptic group**. All public-key cryptosystems have some underlying mathematical operation.

- RSA has exponentiation
- ECC has point multiplication

Procedure:

- Both parties agree to some publicly-known data items
 - The elliptic curve equation
 - values of a and b
 - prime, p
 - The elliptic group computed from the elliptic curve equation
 - A base point, B , taken from the elliptic group
 - Similar to the generator used in current cryptosystems
- Each user generates their public/private key pair
 - Private Key = an integer, x , selected from the interval $[1, p-1]$
 - Public Key = product, Q , of private key and base point
 - $(Q = x*B)$

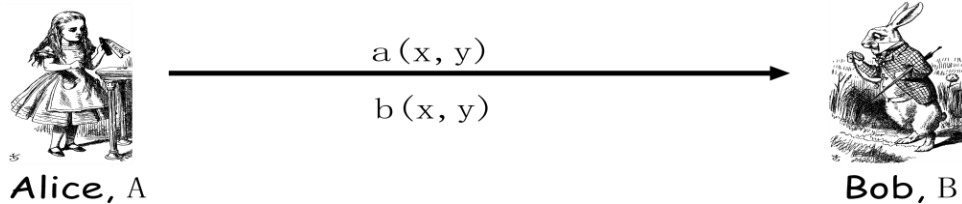
Ex:

- Suppose Alice wants to send to Bob an encrypted message.
 - Both agree on a base point, B .
 - Alice and Bob create public/private keys.
 - Alice
 - Private Key = a
 - Public Key = $P_A = a * B$
 - Bob
 - Private Key = b
 - Public Key = $P_B = b * B$
 - Alice takes plaintext message, M , and encodes it onto a point, P_M , from the elliptic group
 - Alice chooses another random integer, k from the interval $[1, p-1]$
 - The ciphertext is a pair of points
 - $P_C = [(kB), (P_M + kP_B)]$

- To decrypt, Bob computes the product of the first point from P_C and his private key, b
 - $b * (kB)$
- Bob then takes this product and subtracts it from the second point from P_C
 - $(P_M + kP_B) - [b(kB)] = P_M + k(bB) - b(kB) = P_M$
- Bob then decodes P_M to get the message, M .

ECC Diffie-Hellman Key Exchange:

- **Public:** Elliptic curve and point $B=(x,y)$ on curve
- **Secret:** Alice's a and Bob's b



Alice computes $a(b(x,y))$

- Bob computes $b(a(x,y))$
- These are the same since $ab = ba$
- Alice and Bob want to agree on a shared key.
 - Alice and Bob compute their public and private keys.
 - Alice
 - Private Key = a
 - Public Key = $P_A = a * B$
 - Bob
 - Private Key = b
 - Public Key = $P_B = b * B$
 - Alice and Bob send each other their public keys.
 - Both take the product of their private key and the other user's public key.
 - Alice $\rightarrow K_{AB} = a(bB)$
 - Bob $\rightarrow K_{AB} = b(aB)$
 - **Shared Secret Key = $K_{AB} = abB$**

Security:

- To **protect** a 128 bit AES key it would take a:
 - RSA Key Size: 3072 bits

-
- ECC Key Size: 256 bits
 - How do we strengthen RSA?
 - Increase the key length

NIST guidelines for public key sizes for AES			
ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Supplied by NIST to ANSI X9FT

1. WHAT IS MEANT BY PUBLIC KEY CRYPTOGRAPHY? WHAT ARE THE PRINCIPLES OF PUBLIC KEY CRYPTOSYSTEMS?
2. EXPLAIN ABOUT RSA ALGORITHM WITH AN EXAMPLE.
3. BRIEFLY EXPLAIN ABOUT DIFFIE-HELLMAN KEY EXCHANGE.
4. BRIEFLY EXPLAIN ABOUT ELLIPTIC CURVE CRYPTOGRAPHY.
5. WHAT ARE THE APPLICATIONS OF PUBLIC KEY CRYPTOSYSTEMS?

UNIT – IV

CRYPTOGRAPHIC HASH FUNCTIONS & DIGITAL SIGNATURES

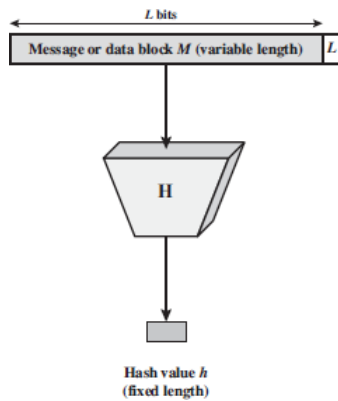
OBJECTIVES: PRESENT OVERVIEW OF THE BASIC STRUCTURE OF THE CRYPTOGRAPHIC FUNCTIONS. MESSAGE AUTHENTICATION CODES, UNDERSTAND THE OPERATION OF SHA-512, HMAC, DIGITAL SIGNATURES.

APPLICATIONS OF CRYPTOGRAPHIC HASH FUNCTIONS, REQUIREMENTS & SECURITY, SECURE HASH ALGORITHM, MESSAGE AUTHENTICATION FUNCTIONS, REQUIREMENTS & SECURITY, HMAC & CMAC, DIGITAL SIGNATURES, NIST DIGITAL SIGNATURE ALGORITHM, KEY MANAGEMENT & DISTRIBUTION.

WHAT IS A HASH FUNCTION? WHAT ARE VARIOUS APPLICATIONS OF HASH FUNCTIONS?

EXPLAIN.

A hash function maps a variable length message into a fixed length hash value. This value is also called as message digest.



APPLICATIONS OF CRYPTOGRAPHIC HASH FUNCTIONS:

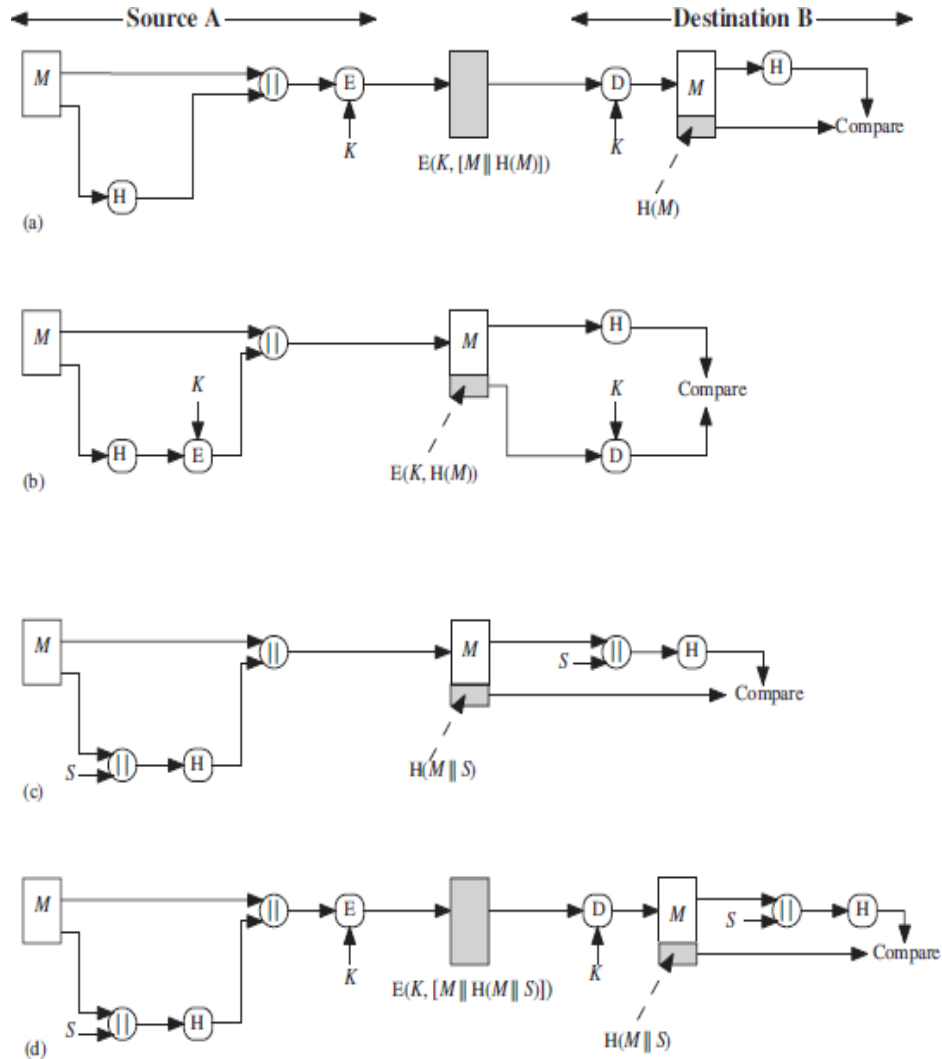
Cryptographic hash functions are used in a variety of security applications and Internet protocols. The following are the applications of hash functions.

1. **Message Authentication:** Message authentication is a service which is used to verify the integrity of the message. It assures that the data received are exactly as sent. When a hash function provides message authentication, the hash function value is called as **message digest**.
 - a. In this the message is concatenated with hash code and is encrypted using symmetric encryption.
 - b. In this only the hash code is encrypted. It reduces the processing burden.
 - c. In this the hash code is concatenated but not encrypted. This is used only for message authentication. It assumes that the two communicating parties can

CRYPTOGRAPHY AND NETWORK SECURITY – UNIT IV

share a secret value S . A computes the hash value over the concatenation of M and S and appends the result to M , because B possess S , it can recomputed the hash value to verify. Because the secret value itself is not sent, an opponent cannot modify an intercepted message and cannot generate a false message.

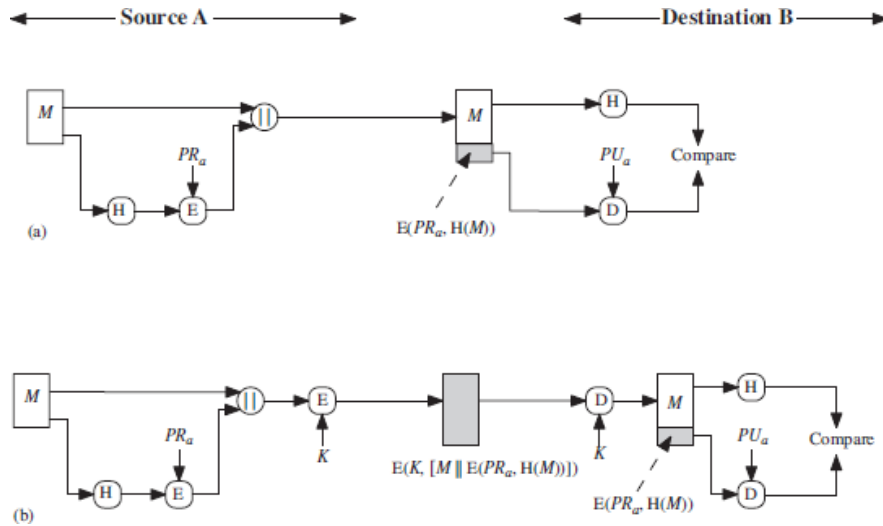
- d. Confidentiality can be added to the approach of method (c) by encrypting the entire message plus the hash code.



2. **Digital signatures:** The operations of digital signature are similar to MAC. In this case the hash value of the message is encrypted with the user's private key. Anyone who knows the user's public key can verify the integrity of the message that is

CRYPTOGRAPHY AND NETWORK SECURITY – UNIT IV

associated with the digital signature. In this case the attacker who wishes to alter the message would need to know the user's private key.



- a. The hash code is encrypted using public key encryption with the sender's private key. It provides authentication because only the sender could have produced the encrypted hash code.
- b. If confidentiality as well as authentication is needed then the message plus the private key encrypted hash code can be encrypted using a symmetric secret key.

3. **Other applications:** Hash functions are commonly used to create a one-way password file. In this a hash of a password file is stored by an OS rather than the password itself. So the actual password is not retrieved by a hacker who gains access to the password file.

EXPLAIN ABOUT SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC HASH FUNCTIONS.

REQUIREMENT	DESCRIPTION
Variable input size	H can be applied to a block of data of any size
Fixed output size	H produced a fixed-length output
Efficiency	H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical
Preimage resistant	For any given hash value h, it is computationally infeasible to find y such that H(y)= h

CRYPTOGRAPHY AND NETWORK SECURITY – UNIT IV

Second Preimage resistant	For any given block x , it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$
Collision resistant	It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$
Pseudo-randomness	Output of H meets standard tests for pseudo-randomness.

EXPLAIN ABOUT SECURE HASH ALGORITHM. (SHA-512)

This is also known as SHA. SHA was developed by National Institute of Standards and Technology and published as a Federal Information Processing Standard (FIPS) in 1993. The initial version of SHA is known as SHA-0. The revised version of SHA-0 is SHA-1. SHA-1 produces a hash value of 160 bits. NIST adds 3 additional versions of SHA i.e. SHA-256, SHA- 384 and SHA-512. These are designed for compatibility with increased security provided by the AES cipher. All versions structure and detail is similar to SHA-1 but security levels are rather higher.

Algorithm:

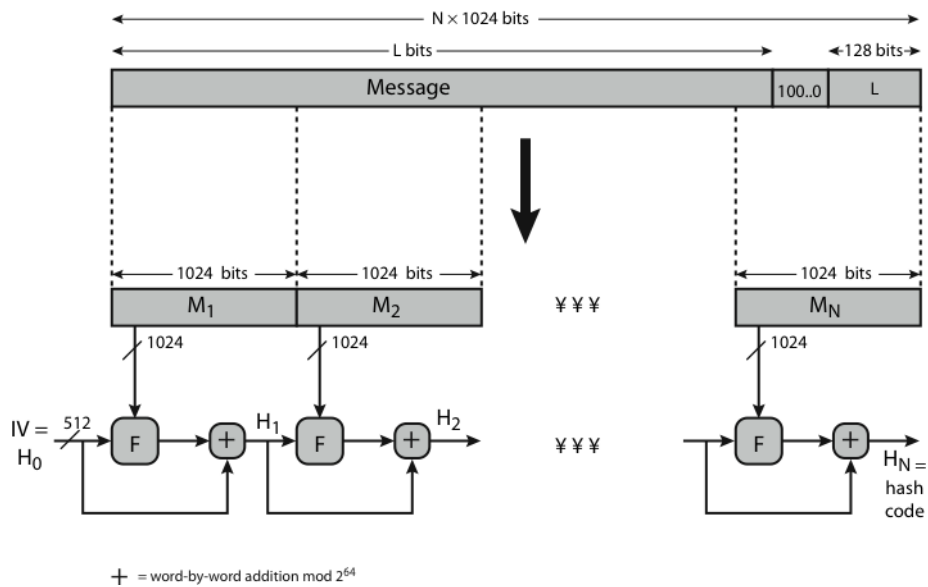


Table 11.3 Comparison of SHA Parameters

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest Size	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
Number of Steps	80	64	64	80	80

Note: All sizes are measured in bits.

This algorithm takes an input message with a maximum length of less than 2^{128} bits and produces 512-bit message digest. The input will be divided into 1024-bit blocks for processing of message to produce the digest. The steps are as follows;

STEP 1:

Append padding bits: Message is padded with a 1 and as many 0's as necessary to bring the message length to 896 congruent modulo 1024.

STEP 2:

Append Length: A block of 128-bits is appended to the message, treated as an unsigned 128-bit integer and it contains the length of the original message. The output of these steps produces a message of integer multiple of 1024 bits length.

STEP 3:

Initialize hash buffer: A 512-bit buffer is used to store intermediate and final results of the hash function. The buffer is represented as eight 64-bit (a, b, c, d, e, f, g, h) registers. These registers are initialized as follows and these values are stored in big-endian format.

a = 6A09E667F3BCC908 e = 510E527FADE682D1
 b = BB67AE8584CAA73B f = 9B05688C2B3E6C1F
 c = 3C6EF372FE94F82B g = 1F83D9ABFB41BD6B
 d = A54FF53A5F1D36F1 h = 5BE0CD19137E2179

STEP 4:

Process message in 1024-bit (128words) blocks: This message will be processed in 80 rounds.

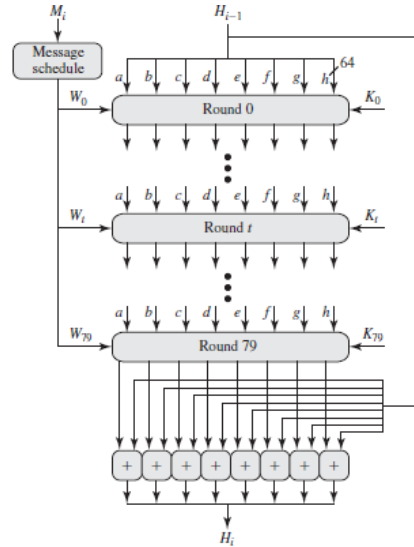


Figure 11.9 SHA-512 Processing of a Single 1024-Bit Block

- Each round takes the input from the buffer value and updates the contents of the buffer.
- In first round the buffers has the value of intermediate hash value.
- Each round makes use of a 64-bit value \$W_t\$ derived from the current 1024 bit block being processed.
- In each round an additive constant \$K_i\$ is used. The constants provide a randomized set of 64-bit patterns. These constants are predefined.
- The output of the eighth round is added to the input of the first round to produce \$H_i\$.

STEP 5:

Output: After all \$N \times 1024\$ blocks have been processed, the output from the \$N\$th stage is the 512-bit message digest.

$$H_0 = IV$$

$$H_i = \text{SUM}_{64}(H_{i-1}, abcdefghi)$$

$$MD = H_N$$

Where,

IV = Initial value of the buffers

abcdefghi = the output of the last round of processing of the \$i^{\text{th}}\$ message block

N = the number of blocks in the message

SUM₆₄ = addition modulo \$2^{64}\$ performed separately on each word of the pair of inputs

MD = final message digest value

WHAT ARE VARIOUS REQUIREMENTS OF MESSAGE AUTHENTICATION?

Message authentication is a mechanism used to verify the integrity of a message. A message authentication code (MAC) is an algorithm that requires the use of a secret key. A MAC takes a variable length message and a secret key as input and produces an authentication code. The receiver can generate MAC code by secret key is used to verify the integrity of the message.

MAC Requirements: While communications across the network the following attacks may be possible.

- **Disclosure:** It means the release of message contents to any person.
- **Traffic Analysis:** It means the discovery of traffic between parties. In connection oriented application, the frequency and duration of connections could be determined. In either connection oriented or connection less environment, the number and the length of messages between parties could be determined.
- **Masquerade:** It means the messages can come from the fraudulent source. It also includes fraudulent acknowledgement.
- **Content Modification:** It means the changes to the contents of the message.
- **Sequence Modification:** It means modification of sequence of messages between parties.
- **Timing Modification:** It means delay or replay of messages.
- **Source Repudiation:** It means the denial of message by source.
- **Destination Repudiation:** It means the denial of message by destination.

MAC deals with the attacks like masquerade, content modification, sequence modification, timing modification. Digital signature is an authentication technique that includes measures to counter repudiation by the source.

EXPLAIN ABOUT MESSAGE AUTHENTICATION FUNCTIONS.

Any message authentication or digital signature mechanism has two levels of functionality. At lower level, a function produces a value to be used to authenticate the message by the sender. At higher level this lower level value will be used to verify the authenticity of the message by the receiver. The functions can be grouped into three classes. They are;

Hash Function:

Hash function will takes a variable length message as input and produces a fixed length hash value, which serves as the authenticator. These are used for message authentication.

Message Encryption:

The cipher text of the entire message serves as its authenticator. It will provide measure of authentication. Message encryption schemes will be symmetric and public key encryption schemes.

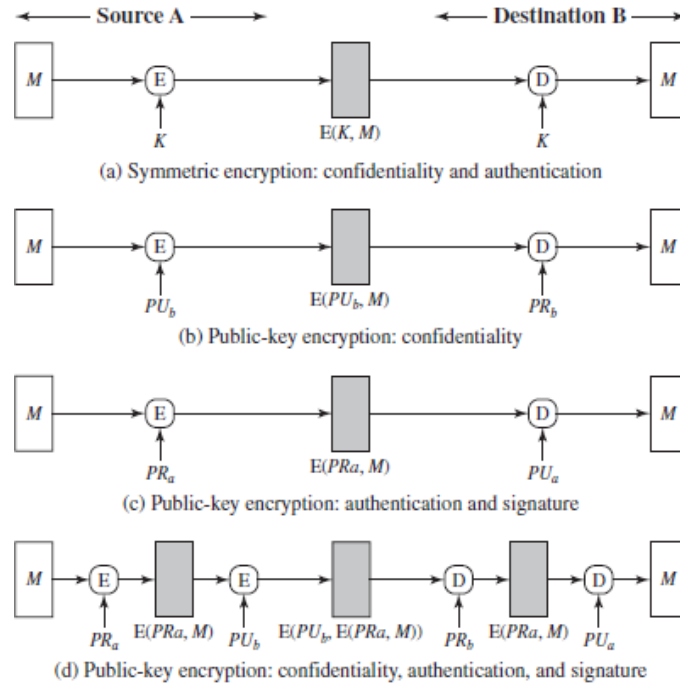


Figure 12.1 Basic Uses of Message Encryption

Message Authentication Code:

MAC function will takes a variable length message and secret key as input and produces a fixed length hash value, which serves as the authenticator. This is also known as **Cryptographic checksum.**

$$MAC = MAC(K, M)$$

Where,

M = Input message

K = Secret key

MAC = Message authentication code

The MAC is transmitted to the intended recipient. The receiver performs the same calculation on the received message, using the same secret key. It will generate a new MAC. This code is compared with the old MAC. If both are equal then,

- The receiver is assured that the message has not been altered.

CRYPTOGRAPHY AND NETWORK SECURITY – UNIT IV

- The receiver is assured that the message has been from the alleged sender because no one else knows the secret key to prepare the message.
- If the message includes a sequence number then the receiver can be assured of the proper sequence because attacker cannot successfully alter the sequence number.

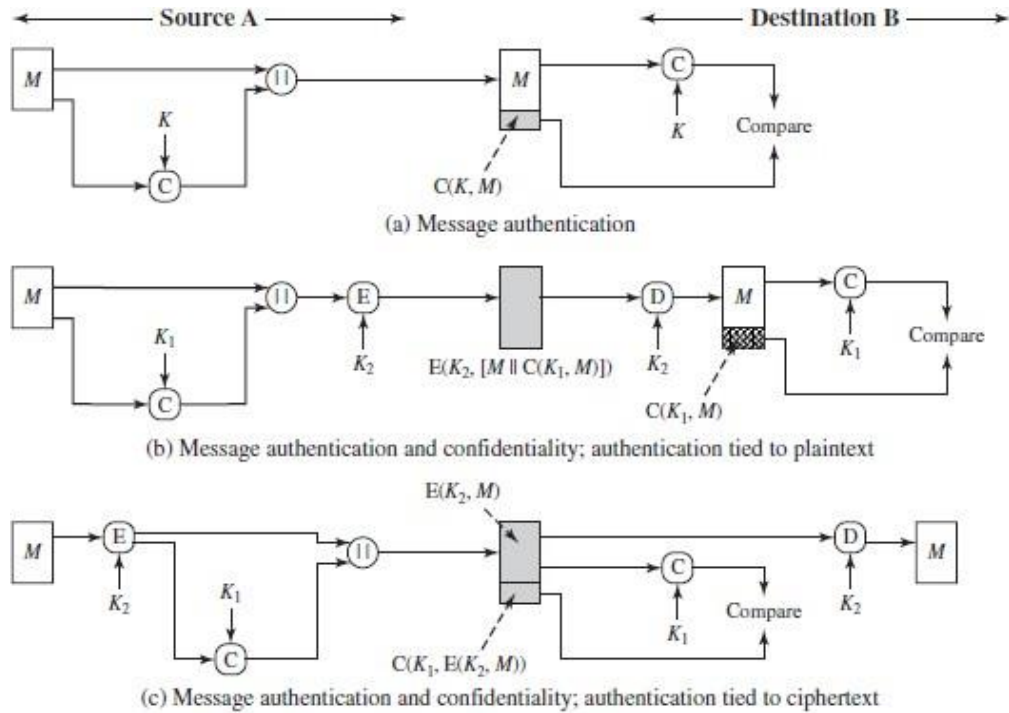


Figure 12.4 Basic Uses of Message Authentication code (MAC)

MAC is similar to encryption but the difference is MAC algorithm need not be reversible.

- Figure (a) will provide message authentication but not confidentiality.
- Figure (b) will provide message authentication and confidentiality and authentication will be tied with plaintext.
- Figure (c) will provide message authentication and confidentiality and authentication will be tied with cipher text.

Explain about MAC based Hash functions. (HMAC)

HMAC means MAC based on Hash Functions. In traditional approach MAC is based on the use of a symmetric block cipher. In recent years MAC is derived from a cryptographic hash function. Motivation for hash based MAC's are as follows;

- Hash functions such as MD5 and SHA-1 are generally faster than DES
- Crypto hash function code is widely available

SHA is not relying on the secret key. HMAC incorporates secret key into an existing hash algorithm.

HMAC Design objectives:

- Available hash functions will be used without any modification
- To preserve the original performance of hash function
- To use and handle keys in a simple way
- To have well understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions about the embedded hash function.

Algorithm:

The following figure shows the overall operation of HMAC.

H = embedded hash function such as MD5 or SHA-1

IV = initial value input to hashfunction

M = message input to HMAC

Y_i = ith block of M

L = number of block in M

b = number of bits in a block

n = length of hash code produced by embedded hash function

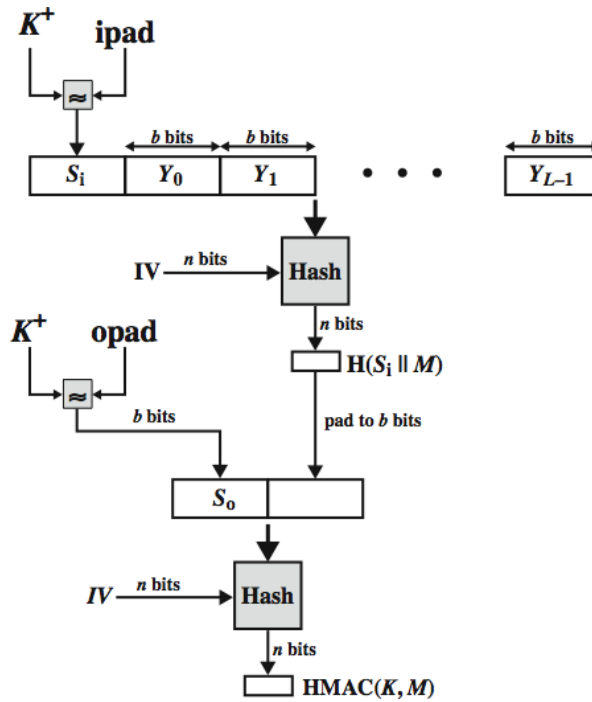
K = secret key

K⁺ = k padded with zeros on the left so that the result is b bits in length

ipad = 00110110 repeated b/8 times

opad = 01011100 repeated b/8 times

HMAC Structure:



HMAC can be expressed as;

$$HMAC(K, M) = H[(K^+ \oplus opad) || H[(K^+ \oplus ipad) || M]]$$

1. Append zeros to the left and of of K to create a b -bit string K^+ .
2. XOR K^+ WITH $IPAD$ TO PRODUCE THE B -BIT BLOCK S_i .
3. Append M to S_i .
4. Apply H to the stream generated in step 3.
5. XOR with $opad$ to produce the b -bit block .
6. Append the hash result from step 4 to .
7. Apply H to the stream generated in step 6 and output the result.

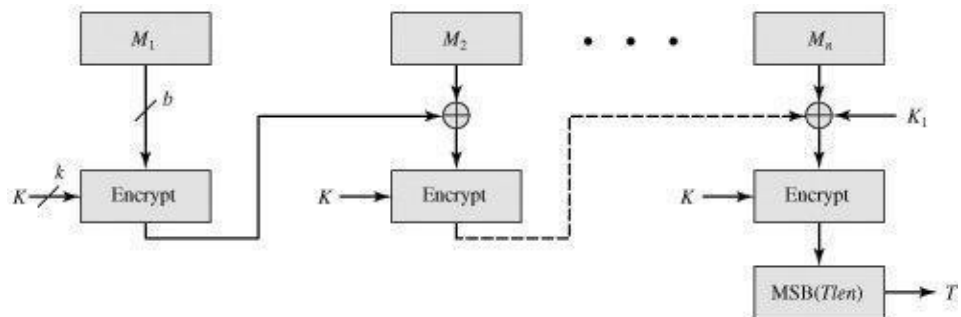
Explain about CMAC. (Cipher-based Message Authentication Code)

CMAC is a tool for calculating MAC using a block cipher couple with a secret key. CMAC is used to verify both the integrity and authenticity of a message. CMAC operation is used with AES and TDES.

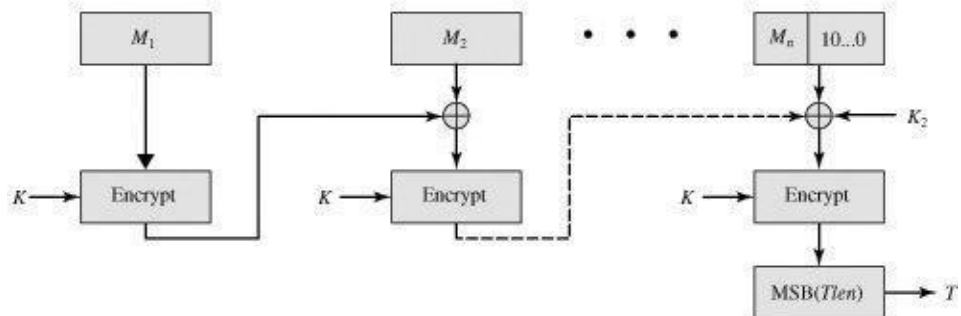
Operation of CMAC:

- Message is an integer multiple of n of the cipher block length b.
- For AES b= 128 and TDES b = 64.
- The message is divided into n blocks (M1, M2, ...,Mn).

The algorithm uses a k-bit encryption key and an n bit constant K1. For AES key size k is 128, 192 or 256 bits and TDES the key size is 112 or 128 bits. CMAC is calculated as follows;



(a) Message length is integer multiple of block size



(b) Message length is not integer multiple of block size

$$C1 = E(K, M1)$$

$$C2 = E(K, [M2 \text{ XOR } C1])$$

$$C2 = E(K, [M3 \text{ XOR } C2])$$

•

•

•

•

•

$$CN = E(K, [Mn \text{ XOR } Cn-1])$$

$$T = \text{MSB}(\text{Tlen}(C_n))$$

Where,

T = message authentication code

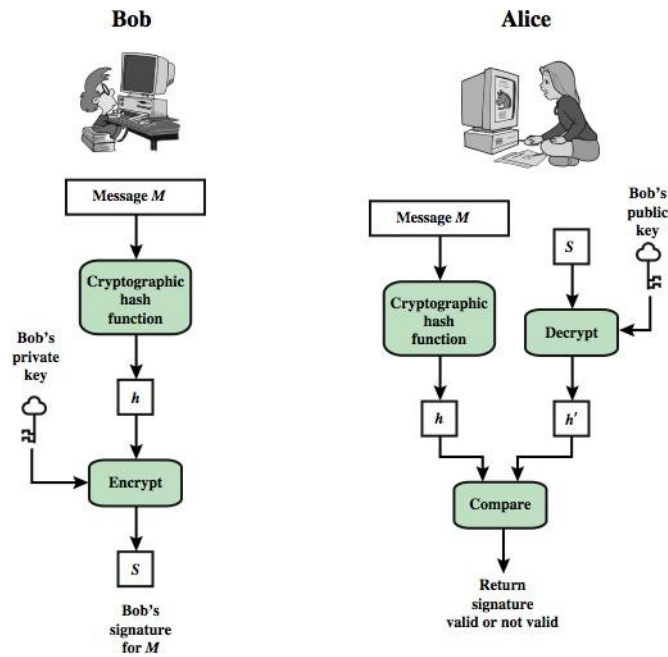
Tlen = bit length of T

MSBs(X) = the s leftmost bits of the bit string X

If the message is not an integer multiple of the cipher block length, then the final block is padded to the right with a 1 and as many as 0s as necessary so that the final block is also of length of b.

WRITE ABOUT DIGITAL SIGNATURES.

A digital signature is an authentication mechanism that enables the sender to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the sender's private key. This signature guarantees the integrity of the sender. For this DSS (Digital Signature Standard) algorithm is used.



Message authentication protects sender and receiver who exchange messages from any third party but it does not protect sender and receiver from each other.

Digital Signature Properties:

- It must verify the author, date and time of the signature
- It must authenticate the contents at the time of the signature
- It must be verifiable by third parties, to resolve disputes

Digital Signature Requirements:

On the basis of properties and for the purpose of denying the attacks, the following requirements are needed for a digital signature.

- The signature must be a bit pattern that depends on the message
- The signature must use some information unique to the sender to prevent forgery and deny
- Must be easy to produce the digital signature
- Must be easy to recognize and verify the digital signature
- Must be computationally infeasible to forge a digital signature
- Must be practical to retain a copy of the digital signature in storage

Direct Digital Signature:

Direct digital signature scheme involves only the communicating parties. Message and signature can be encrypted by using symmetric encryption provides confidentiality.

EXPLAIN ABOUT VARIOUS DIGITAL SIGNATURE SCHEMES.

ELGAMAL DIGITAL SIGNATURE SCHEME:

This scheme requires a prime number and primitive root for that prime number. User A generates key pair as follows;

- Choose a prime number p
- Choose a primitive root for p i.e. α
- Generate a random integer X_A such that $1 < X_A < q-1$
- Compute $Y_A = \alpha^{X_A} \text{ mod } q$
- A's private key is X_A and public key is $[q, \alpha, Y_A]$

For signing a message A first computes the hash $m = H(m)$ such that m is an integer in the range $0 \leq m \leq q-1$. A then forms a digital signature as follows;

1. Choose a random integer K such that $1 \leq K \leq q-1$ and $\text{gcd}(K, q-1) = 1$
2. Compute $S_1 = \alpha^K \text{ mod } q$
3. Compute $K^{-1} \text{ mod } (q-1)$
4. Compute $S_2 = \alpha^{K^{-1}(m - X_A S_1)} \text{ mod } (q-1)$
5. The signature consists of the pair (S_1, S_2)

Any user B can verify the signature as follows.

1. Compute $V_1 = a^m \text{ mod } q$
2. Compute $V_2 = (Y_a)^{S_1} (S_1)^2 \text{ mod } q$

The signature is valid if $V_1 = V_2$.

For example, let us start with the prime field $GF(19)$; that is, $q = 19$. It has primitive roots $\{2, 3, 10, 13, 14, 15\}$, primitive root as 10.

Alice generates a key pair as follows:

1. Alice chooses $X_A = 16$
2. Then $Y_A = \alpha^{X_A} \text{ mod } q = 10^{16} \text{ mod } 19 = 4$
3. Alice's private key is 16; Alice's public key is $[19, 10, 4]$

Suppose Bob wants to sign a message with hash value $m=14$.

1. Bob choose $K=5$, which is relatively prime to $q-1= 18$
2. $S_1 = a^K \text{ mod } q = 10^5 \text{ mod } 19 = 3$
3. Compute $K^{-1} \text{ mod } (q-1) = 5^{-1} \text{ mod } 18 = 11$
4. Compute $S_2 = a^{K^{-1} (m - X_A S_1)} \text{ mod } (q - 1) = 11(14 - (16)(3)) \text{ mod } 18 = -374 \text{ mod } 18 = 4$

Alice can verify the signature as follows;

1. Compute $V_1 = a^m \text{ mod } q = 10^{14} \text{ mod } 19 = 16$
2. Compute $V_2 = (Y_a)^{S_1} (S_1)^{S_2} \text{ mod } q = (4)^3 (3)^4 \text{ mod } 19 = 5184 \text{ mod } 19 = 16$

So the signature is valid

SCHNORR DIGITAL SIGNATURE SCHEME:

This scheme is based on discrete logarithms. In this signature generation is not depended on the message and it can be done during the idle time of the processor. The generation of key pair is as follows;

1. Choose primes p and q , such that q is a prime factor of $p-1$
2. Choose an integer a , such that $a^q = 1 \pmod p$. The values a , p and q comprise a global public key that can be common to a group of users.
3. Choose a random integer s with $0 < s < q$. This will be used as private key.
4. Calculate $v = a^{-1} \pmod p$. This is used as public key.

A user with private key s and public key v generates a signature as follows;

1. Choose a random integer r with $0 < r < q$ and compute $x = a^r \pmod p$. This computation is a preprocessing stage independent of the message M to be signed.
2. Concatenate the message with and hash the result to compute the value e :
$$e = H(M || x)$$
3. Compute $y = (r + se) \pmod q$. The signature consists of the pair (e, y) .

Any other user can verify the signature as follows;

1. Compute $X' = a^y v^e \pmod p$.
2. Verity that $e = H(M || X')$

EXPLAIN ABOUT DIGITAL SIGNATURE ALGORITHMS.

NIST Digital Signature Algorithm:

The National Institute of Standards and Technology has published Federal Information Processing Standards FIPS 186 is also known as Digital Signature Standard. DSS uses Secure Hash Algorithm (SHA).

The DSA Approach

This algorithm provides only digital signature function.

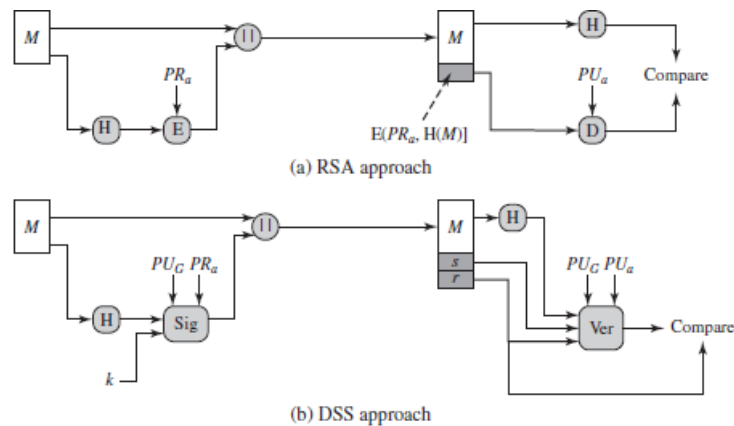


Figure 13.3 Two Approaches to Digital Signatures

(a) RSA Approach:

- The message to be signed is the input to the hash function. Hash function generates hash code and then the hash code is encrypted with the private key of the sender to form the signature. Then both the message and signature is transmitted.
- The receiver takes the message and produces hash code and then decrypts the signature received from the sender by using sender's public key. If both signatures are matched then the signature is valid and message is accepted otherwise it is rejected.

(b) DSA Approach:

- The hash code is provided as input to a signature function along with a random number generated for this particular signature. The signature function depends on the sender's private key and a set of parameters. The resultant signature consists of two components labeled as s and r .
- At the receiver end the hash code of the incoming message is generated. The hash code and the signature are inputs to a verification function. The verification function depends on global public key as well as the sender's

public key. The output of the verification function is the value that is equal to the signature component r if the signature is valid.

Algorithm:

(a) Global Public Key Components:

P - Prime number in between $512 \leq L \leq 1024$ and L is multiple of 64 bits and in between 512 and 1024 bits.

Q - Prime divisor of $(p - 1)$

$G = h(p-1) / q$, h is any integer with $1 < h < (p-1)$

(b) User's Private Key:

X random number with $0 < x < q$

(c) User's Public Key:

$Y = g^x \text{ mod } p$

(d) User's Per Message Secret Number:

K random number with $0 < k < q$

(e) Signing:

$r = (g^k \text{ mod } p) \text{ mod } q$

$s = [k^{-1}(H(M) + xr)] \text{ mod } q$

Signature = (r, s)

(f) Verifying:

$W = (s^{-1}) \text{ mod } q$

$U1 = [H(M')w] \text{ mod } q$

$U2 = (r') w \text{ mod } q$

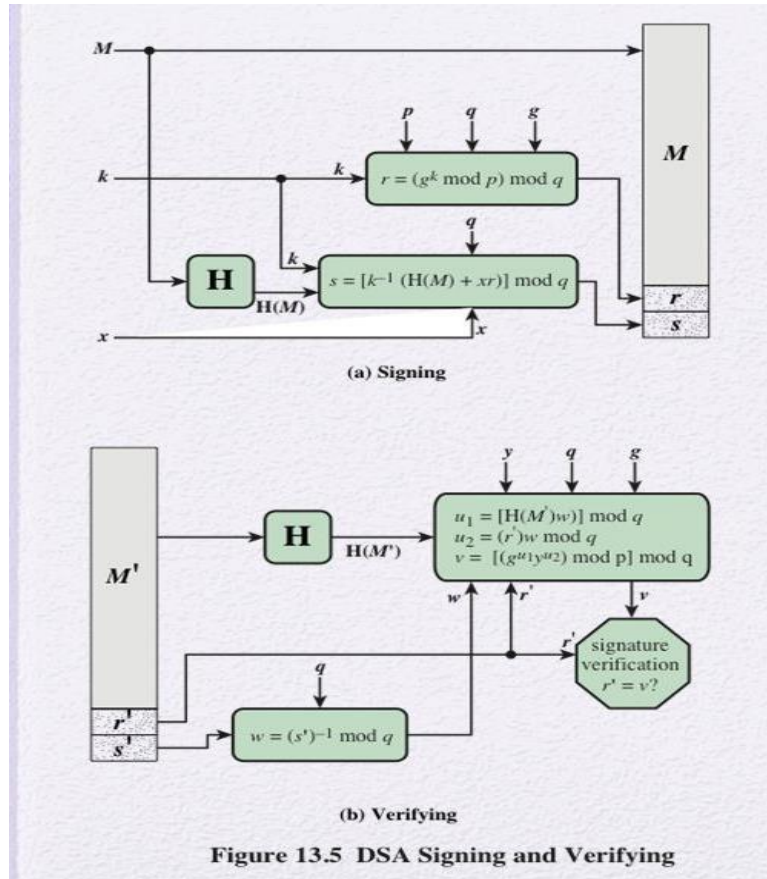
$V = [g^{u1}y^{u2} \text{ mod } p] \text{ mod } q$

TEST: $v = r'$

Digital Signature Algorithm: (DSA)

DSA is based on the difficulty of computing discrete logarithms.

1. Choose a random primer number q .
2. Choose another prime number p with a length in between 512 and 1024 bits such that q divides $(p-1)$.
3. Choose $g = h^{(p-1)/r} \text{ mod } p$, where h is in between 1 and $(p-1)$ and $g > 1$.
4. Choose the private key x must be number from 1 to $(q-1)$.
5. Calculate public key $y = g^x \text{ mod } p$.



- The signature of the message M consists of the pair of numbers r and s, which are the functions of public key components (p, q, g) and the private key(x), the hash code H(M) and an additional integer k.
- M, r', s' are the received versions of M, r, s respectively.

Elliptic Curve Digital Signature Algorithm:

Global Parameters:

- Q Prime Number
- A, b Integers defined over an equation $y^2 = x^3 + ax + b$
- G A base point
- N Order of point G

Key Generation:

1. Select a random integer d, $1 \leq d \leq n-1$ (private key)
2. Compute $Q = dG$ (public key)

Digital Signature Generation:

1. Select a random number k
2. Compute point $P=(x, y) = kG$ and $r = x \bmod n$
3. Compute $t = k^{-1} \bmod n$
4. Compute $e = H(m)$
5. Compute $s = k^{-1}(e+dr)$
6. The signature of message m is the pair (r,s)

EXPLAIN ABOUT KEY MANAGEMENT AND DISTRIBUTION.

Key distribution means to deliver a key in between two parties who wish to exchange the encrypted data securely. Keys are distributed in the following ways;

1. Symmetric key distribution using **symmetric encryption**
2. Asymmetric key distribution using **asymmetric encryption**

Symmetric key distribution using symmetric encryption

In symmetric encryption the two parties can exchange and must share the same key and that key must be protected from others. The keys are frequently changed to limit the amount of data compromised if an attacker learns the key. The strength of any cryptographic system rests with the key distribution technique. For two parties A and B, can be achieved the key distribution in a number of ways, as follows:

1. A can select a key and physically deliver it to B.
2. A third party can select the key and physically deliver it to A and B.
3. If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
4. If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

Symmetric key distribution using asymmetric encryption

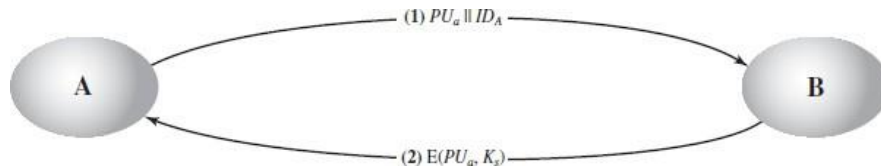
Public key cryptosystem's one of the important use is encrypting the secret keys for distribution. The following are the general principles and approaches.

Simple Secret Key Distribution:

If A wishes to communicate with B, the procedure is as follows;

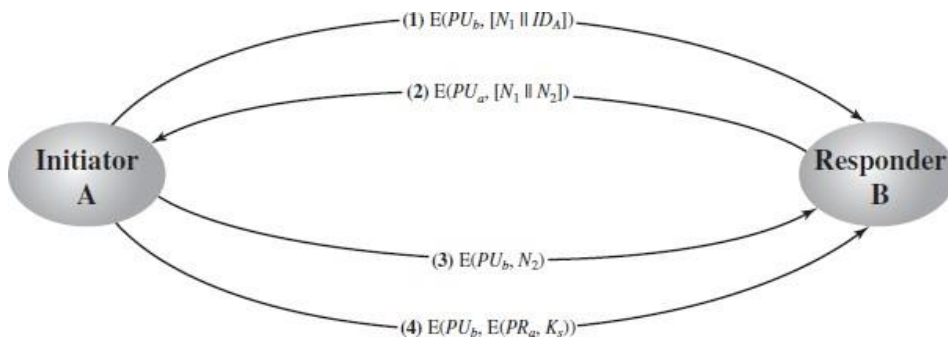
- A generates a public/private key pair and transmits a message to B consisting of PU_A and an identifier of A, ID_A .
- B generates a secret key K_s and transmits to A, which is encrypted with A's public key.
- A decrypts K_s to recover the secret key.
- A discards PU_A and PR_A and B discards PU_A .

A and B can now securely communicate using conventional encryption and the session key K_s . After completing the exchange both A and B discards K_s . This scheme is vulnerable to man-in-middle attack.



Secret key distribution with confidentiality and authentication:

This method provides protection against both active and passive attacks.



- A uses B's public key to encrypt a message to B containing an identifier of A and a nonce which is used to identify the identity of the current transaction.

CRYPTOGRAPHY AND NETWORK SECURITY – UNIT IV

- B sends a message to A encrypted with PU_a and containing A's nonce as well as a new nonce generated by B.
- A returns B's nonce encrypted using B's public key for assuring that it came from A.
- A selects a secret key K_s and sends $M = E(Pub, E(PR_a, K_s))$ to B.
- B computes $D(PU_a, D(PR_b, M))$ to recover the secret key.

Distribution of public keys:

The following are the various techniques for distributing public keys.

1. Public announcement
2. Publicly available directory
3. Public key authority
4. Public key certificates

PUBLIC ANNOUNCEMENT OF PUBLIC KEYS Here any participant can send his or her public key to any other participant or broadcast the key to the community at large. For example, many PGP users have adopted the practice of appending their public key to messages that they send to public forums.



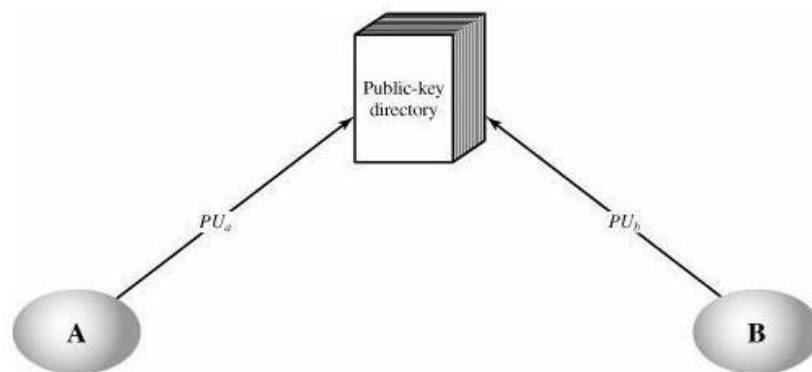
Drawbacks:

- Anyone can forge such a public announcement. Some user could pretend to be user A and send a public key to another participant or broadcast such a public key.
- Until the time when A discovers about the forgery and alerts other participants, the forger is able to read all encrypted messages intended for A and can use the forged keys for authentication.

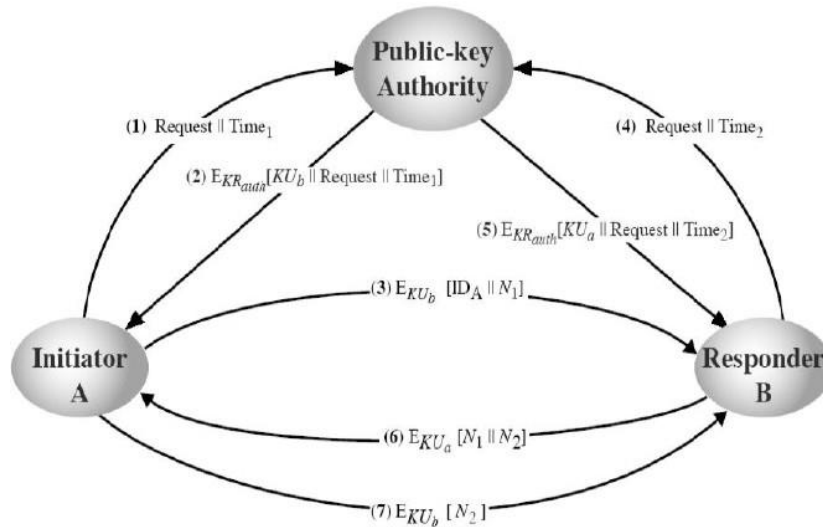
PUBLICLY AVAILABLE DIRECTORY A greater degree of security can be achieved by maintaining a publicly available dynamic directory of public keys. Maintenance and distribution of the public directory would have to be the responsibility of some trusted entity or organization. It includes the following elements:

CRYPTOGRAPHY AND NETWORK SECURITY – UNIT IV

1. The authority maintains a directory with a {name, public key} entry for each participant.
2. Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication.
3. A participant may replace the existing key with a new one at any time, either because of the desire to replace a public key that has already been used for a large amount of data, or because the corresponding private key has been compromised in some way.
4. Participants could also access the directory electronically. For this purpose, secure, authenticated communication from the authority to the participant is mandatory.



PUBLIC-KEY AUTHORITY Stronger security for public-key distribution can be achieved by providing tighter control over the distribution of public keys from the directory. This scenario assumes the existence of a public authority (whoever that may be) that maintains a dynamic directory of public keys of all users. The public authority has its own (private key, public key) that it is using to communicate to users. Each participant reliably knows a public key for the authority, with only the authority knowing the corresponding private key. For example, consider that Alice and Bob wish to communicate with each other and the following steps take place and are also shown in the figure below:

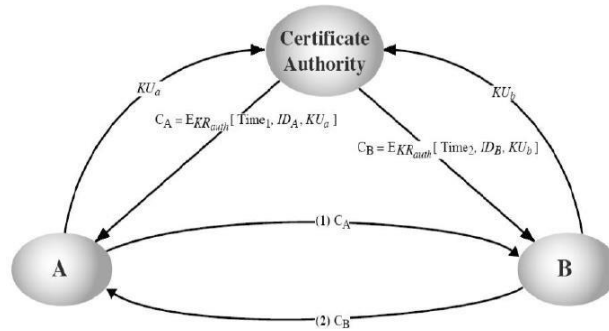


1. Alice sends a **timestamped** message to the central authority with a request for Bob's public key (the time stamp is to mark the moment of the request)
2. The authority sends back a message encrypted with its private key (for authentication) –message contains Bob's public key and the original message of Alice –this way Alice knows this is not a reply to an old request;
3. Alice starts the communication to Bob by sending him an encrypted message containing her identity IDA and a nonce N1 (to identify uniquely this transaction)
4. Bob requests Alice's public key in the same way (step 1)
5. Bob acquires Alice's public key in the same way as Alice did. (Step-2)
6. Bob replies to Alice by sending an encrypted message with N1 plus a new generated nonce N2 (to identify uniquely the transaction)
7. Alice replies once more encrypting Bob's nonce N2 to assure bob that its correspondent is Alice

PUBLIC-KEY CERTIFICATES

The above technique looks attractive, but still has some drawbacks. For any communication between any two users, the central authority must be consulted by both users to get the newest public keys i.e. the central authority must be online 24 hours/day. If the central authority goes offline, all secure communications get to a halt. This clearly leads to an undesirable bottleneck. A further improvement is to use certificates, which can be used to exchange keys without contacting a public-key authority. This certificate issuing scheme does have the following requirements:

1. Any participant can read a certificate to determine the name and public key of the certificate's owner.
2. Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
3. Only the certificate authority can create and update certificates.
4. Any participant can verify the currency of the certificate.



Explain about X.509 Directory Authentication Service.

X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. It also defines alternative authentication protocols based on the uses of public key certificates. This authentication service is based on public key cryptography and digital signatures.

Certificates:

Public key certificate with the associated user is the heart of the X.509 scheme. These user certificates are assumed to be created by some trusted certification authority and placed it in the directory by the CA or by the user.

- **Version:** It specifies the version of the certificate.
- **Serial number:** An integer value unique within the issuing CA associated with this certificate.
- **Signature algorithm identifier:** The algorithm used to sign the certificate together with any associated parameters
- **Issuer name:** X.500 is the name of the CA that created and signed this certificate.
- **Period of validity:** It consists of the validity period of the certificate.
- **Subject name:** The name of the user to whom this certificate refers.
- **Subject's public-key information:** The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.

- **Issuer unique identifier:** An optional-bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.
- **Subject unique identifier:** An optional-bit string field used to identify uniquely the subject in the event the X.500 name has been reused for different entities.
- **Extensions:** A set of one or more extension fields. Extensions were added in version 3.
- **Signature:** It contains the hash code of the other fields encrypted with the CA's private key. This field includes the signature algorithm identifier.

WRITE ABOUT PUBLIC KEY INFRASTRUCTURE. (PKI)

RFC 822 defines public key infrastructure (PKI) defines the set of hardware, software, people, policies and procedures needed to manage, store, distribute and revoke digital certificates based on asymmetric cryptography. The main objective of PKI is to enable secure, convenient and efficient acquisition of public keys. This model based on X.509 suitable for deploying a certificate based architecture on the Internet. It described PKIX model. The following figure shows the interrelationship between the key elements of the PKIX model. These elements are;

END ENTITY:

It denotes end users, devices or any other entity that can be identified in the subject field of public key certificate.

CERTIFICATION AUTHORITY (CA):

CA is the issuer of certificates and Certificate Revocation Lists (CRLs). It may support a variety of administrative functions and also assign to one or more Registration Authorities.

REGISTRATION AUTHORITY (RA):

This is associated with the end entity registration process but also assists a number of other areas.

CRL ISSUER:

An optional component that a CA can assign to public CRLs.

REPOSITORY:

This term denotes any method for storing certificates and CRLs so that it can be retrieved by End Entities.

IMPORTANT QUESTIONS

1. Give the structure of SHA-512 compression function. Explain the structure of each round. Is Man in the Middle attack possible on SHA-512.
2. Give the structure of HMAC and explain the applications of HMAC.
3. Write about HMAC algorithm. What need to be done to speed up HMAC algorithm?
4. Give the structure of CMAC.
5. Describe the process involved in digital signatures. Explain about various digital signature algorithms.
6. Write about Digital Signature Algorithm and also describe attacks on Digital Signatures.
7. Explain about key management and distribution.

UNIT - V

Objectives: Present an overview of techniques for remote user authentication, Kerberos, Summarize Web Security threats and Web Traffic security approaches, overview of SSL & TLS. Present an overview of electronic mail security.

User Authentication: Remote User Authentication Principles, Kerberos

Transport Layer Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Shell (SSH)

Electronic Mail Security: Pretty Good Privacy (PGP), S/MIME.

WHAT IS MEANT BY USER AUTHENTICATION? WHAT ARE THE PRINCIPLES OF REMOTE USER AUTHENTICATION?

User authentication is the process of verifying the identity of the claimed entity. This process consists of two steps.

- 1. Identification Step**
- 2. Verification Step**

NIST MODEL FOR ELECTRONIC USER AUTHENTICATION:

NIST defined a model for electronic user authentication for establishing confidence while electronic communication. The main requirement for performing user authentication is the user must register with the system. The process of e E-authentication model is as follows;

1. The user registered with Registration Authority (RA) to become a subscriber of Credential Service Provider (CSP). RA is a trusted third party.
2. The CSP issues some electronic credentials to the subscriber. The credential is a data structure that binds an identity and additional attributes to a token possessed by a subscriber and can be verified at the time of authenticating a transaction.
3. The token is an encrypted key which identifies the subscriber. The token may be issued by CSP or provided by trusted third party.

Once the user is registered as subscriber, the authentication process can take place between the subscriber and one or more systems that perform authentication. The party to be authenticated is called as **Claimant** and the party verifying that entity is called as **Verifier**.

Means of Authentication: There are four means of authenticating a user's identity, which can be alone or in combination:

1. Something the individual knows

Ex: Password, Personal Identification Number or answers to a pre arranged questions

2. Something the individual possesses

Ex: Cryptographic keys, electronic cards, smart cards, etc.

3. Something the individual is (static biometrics)

Ex: Fingerprint, retina, face recognition etc.

4. Something the individual does (dynamic biometrics)

Ex: Voice recognition, handwriting characteristics, typing rhythm, etc.

All the above methods properly implemented and used can provide user authentication.

Mutual Authentication:

Mutual authentication protocols enable communicating parties to satisfy themselves mutually about each user's identity and to exchange session keys. The main problem of authenticated key exchange is **confidentiality** and **timeliness**. To prevent masquerading and compromising the session keys the information must be in encrypted form. The second issue, timeliness is important because of the threat of message replays. To cope the replay attacks is to attach a sequence number to each message in an authenticated exchange. A new message is accepted only if its sequence number is in the proper order. The main difficulty is to keep track the sequence numbers. Because of this the sequence numbers are generally not used for authentication and key exchange. Instead of this the following approaches are used;

- 1. Timestamps:** Party A accepts a message as fresh only if the message contains a timestamp which is close enough to current time. In this synchronization of clocks are required. Because of the variable and unpredictable nature of network delays, distributed clocks cannot be synchronized.
- 2. Challenge/Response:** Party A expecting a fresh message from B, first sends B a nonce and requires that the subsequent message received from B contain the correct nonce value. This approach is unsuitable for a connectionless type of application, because it requires handshake, which exists only in connection oriented service.

One Way Authentication:

E-mail is one of the applications for which encryption is growing. In E-mail it is not necessary for the sender and receiver to be online at the same time. Instead, the e-mail message is forwards to the receiver's electronic mailbox, where it is buffered until the receiver is available to read it.

EXPLAIN ABOUT KERBEROS.

Kerberos is an authentication protocol which works on the basis of tickets to allow the users those who are communicating over a non-secure network. This protocol allows users to prove their identity to one another in a secure manner. Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos build on symmetric cryptography and requires a trusted third party.

Requirements:

- **Secure:** A network eavesdropper should not be able to impersonate a user.
- **Reliable:** Kerberos should be highly reliable and should employ distributed server architecture, with one system able to backup another.
- **Transparent:** Operations of Kerberos is transparent to user, beyond the requirement to enter a password.
- **Scalable:** The system is capable of supporting large number of clients and servers.

Kerberos version 4:

Kerberos version 4 makes use of DES for providing authentication service. Some aspects of this version are;

1. A Simple Authentication Dialogue
2. More Secure Authentication Dialogue
3. The Version 4 Authentication Dialogue

A Simple Authentication Dialogue

In an unprotected network a client can apply for any service, but the server needs to check whether the client is an authenticated client or not. If it will not do properly an opponent may gain access the services. It places an additional burden on the server. For this purpose an authentication server (AS) is used. The AS knows the passwords of all users and stores these in a centralized database. The AS also shares a unique secret key to each server. These keys have been distributed physically or in some other secure manner.

1. $C \rightarrow AS : ID_c || P_c || ID_v$
2. $AS \rightarrow C$ Ticket
3. $C \rightarrow V ID_c || Ticket$

Ticket = $E(K_v, ID_c || AD_c || ID_v)$

Where,

C = Client

AS = Authentication Server

V	=	Server
ID _c	=	Identifier of user on C
ID _v	=	Identifier of V
P _c	=	Password of user on C
AD _c	=	Network address of C
K _v	=	Secret encryption key shared by AS and V

- The client requests to access the server V
- The client module C in the workstation requests user name and password and then sends a message to the AS. It includes user's ID, server's ID and user's password
- The AS checks whether the user is allowed to access the server V or not
- The both tests are passed then AS creates a ticket, contains user ID and network address and the server ID
- This ticket is encrypted using the secret key that can be shared by the AS and this server
- This ticket is sent back to C. This ticket is encrypted and it is not altered by C or any other opponent
- By using this ticket C can apply V for a service. V decrypts the ticket and verifies the user ID in the ticket with the decrypted ticket. If both are same the user is allowed to access the requested service

More Secure Authentication Dialogue

The above scenario solves some of the problems of authentication in an open network environment and some problems remain. First, we would like to minimize the number of times that a user has to enter a password. The second problem in earlier scenario involved a plaintext transmission of the password. An eavesdropper could capture the password and use any service accessible to the victim. To solve these additional problems, we introduce a scheme for avoiding plaintext passwords and a new server, known as the **ticket-granting server** (TGS). The new scenario is as follows.

Once per user logon session:

1. C → AS ID_c || ID_{tgs}
2. AS → C E(K_c, Ticket_{tgs})

Once per type of service:

3. C → TGS ID_c || ID_v || Ticket_{tgs}
4. TGS → C Ticket_v

Once per service session:

$$5. C \rightarrow V \text{ ID}_c || \text{Ticket}_v$$

$$\text{Ticket}_{tgs} = E(K_{tgs}, [\text{ID}_c || \text{AD}_c || \text{ID}_{tgs} || \text{TS1} || \text{Lifetime1}])$$

$$\text{Ticket}_v = E(K_v, [\text{ID}_c || \text{AD}_c || \text{ID}_v || \text{TS2} || \text{Lifetime2}])$$

THE VERSION 4 AUTHENTICATION DIALOGUE:

Although the foregoing scenario enhances security compared to the first attempt, two additional problems remain. The heart of the first problem is the lifetime associated with the ticket-granting ticket. If this lifetime is very short, then the user will be repeatedly asked for a password. If the lifetime is long, then an opponent has a greater opportunity for replay.

So the additional requirement is that a network service must be able to prove that the person using a ticket is the same person to whom that ticket was issued.

The second problem is that there may be a requirement for servers to authenticate themselves to users.

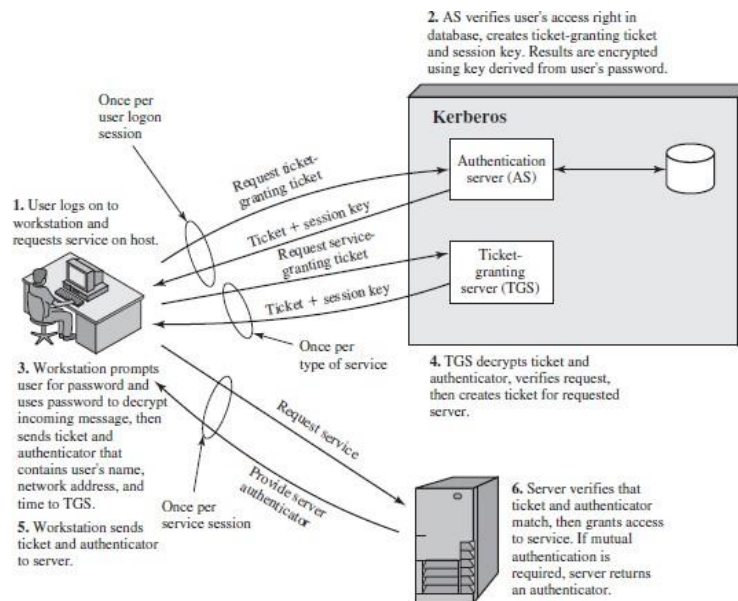


Figure 15.1 Overview of Kerberos

EXPLAIN ABOUT WEB SECURITY AND WEB SECURITY REQUIREMENTS.

The WWW is fundamentally a client/server application running over the Internet and TCP/IP intranets.

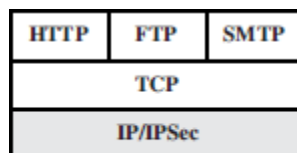
Web Security Threats:

The following table shows various threats to web security.

	Threats	Consequences	Countermeasures
Integrity	<ul style="list-style-type: none"> • Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit 	<ul style="list-style-type: none"> • Loss of information • Compromise of machine • Vulnerability to all other threats 	Cryptographic checksums
Confidentiality	<ul style="list-style-type: none"> • Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server 	<ul style="list-style-type: none"> • Loss of information • Loss of privacy 	Encryption, Web proxies
Denial of Service	<ul style="list-style-type: none"> • Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks 	<ul style="list-style-type: none"> • Disruptive • Annoying • Prevent user from getting work done 	Difficult to prevent
Authentication	<ul style="list-style-type: none"> • Impersonation of legitimate users • Data forgery 	<ul style="list-style-type: none"> • Misrepresentation of user • Belief that false information is valid 	Cryptographic techniques

Web Traffic Security Approaches:

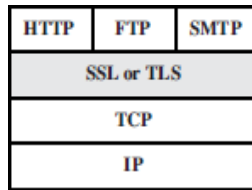
For web security number of approaches is possible. Web security is to use IPSecurity (IPSec). The advantage is that it is transparent to end users and applications and provides a general purpose solution. IPSec includes filtering capability so that only selected traffic need to be incur the overhead of IPSec processing.



(a) Network level

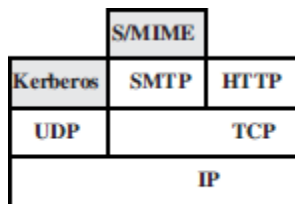
CRYPTOGRAPHY AND NETWORK SECURITY – UNIT V

Another solution is to implement security just above TCP. It is possible by using SSL or TLS, SSL means Secure Socket Layer and TLS means Transport Layer Security.



(b) Transport level

Application specific security services are also embedded within the particular applications also.



(c) Application level

EXPLAIN ABOUT SECURE SOCKET LAYER (SSL) WITH A NEAT DIAGRAM.

SSL was developed by Netscape.

SSL Architecture:

SSL is designed to provide reliable end to end secure service to make use of TCP. It is not a single protocol but rather two layers of protocols. SSL record protocol provides basic security services to various higher layer protocols. Handshake protocol, change cipher spec protocol and the alert protocol are the three higher layer protocols that are defined as a part of SSL.

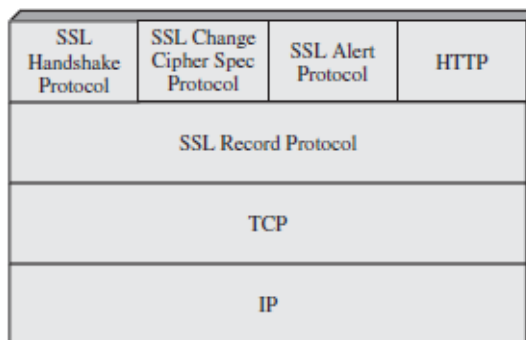


Figure 16.2 SSL Protocol Stack

SSL connection concepts:**Connection:**

For SSL connections are peer to peer relationship. The connections are transient. Every connection is associated with one session.

Session:

An SSL session is an association between a client and a server. Sessions are created by the handshake protocol.

A session state is identified by the following parameters;

- **Session identifier:** An arbitrary byte sequence chosen by the server to identify an active or resumable session state.
- **Peer certificate:** An X509.v3 certificate of the peer.
- **Compression method:** The algorithm used to compress data prior to encryption.
- **Cipher spec:** Specifies data encryption algorithm and a hash algorithm used for MAC calculation.
- **Master secret:** 48-byte secret shared between the client and server.
- **Is resumable:** A flag indicating whether the session can be used to initiate new connections.
- **Server and client random:** Byte sequences that are chosen by the server and client for each connection.
- **Server write MAC secret:** The secret key used in MAC operations on data sent by the server.
- **Client write MAC secret:** The secret key used in MAC operations on data sent by the client.
- **Server write key:** The secret encryption key for data encrypted by the server and decrypted by the client.
- **Client write key:** The symmetric encryption key for data encrypted by the client and decrypted by the server.
- **Initialization vectors:** When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL Handshake Protocol.
- **Sequence numbers:** Each party maintains separate sequence numbers for transmitted and received messages for each connection. Sequence numbers may not exceed $2^{64} - 1$.

SSL Record Protocol

The SSL Record Protocol provides two services for SSL connections:

- **Confidentiality:** This protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
- **Message Integrity:** This protocol defines a shared secret key that is used to form a message authentication code.

The following figure shows the overall operation of the SSL Record Protocol. The first step is **fragmentation**. Next, **compression** is optionally applied. Compression must be lossless and may not increase the content length by more than 1024 bytes. The next step in processing is to compute a **message authentication code** over the compressed data.

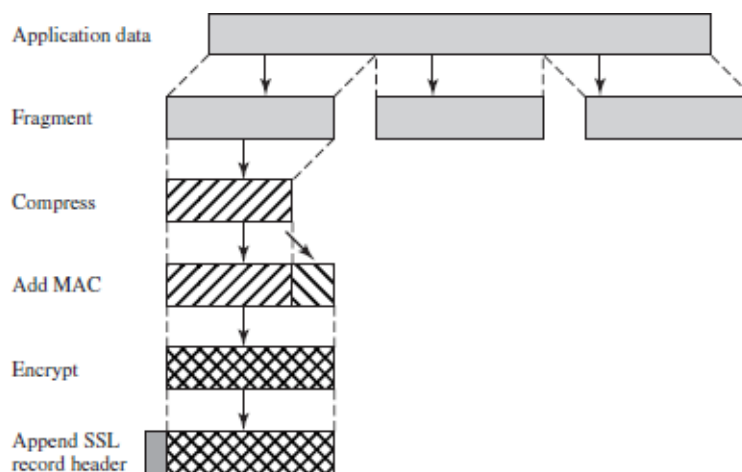


Figure 16.3 SSL Record Protocol Operation

SSL Record Format:

- **Content Type (8 bits):** The higher-layer protocol used to process the enclosed fragment.
- **Major Version (8 bits):** Indicates major version of SSL in use.
- **Minor Version (8 bits):** Indicates minor version in use.
- **Compressed Length (16 bits):** The length in bytes of the plaintext fragment.

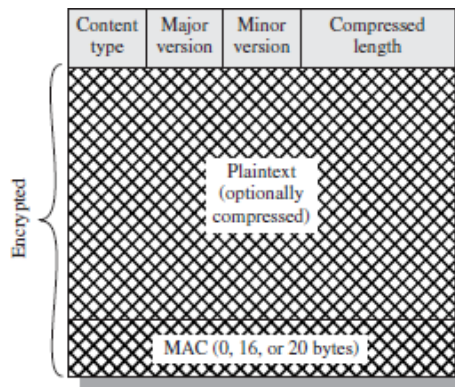


Figure 16.4 SSL Record Format

Change Cipher Spec Protocol

The Change Cipher Spec Protocol is one of the three **SSL-specific protocols** that use the SSL Record Protocol. This protocol consists of a single message, which consists of a single byte with the value 1. The main purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.

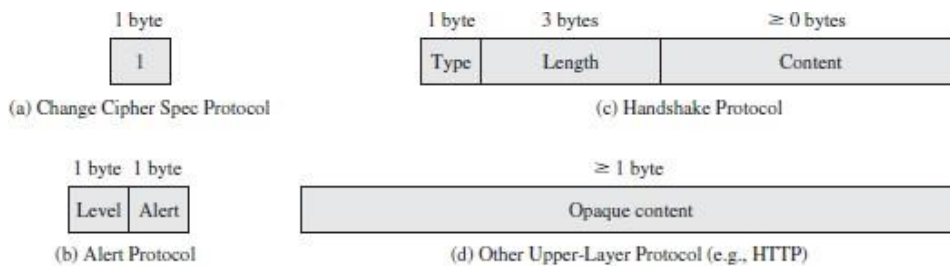


Figure 16.5 SSL Record Protocol Payload

Alert Protocol

The Alert Protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol consists of two bytes. The first byte takes the value warning (1) or fatal (2) to convey the severity of the message. If the level is fatal, SSL immediately terminates the connection. Other connections on the same session may continue, but no new connections on this session may be established. **certificate_revoked:** A certificate has been revoked by its signer.

Handshake Protocol

The most complex part of SSL is the Handshake Protocol. This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and

cryptographic keys to be used to protect data sent in an SSL record. The Handshake Protocol is used before any application data is transmitted. Each message has three fields:

- **Type (1 byte):** Indicates one of 10 messages that are defined in the following table.
- **Length (3 bytes):** The length of the message in bytes.
- **Content (bytes):** The parameters associated with this message.

The following figure shows the initial exchange needed to establish a logical connection between server and client.

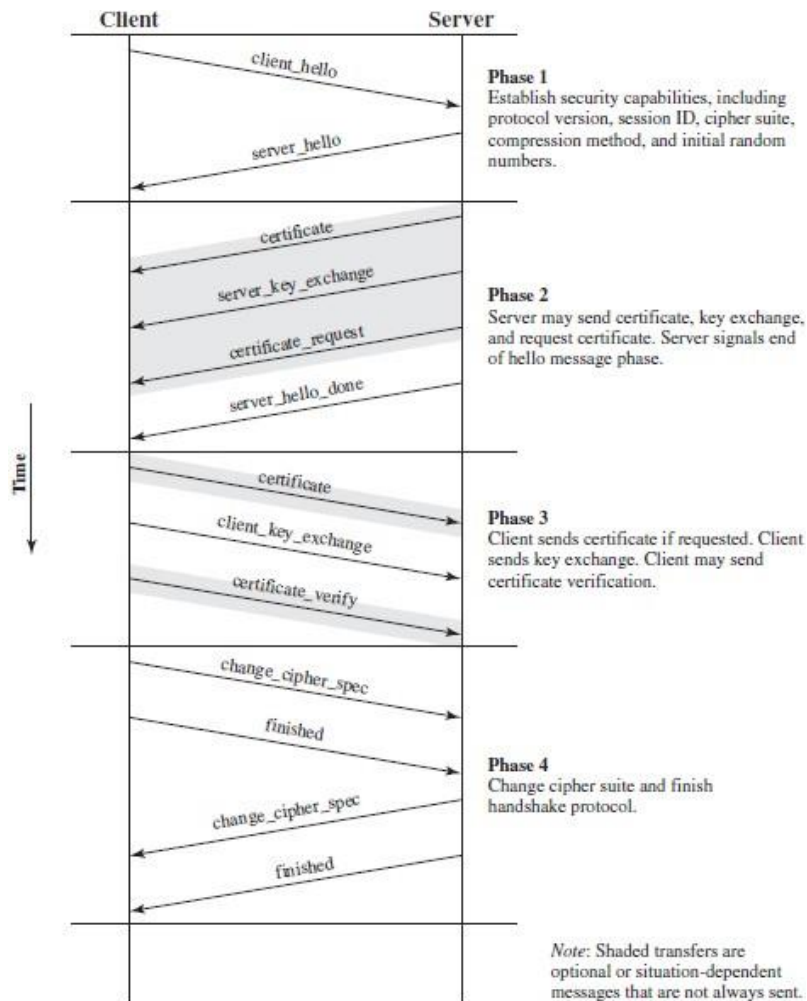


Figure 16.6 Handshake Protocol Action

EXPLAIN ABOUT TRANSPORT LAYER SECURITY (TLS) WITH A NEAT DIAGRAM.

TLS is a cryptographic protocol that provides communication security over the Internet. TLS uses asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. It is an Internet standard version of SSL. The following are the main differences between SSL and TLS.

Version Number:

The record format for TLS and SSL are the same and one of the differences is in version value.

Message Authentication Code:

SSLv3 TLS MAC schemes have two differences. They are the actual algorithm and the scope of the MAC calculation. TLS makes use of HMAC defined in RFC 2104. HMAC is defined as;

$$HMAC_K(M) = H[(K^+ \oplus opad) \parallel H[(K^+ \oplus ipad) \parallel M]]$$

Where,

- H - Embedded hash function for MD5 or SHA
- M - Input Message
- K⁺ - Secret key padded with zeros
- ipad - 00110110
- opad - 00111100

In SSL3 the padded bytes are XORed with the secret key instead of padded with secret key.

Pseudorandom Function:

TLS uses a Pseudorandom function (PRF) to expand secrets into blocks of data for the purpose of key generation and validation.

Alert Codes:

TLS supports all alert codes that are defined in SSL v3 except no_certificate. The following are the additional codes in TLS.

- Record overflow
- Unknown_ca
- Access_denied
- Decode_error
- Protocol_version

- Insufficient_security
- Unsupported_extension
- Internal_error
- Decrypt_error
- User_canceled
- No_renegotiation

Cipher Suites:

The major differences in cipher suites are;

- *Key exchange:* Except Fortezza all key exchange techniques of SSLv3 are supported by TLS.
- *Symmetric encryption algorithms:* Except Fortezza all symmetric encryption techniques of SSLv3 are supported by TLS.

Client Certificate Types:

TLS defines rsa_sign, dss_sign, rsa_fixed_dh, and dss_fixed_dh certificate types. These are all defined in SSLv3. In addition, SSLv3 TLS includes rsa_ephemeral_dh, dss_ephemeral_dh, and fortezza_kea.

Certificate_Verify and Finished Messages:

In the TLS certificate_verify message, the MD5 and SHA-1 hashes are calculated only over handshake_messages. In SSLv3, the hash calculation also included the master secret and pads.

Cryptographic Computations:

The pre_master_secret for TLS is calculated in the same way as in SSLv3. As with SSLv3, the key_block is a function of the master_secret and the client and server random numbers, but for TLS, the actual algorithm is different.

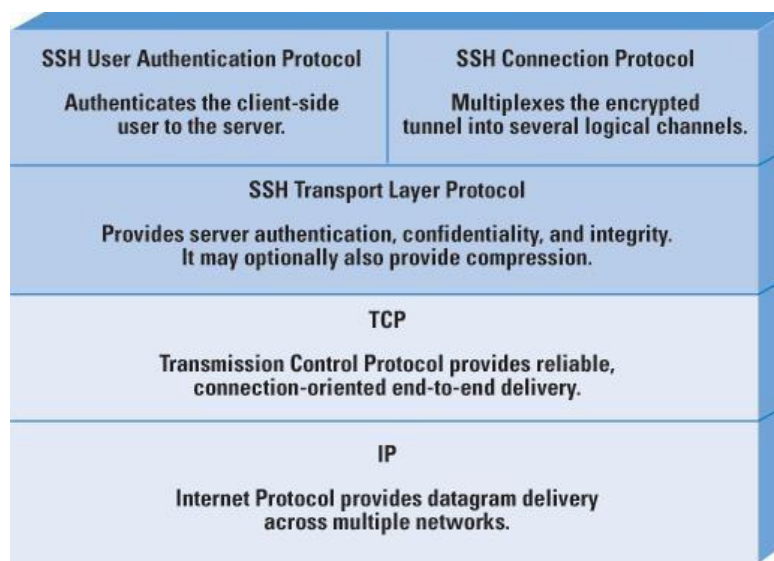
Padding:

In SSL, the padding added prior to encryption of user data is the minimum length is required so that the total size of the data to be encrypted is a multiple of the cipher's block length. In TLS, the padding can be any amount that results in a total that is a multiple of the cipher's block length, up to a maximum of 255 bytes.

WRITE ABOUT SECURE SHELL (SSH).

SSH is a protocol for secure network communication and designed to be relatively simple and inexpensive to implement. SSH applications are widely available for most Operating Systems. SSH is organized as three protocols that typically run on top of TCP.

- **Transport Layer Protocol:** It provides server authentication, data confidentiality and data integrity with forward secrecy.
- **User Authentication Protocol:** It authenticates the user with the server.
- **Connection Protocol:** It multiplexes multiple logical communication channels over a single, underlying SSH connection.



Transport Layer Protocol:

Server authentication occurs at the transport layer, based on the server possessing a public/private key pair. A server having multiple host keys using multiple different asymmetric key encryption algorithms. Multiple hosts may share the common host key. In any case the server host key is used during key exchange to authenticate the identity of the host. For this the client must have priori knowledge of the server’s public host key. The alternative trust models are;

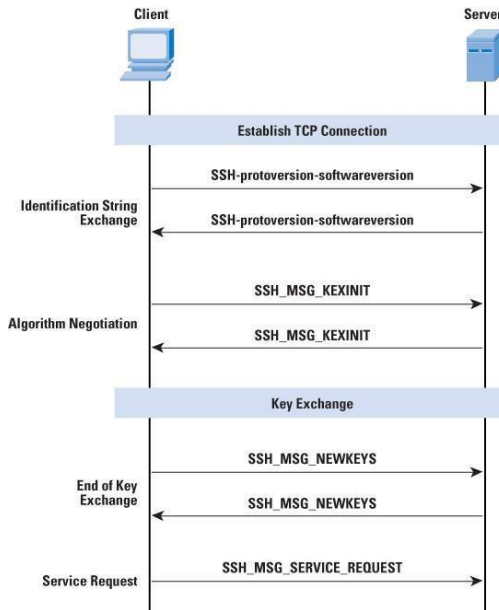
1. The client has a local database that associates each host name with the corresponding public key.
2. The host name-to-key association is certified by a trusted certification authority. The client only knows the CA root key and can verify the validity of the host keys certified by accepted CAs.

Packet Exchange:

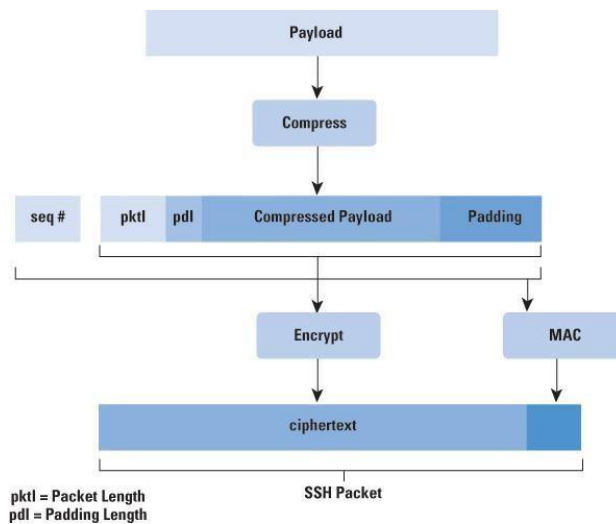
1. In this first the client establishes a TCP connection to the server. Once the connection is established, the client and server exchange data referred to as packets in the data field of TCP segment.

Sequence of events in the SSH Transport Layer Protocol:

SSH Packet:



SSH PACKET FORMAT:



Packet length: Length of the packet in bytes.

Padding length: Length of the random padding field.

Payload: Useful contents of the packet.

Random padding: once an encryption algorithm has been negotiated, this field is added.

Message authentication code (MAC): If message authentication has been negotiated, this field contains the MAC value.

2. The next step is key generation.
3. Key exchange
4. The final step is service request.

User Authentication Protocol:

It provides the means by which the client is authenticate to the server.

Message types and formats: Three types of messages are always used in the user authentication protocol. Authentication requests from the client have the format.

Byte	SSH_MSGUSERAUTH_REQUEST(50)
String	USERNAME
String	SERVICE NAME
String	METHOD NAME
.....	METHOD SPECIFIC FIELDS.

Message exchange: The message exchange involves the following steps.

1. The client sends request message.
2. The server checks to determine if the user name is valid or not. If not, the server returns false otherwise the server proceeds step 3.
3. The server returns with a list of one or more authentication methods to be used.
4. The client selects one of the acceptable authentication methods and sends with the method name and the required method-specific fields.
5. If the authentication succeeds and more authentication methods are required, the server proceeds step 3, using a partial success value of true. Otherwise the server proceeds step 3, using a partial success value of false.
6. When all required authentication methods succeed, the server sends a message, and the authentication protocol is over.

Authentication methods: The server may require one or more following authentication methods.

1. **Publickey:** The details of this method depend on the public key algorithm chosen.
2. **Password:** The client sends a message containing a plain text password, which is protected by encryption by the Transport Layer Protocol.
3. **Hostbased:** Authentication is performed on the client's host rather than the client itself.

Connection Protocol:

The SSH connection protocol runs on the top of the SSH Transport Layer Protocol and assumes that a secure authentication connection is in use. That secure authentication connection referred to as a **tunnel**, is used by the connection protocol to multiplex a number of logical channels.

Channel Mechanism:

All types of communication using SSH, such as a terminal session are supported by using separate channels. Each channel, each side associates a unique channel number, which need not be the same on the both ends. Channels are flow controlled using a window mechanism. No data may be sent to a channel until a message is received to indicate that window space is available. The life of a channel progresses through three stages. They are;

- Opening a channel
- Data transfer
- Closing a channel

Channel Types: Four channel types are recognized in the SSH connection protocol specification. They are;

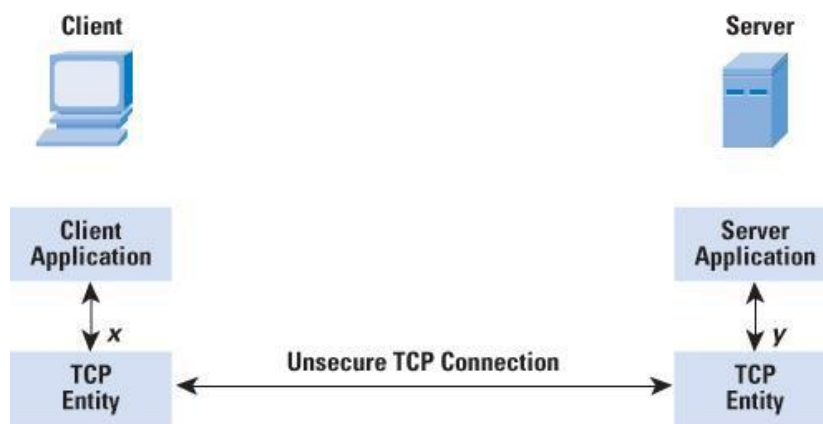
- **Session:** The remote execution of a program.
- **x11:** This refers to the X window system, a computer system and network protocol that provides a GUI for networked computers. X allows application to run on a network server but to be displayed on a desktop machine.
- **Forwarded-tcpip:** This is remote port forwarding.
- **Direct-tcpip:** This is local port forwarding.

Port Forwarding:

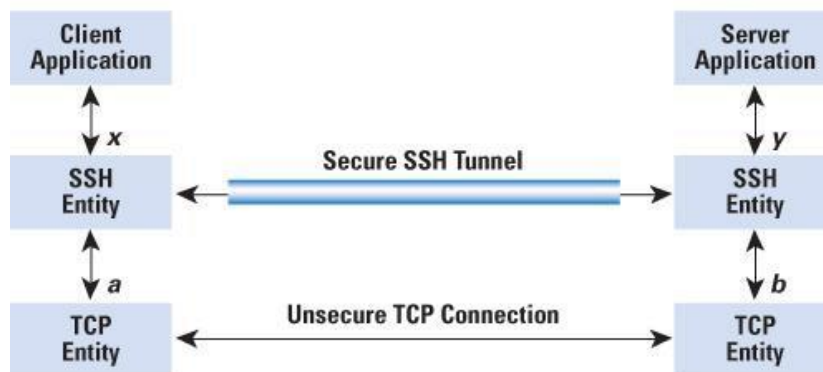
One of the most useful features of SSH is port forwarding. It provides the ability to convert any insecure TCP connection into a secure SSH connection. This is also referred to as SSH tunneling.

SSH supports two types of port forwarding. They are;

- **Local forwarding:**
- **Remote forwarding**



(a) Connection via TCP



(b) Connection via SSH Tunnel

EXPLAIN ABOUT E-MAIL SECURITY. (PGP OR PRETTY GOOD PRIVACY)

Mail is the most heavily used network based application. It will be used widely in various platforms. PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.

- PGP stands for Pretty Good Privacy. It was developed originally by Phil Zimmerman. PGP is open-source. PGP is used primarily for email security.
- PGP is a complete e-mail security package that provides privacy, authentication, digital signatures, and compression all in an easy to use form.
- The complete package, including all the source code, is distributed free of charge via the Internet. Due to its quality, zero price, and easy availability on UNIX, Linux, Windows and Mac OS platforms, it is widely used today.
- PGP encrypts data by using a block cipher called IDEA, key management uses RSA and data integrity uses MD5.

Notation

Most of the notation used in this chapter has been used before, but a few terms are new. It is perhaps best to summarize those at the beginning. The following symbols are used:

K_s	= session key used in symmetric encryption scheme
PR_a	= private key of user A, used in public-key encryption scheme
PU_a	= public key of user A, used in public-key encryption scheme
EP	= public-key encryption
DP	= public-key decryption
EC	= symmetric encryption
DC	= symmetric decryption
H	= hash function
	= concatenation
Z	= compression using ZIP algorithm
R64	= conversion to radix 64 ASCII format

Operational Description

The actual operation of PGP, as opposed to the management of keys, consists of five services: authentication, confidentiality, compression, e-mail compatibility, and segmentation

Function	Algorithms	Used Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the

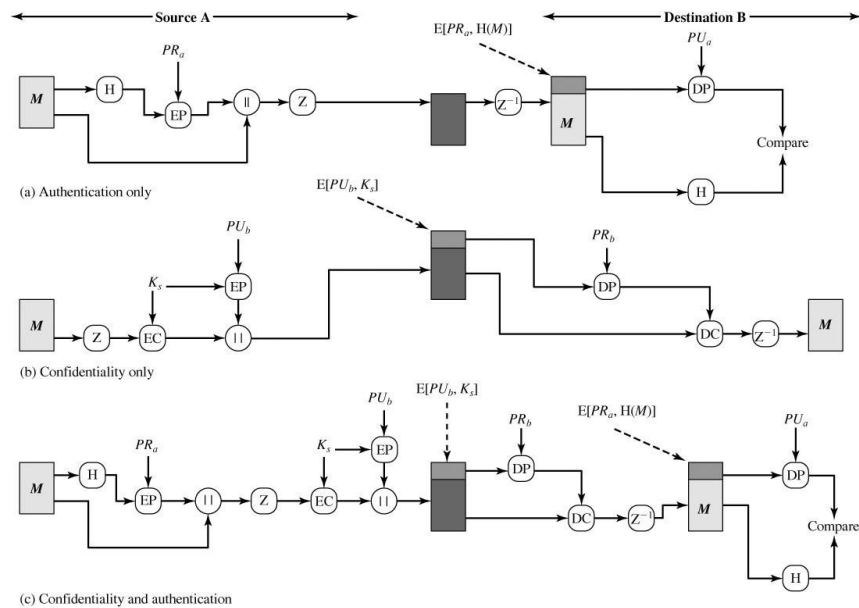
CRYPTOGRAPHY AND NETWORK SECURITY – UNIT V

Function	Algorithms	Used Description
		message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed, for storage or transmission, using ZIP.
Email compatibility	Radix 64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix 64 conversion.
Segmentation		To accommodate maximum message size limitations, PGP performs segmentation and reassembly.

Authentication

The following figure illustrates the digital signature service provided by PGP. The sequence is as follows:

1. The sender creates a message.
2. SHA-1 is used to generate a 160-bit hash code of the message.
3. The hash code is encrypted with RSA using the sender's private key, and the result is prepended to the message.
4. The receiver uses RSA with the sender's public key to decrypt and recover the hash code.
5. The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic.



Confidentiality

Another basic service provided by PGP is confidentiality, which is provided by encrypting messages to be transmitted or to be stored locally as files. In both cases, the symmetric encryption algorithm CAST-128 may be used. Alternatively, IDEA or 3DES may be used. The 64-bit cipher feedback (CFB) mode is used.

The above illustrates the sequence, which can be described as follows:

1. The sender generates a message and a random 128-bit number to be used as a session key for this message only.
2. The message is encrypted, using CAST-128 (or IDEA or 3DES) with the session key.
3. The session key is encrypted with RSA, using the recipient's public key, and is prepended to the message.
4. The receiver uses RSA with its private key to decrypt and recover the session key.
5. The session key is used to decrypt the message.

Confidentiality and Authentication

As per the above figure illustrates, both services may be used for the same message. First, a signature is generated for the plaintext message and prepended to the message. Then the plaintext message plus signature is encrypted using CAST-128 (or IDEA or 3DES), and the session key is encrypted using RSA (or ElGamal). This sequence is preferable to the opposite: encrypting the message and then generating a signature for the encrypted message. It is generally more convenient to store a signature with a plaintext version of a message.

Furthermore, for purposes of third-party verification, if the signature is performed first, a third party need not be concerned with the symmetric key when verifying the signature.

In summary, when both services are used, the sender first signs the message with its own private key, then encrypts the message with a session key, and then encrypts the session key with the recipient's public key.

Compression

As default, PGP compresses the message after applying the signature but before encryption. This has the benefit of saving space both for e-mail transmission and for file storage. The placement of the compression algorithm, indicated by Z for compression and Z^{-1} for decompression in Figure is critical:

1. The signature is generated before compression for two reasons:
 - a. It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification.
2. Message encryption is applied after compression to strengthen cryptographic security. Because the compressed message has less redundancy than the original plaintext, cryptanalysis is more difficult.
3. The compression algorithm used is ZIP.

E-mail Compatibility

When PGP is used, at least part of the block to be transmitted is encrypted. If only the signature service is used, then the message digest is encrypted (with the sender's private key). If the confidentiality service is used, the message plus signature (if present) are encrypted (with a one-time symmetric key). Thus, part or all of the resulting block consists of a stream of arbitrary 8-bit octets. However, many electronic mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction, PGP provides the service of converting the raw 8-bit binary stream to a stream of printable ASCII characters.

The scheme used for this purpose is radix-64 conversion. Each group of three octets of binary data is mapped into four ASCII characters. This format also appends a CRC to detect transmission errors. The use of radix 64 expands a message by 33%.

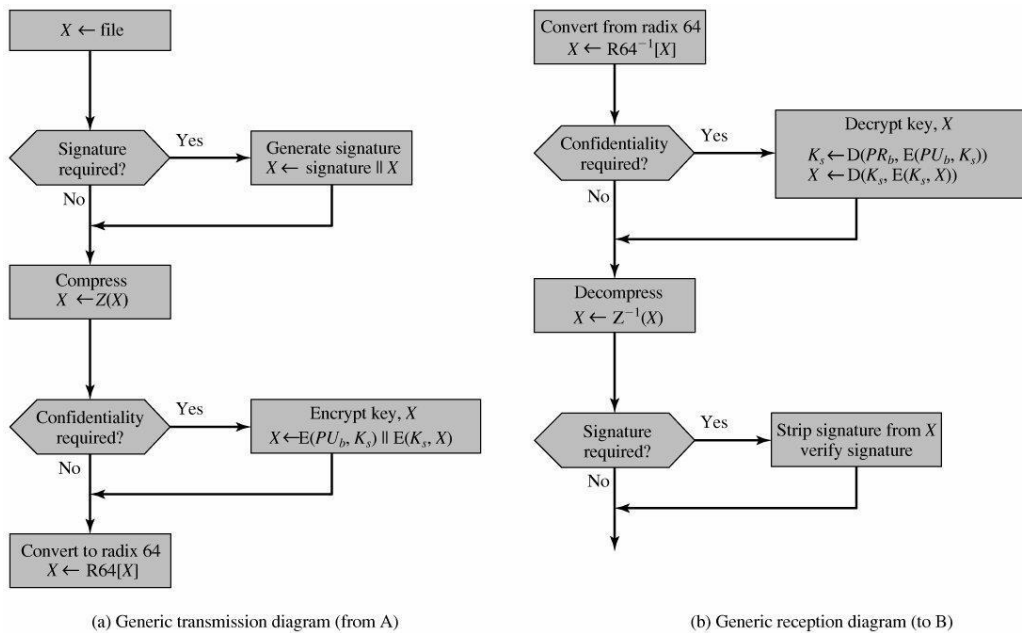


Figure-2 shows the relationship among the four services so far discussed. On transmission, if it is required, a signature is generated using a hash code of the uncompressed plaintext. Then the plaintext, plus signature if present, is compressed. Next, if confidentiality is required, the block (compressed plaintext or compressed signature plus plaintext) is encrypted and prepended with the public-key-encrypted symmetric encryption key. Finally, the entire block is converted to radix-64 format.

On reception, the incoming block is first converted back from radix-64 format to binary. Then, if the message is encrypted, the recipient recovers the session key and decrypts the message. The resulting block is then decompressed. If the message is signed, the recipient recovers the transmitted hash code and compares it to its own calculation of the hash code.

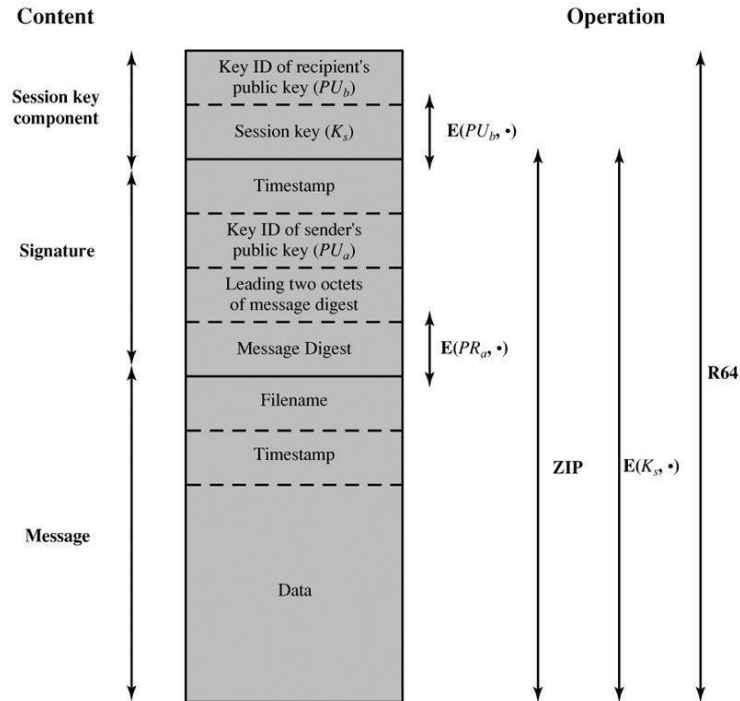
Segmentation and Reassembly

E-mail facilities often are restricted to a maximum message length. For example, many of the facilities accessible through the Internet impose a maximum length of 50,000 octets. Any message longer than that must be broken up into smaller segments, each of which is mailed separately.

To accommodate this restriction, PGP automatically subdivides a message that is too large into segments that are small enough to send via e-mail. The segmentation is done after all of

the other processing, including the radix-64 conversion. Thus, the session key component and signature component appear only once, at the beginning of the first segment. At the receiving end, PGP must strip off all e-mail headers and reassemble the entire original block before performing the steps illustrated in the above Figure.

PGP Message Format:



Notation:
 $E(PU_b, *)$ = encryption with user b's public key
 $E(PR_a, *)$ = encryption with user a's private key
 $E(K_s, *)$ = encryption with session key
 ZIP = Zip compression function
 R64 = Radix-64 conversion function

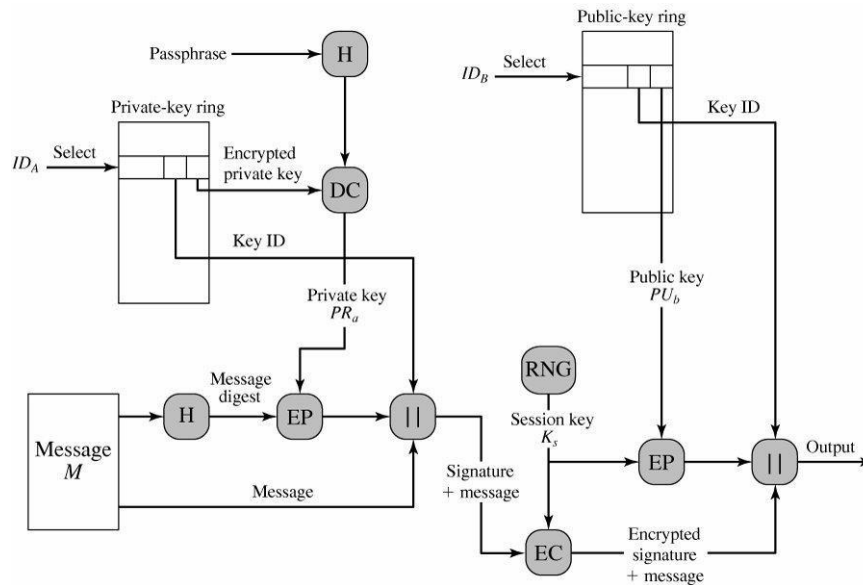
General Format of PGP Message (from A to B)

The sending PGP entity performs the following steps for sending the message:

1. Signing the message
 - a. PGP retrieves the sender's private key from the private-key ring using your_userid as an index. If your_userid was not provided in the command, the first private key on the ring is retrieved.
 - b. PGP prompts the user for the passphrase to recover the unencrypted private key.
 - c. The signature component of the message is constructed.

2. Encrypting the message

- a. PGP generates a session key and encrypts the message.
- b. PGP retrieves the recipient's public key from the public-key ring using her_userid as an index.
- c. The session key component of the message is constructed.



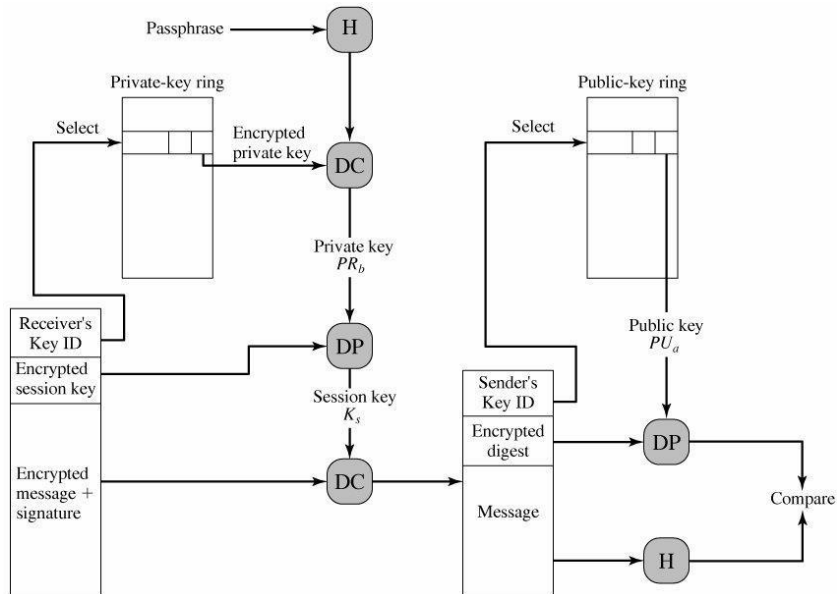
The receiving PGP entity performs the following steps

1. Decrypting the message

- a. PGP retrieves the receiver's private key from the private-key ring, using the Key ID field in the session key component of the message as an index. PGP prompts the user for the passphrase to recover the unencrypted private key.
- b. PGP then recovers the session key and decrypts the message.

2. Authenticating the message

- a. PGP retrieves the sender's public key from the public-key ring, using the Key ID field in the signature key component of the message as an index.
- b. PGP recovers the transmitted message digest.
- c. PGP computes the message digest for the received message and compares it to the transmitted message digest to authenticate.



PGP Message Reception (from User A to User B; no compression or radix 64 conversion)

Explain about S/MIME.

S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard.

RFC 822

RFC 822 defines a format for text messages that are sent using electronic mail. It has been the standard for Internet-based text mail message and remains in common use. In the RFC 822 context, messages are viewed as having an envelope and contents. The envelope contains whatever information is needed to accomplish transmission and delivery. The contents compose the object to be delivered to the recipient. The RFC 822 standard applies only to the contents. However, the content standard includes a set of header fields that may be used by the mail system to create the envelope, and the standard is intended to facilitate the acquisition of such information by programs.

The overall structure of a message that conforms to RFC 822 is very simple. A message consists of some number of header lines (the header) followed by unrestricted text (the body). The header is separated from the body by a blank line. Put differently, a message is ASCII text, and all lines up to the first blank line are assumed to be header lines used by the user agent part of the mail system.

A header line usually consists of a keyword, followed by a colon, followed by the keyword's arguments; the format allows a long line to be broken up into several lines. The most frequently used keywords are From, To, Subject, and Date. Here is an example message:

Date: Tue, 16 Jan 1998 10:37:17 (EST)
From: "William Stallings" <ws@shore.net>
Subject: The Syntax in RFC 822
To: Smith@Other-host.com
Cc: Jones@Yet-Another-Host.com

Hello. This section begins the actual message body, which is delimited from the message heading by a blank line.

Another field that is commonly found in RFC 822 headers is Message-ID. This field contains a unique identifier associated with this message.

Multipurpose Internet Mail Extensions

MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer Protocol) or some other mail transfer protocol and RFC 822 for electronic mail. MIME is intended to resolve these problems in a manner that is compatible with existing RFC 822 implementations. The specification is provided in RFCs 2045 through 2049.

- MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP.
- MIME defined by IETF to allow transmission of non-ASCII data via e-mail.
- It allows arbitrary data to be encoded in ASCII for normal transmission.
- All media types that are sent or received over the World Wide Web (WWW) are encoded using different MIME types.
- Messages sent using MIME encoding includes information that describes the type of data and the encoding that was used.
- RFC822 specifies the exact format for mail header lines as well as their semantic interpretations.
- The following figure shows the working of MIME.
- MIME defines five header fields.

1. MIME – Version

- 2. Content – Type
- 3. Content – Transfer – Encoding
- 4. Content – Id
- 5. Content – Description

Mail Message Header

From: rama@e-mail.com

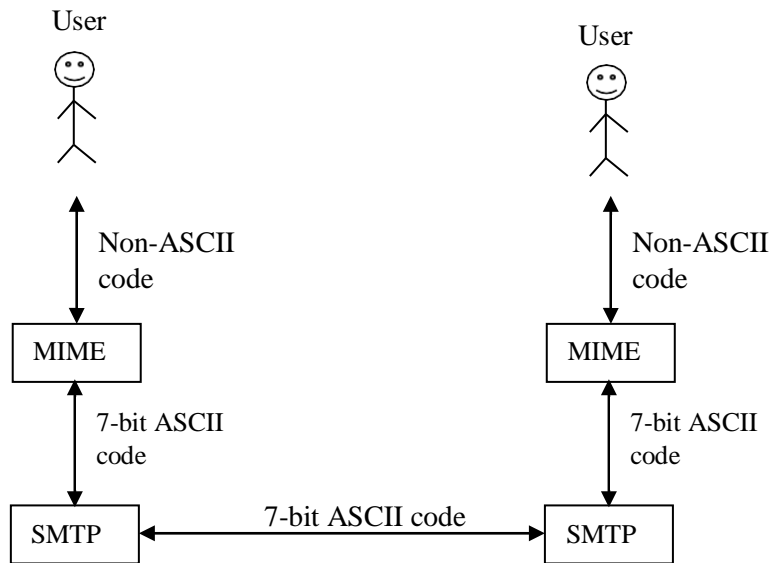
To: sita@sinhgad.edu

MIME – Version: 1.0

Content – type: image/gif

Content – Transfer – Encoding: base64

.....data for the image.....
.....
.....
.....



MIME Content Types

The following table lists the content types specified in RFC 2046.

Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript.
	octet-stream	General binary data consisting of 8-bit bytes.

S/MIME Functions

S/MIME provides the following functions:

- Enveloped data: This consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.
- Signed data: A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.
- Clear-signed data: As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using base64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.
- Signed and enveloped data: Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

Cryptographic Algorithms

Cryptographic Algorithms Used in S/MIME

Function	Requirement
Create a message digest to be used in forming a digital signature. Encrypt message digest to form digital signature.	MUST support SHA-1. Receiver SHOULD support MD5 for backward compatibility. Sending and receiving agents MUST support DSS. Sending agents SHOULD support RSA encryption. Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits.
Encrypt session key for transmission with message.	Sending and receiving agents SHOULD support Diffie-Hellman. Sending and receiving agents MUST support RSA encryption with key sizes 512 bits to 1024 bits.
Encrypt message for transmission with one-time session key.	Sending and receiving agents MUST support encryption with triple DES Sending agents SHOULD support encryption with AES. Sending agents SHOULD support encryption with RC2/40.

CRYPTOGRAPHY AND NETWORK SECURITY – UNIT V

Cryptographic Algorithms Used in S/MIME

Function	Requirement
Create a message authentication code	Receiving agents MUST support HMAC with SHA-1. Receiving agents SHOULD support HMAC with SHA-1.

IMPORTANT QUESTIONS

1. What are the different servers used in Kerberos? Explain the role of each.
2. What are the differences between Kerberos 4 and Kerberos 5.
3. Write about PGP.
4. What protocols compromise SSL? What is the difference between an SSL connection and an SSL session?
5. Explain about SSL handshake protocol.
6. In S/MIME, how does a receiver find out what cryptographic algorithms the sender has used when receives an S/MIME message.

CRYPTOGRAPHY AND NETWORK SECURITY – UNIT V

UNIT - VI

IP SECURITY: IP SECURITY OVERVIEW, IP SECURITY ARCHITECTURE, AUTHENTICATION HEADER, ENCAPSULATING SECURITY PAYLOAD, COMBINING SECURITY ASSOCIATIONS AND KEY MANAGEMENT.

INTRUSION DETECTION: OVERVIEW, APPROACHES FOR IDS/IPS, SIGNATURE BASED IDS, HOST BASED IDS/IPS (TEXT BOOK 2)

EXPLAIN ABOUT IP SECURITY.

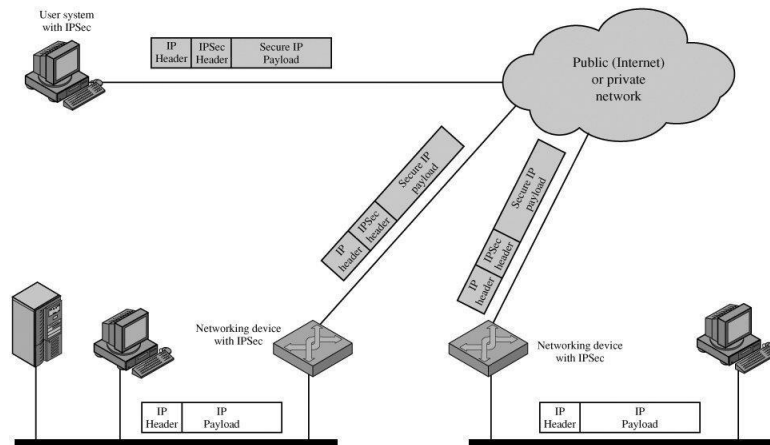
IP-level security focuses on *authentication, confidentiality, and key management*. The authentication mechanism assures that a received packet was, in fact, transmitted by the party *identified as the source* in the packet header. In addition, this mechanism assures that the packet has not been *altered* in transit. The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties. The key management facility is concerned with the secure exchange of keys.

IP SECURITY OVERVIEW:

The main feature of IPSec is IP level security by encrypting and/or authenticate all traffic at
AMRN ::1::

the IP level.

The following figure shows is a typical scenario of IPSec usage. An organization maintains LANs at dispersed locations. The IPSec networking device will typically encrypt and compress all traffic going into the WAN, and decrypt and decompress traffic coming from the WAN; these operations are transparent to workstations and servers on the LAN. Secure transmission is also possible with individual users who dial into the WAN. Such user workstations must implement the IPSec protocols to provide security.



Explain about IP Security ARCHITECTURE.

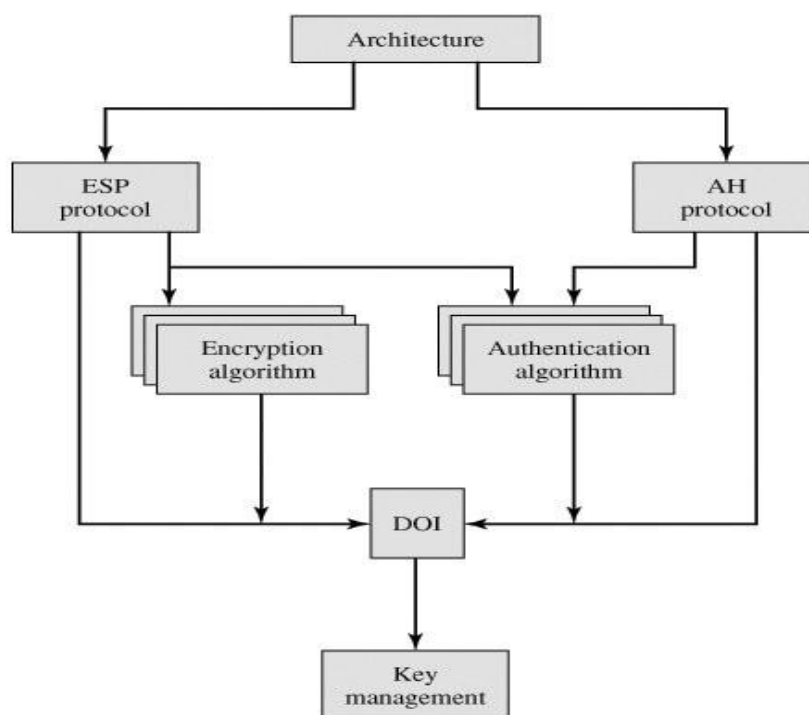
The architecture of IPSec is constituted by the following components.

1. IPSec Documents
2. IPSec Services
3. Security Associations (SA)

IPSec Documents

- IPSec specifications are described in various documents. Few important documents and specifications are described in the following table.

S. No.	Documents	Specifications
1.	RFC 2401	An overview of a security architecture
2.	RFC 2402	Description of a packet authentication extension to IPv4 and IPv6
3.	RFC 2406	Description of a packet encryption extension to IPv4 and IPv6
4.	RFC 2408	Specification of key management capabilities



- **Architecture:** Covers the general concepts, security requirements, definitions, and IPSec technology.
- **Encapsulating Security Payload (ESP):** Covers the packet format and general issues related to the use of the ESP for packet encryption and, optionally, authentication.
- **Authentication Header (AH):** Covers the packet format and general issues related to the use of AH for packet authentication.
- **Encryption Algorithm:** A set of documents that describe how various encryption algorithms are used for ESP.
- **Authentication Algorithm:** A set of documents that describe how various authentication algorithms are used for AH and for the authentication option of ESP.
- **Key Management:** Documents that describe key management schemes.
- **Domain of Interpretation (DOI):** Contains values needed for the other documents to relate to each other. These include identifiers for approved encryption and authentication algorithms, as well as operational parameters such as key lifetime.

IP Sec Services

IPSec provides security services at the IP layer by selecting required security protocols, algorithm(s) and cryptographic keys as per the services requested.

The services provided by these protocols are:

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets (a form of partial sequence integrity)
- Confidentiality (encryption)
- Limited traffic flow confidentiality

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✓	✓	✓
Connectionless integrity	✓		✓
Data origin authentication	✓		✓
Rejection of replayed packets	✓	✓	✓
Confidentiality		✓	✓
Limited traffic flow confidentiality		✓	✓

Security Associations (SA)

A security association is a one way relationship between sender and receiver. Security associations are identified by the following three parameters. They are;

- Security Parameter Index
- IP Destination Address
- Security Protocol Identifier

Security Parameter Index (SPI): SPI is a string of bit assigned to this SA and has local significance only. SPI is located in AH and ESP headers. SPI enables the receiving system under which packet is to be processed.

IP Destination Address: It is the end point address of SA, which can be end user system or a network system (firewall/router)

Security Protocol Identifiers: It indicates whether the association is an AH or ESP security association.

SA Parameters

A Security Association is normally defined by the following parameters:

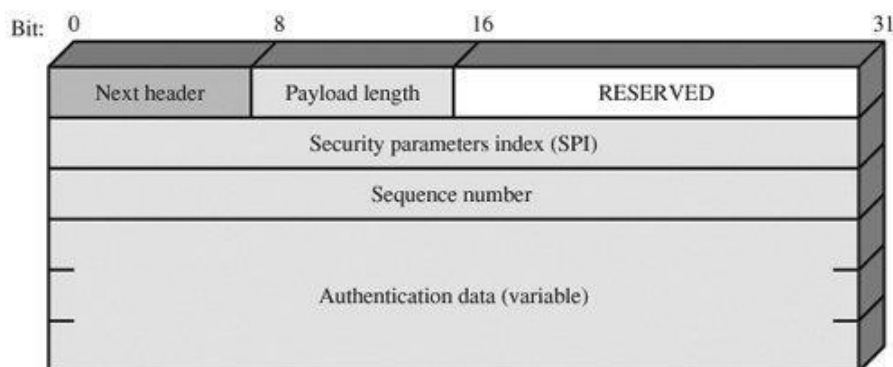
- **Sequence Number Counter:** It is a 32-bit value that indicates the Sequence Number field in AH or ESP headers.
- **Sequence Counter Overflow:** Sequence Counter overflow is a flag used to indicate whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on SA (required for all implementations).
- **Anti-Replay Window:** Used to determine whether an inbound AH or ESP packet is a replay.
- **AH Information:** Authentication algorithm, keys, key lifetimes, and related parameters being used with AH (required for AH implementations).
- **ESP Information:** Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP (required for ESP implementations).
- **IPSec Protocol Mode:** Tunnel, transport, or wildcard (required for all implementations).
- **Path (MTU) Maximum Transmission Unit:** Any observed path maximum transmission unit (maximum size of a packet that can be transmitted without fragmentation) and aging variables (required for all implementations).

EXPLAIN ABOUT AUTHENTICATION HEADER WITH A NEAT DIAGRAM.

- It provides support for data integrity and authentication of IP packets.
- Data integrity service insures that data inside IP packets is not altered during the transit.
- Authentication service enables an end user to authenticate the user at the other end and decides to accept or reject packets accordingly.
- Authentication also prevents the IP address spoofing attack.
- AH is based on the Message Authentication Code (MAC), hence tow communication parties must share a secret key.
- AH header format is shown in following figure

The Authentication Header consists of the following fields;

- **Next Header (8 bits):** Identifies the type of header immediately following this header.
- **Payload Length (8 bits):** this field contains length of Authentication Header in 32-bit words-2 (minus).
- **Reserved (16 bits):** For future use.
- **Security Parameters Index (32 bits):** Identifies a security association.
- **Sequence Number (32 bits):** Sequence Number will be given for all packets to prevent replay attack.
- **Authentication Data (variable):** A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value (ICV), or MAC, for this packet.



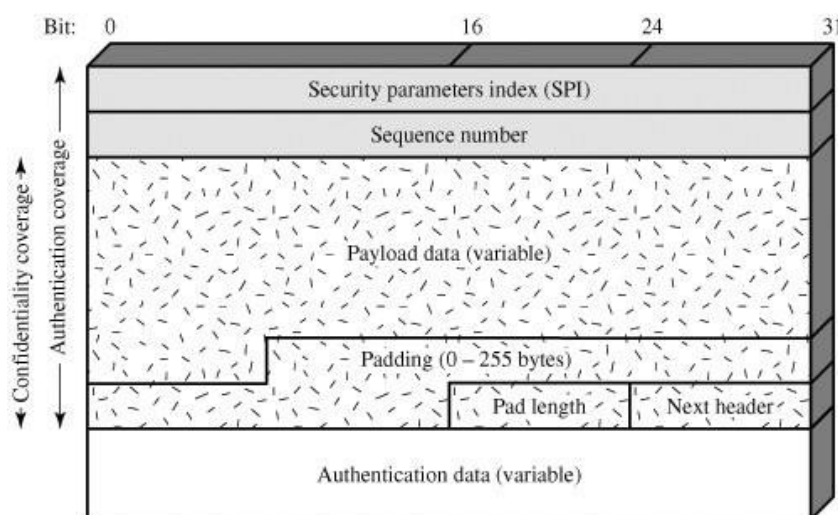
WHAT IS MEANT BY ENCAPSULATING SECURITY PAYLOAD? EXPLAIN ITS FORMAT IN DETAIL.

The Encapsulating Security Payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality. As an optional feature, ESP can also provide an authentication service.

ESP Format

The following figure shows the format of an ESP packet. It contains the following fields:

- **Security Parameters Index (32 bits):** Identifies a security association.
- **Sequence Number (32 bits):** A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH.
- **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- **Padding (0255 bytes):** The purpose of this field is discussed later.
- **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.
- **Next Header (8 bits):** Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP).
- **Authentication Data (variable):** It is variable-length field (must be an integral number of 32-bit words) that contains the Authentication called as the Integrity Check Value for the datagram.



Encryption and Authentication Algorithms

The Payload Data, Padding, Pad Length, and Next Header fields are encrypted by the ESP service. The current specification dictates that a compliant implementation must support DES in cipher block chaining (CBC) mode.

Various algorithms used for encryption are:

- Three-key triple DES
- RC5
- IDEA
- Three-key triple IDEA
- CAST
- Blowfish

Padding

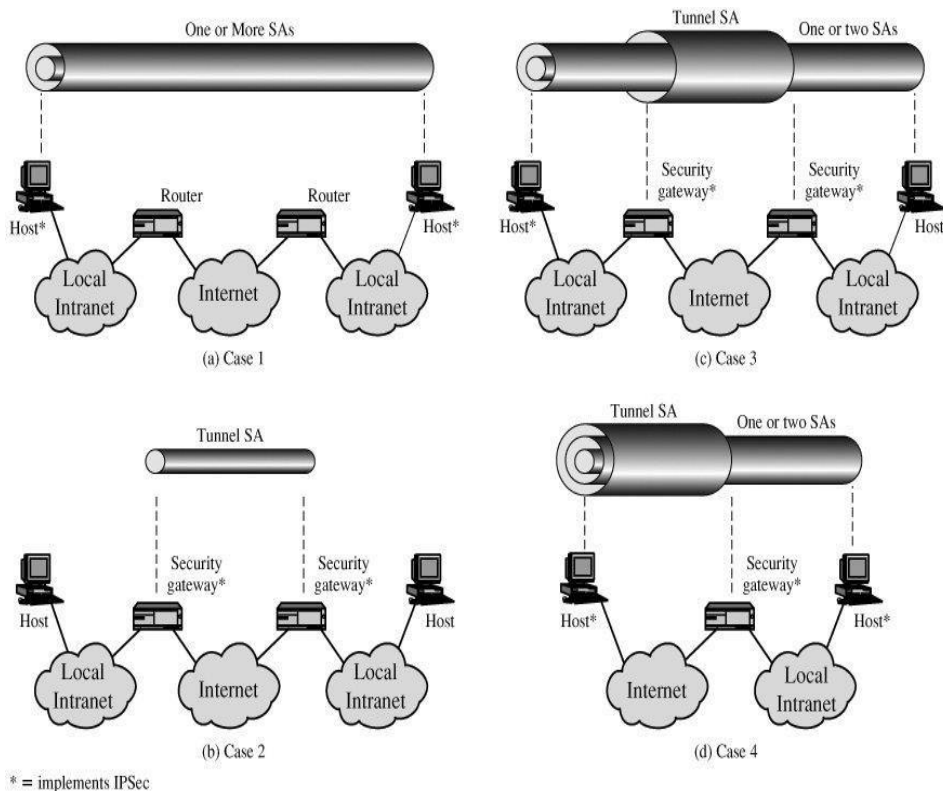
The Padding field serves several purposes:

- If an encryption algorithm requires the plaintext to be a multiple of some number of bytes (e.g., the multiple of a single block for a block cipher), the Padding field is used to expand the plaintext (consisting of the Payload Data, Padding, Pad Length, and Next Header fields) to the required length.
- The ESP format requires that the Pad Length and Next Header fields be right aligned within a 32-bit word. Equivalently, the ciphertext must be an integer multiple of 32 bits. The Padding field is used to assure this alignment.
- Additional padding may be added to provide partial traffic flow confidentiality by concealing the actual length of the payload.

EXPLAIN ABOUT COMBINING SECURITY ASSOCIATIONS.

Basic Combinations of Security Associations

The IPsec Architecture document lists four examples of combinations of SAs that must be supported by compliant IPsec hosts (e.g., workstation, server) or security gateways (e.g. firewall, router). These are illustrated in [Figure 16.10](#). The lower part of each case in the figure represents the physical connectivity of the elements; the upper part represents logical connectivity via one or more nested SAs. Each SA can be either AH or ESP. For host-to-host SAs, the mode may be either transport or tunnel; otherwise it must be tunnel mode.



In **Case 1**, all security is provided between end systems that implement IPsec. For any two end systems to communicate via an SA, they must share the appropriate secret keys. Among the possible combinations:

- a. AH in transport mode
- b. ESP in transport mode
- c. ESP followed by AH in transport mode (an ESP SA inside an AH SA)
- d. Any one of a, b, or c inside an AH or ESP in tunnel mode

For **Case 2**, security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPsec. This case illustrates simple virtual private network support. The security architecture document specifies that only a single tunnel SA is needed for this case. The tunnel could support AH, ESP, or ESP with the authentication option. Nested tunnels are not required because the IPsec services apply to the entire inner packet.

For **Case 3** builds on Case 2 by adding end-to-end security. The same combinations discussed for cases 1 and 2 are allowed here. The gateway-to-gateway tunnel provides either authentication or confidentiality or both for all traffic between end systems. When the gateway-to-gateway tunnel is ESP, it also provides a limited form of traffic confidentiality. Individual hosts can implement any additional IPsec services required for given applications or given users by means of end-to-end SAs.

Case 4 provides support for a remote host that uses the Internet to reach an organization's firewall and then to gain access to some server or workstation behind the firewall. Only tunnel mode is required between the remote host and the firewall. As in Case 1, one or two SAs may be used between the remote host and the local host.

EXPLAIN ABOUT KEY MANAGEMENT (INTERNET KEY EXCHANGE/ISAKMP).

The key management is the determination and distribution of secret keys. The IPsec Architecture supports for two types of key management:

- **Manual:** A system administrator manually configures each system with its own keys and with the keys of other communicating systems. This is practical for small, relatively static environments.
- **Automated:** An automated system enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration.

Key management protocol for IPsec is referred to as ISAKMP/Oakley and it has the following elements;

- **Oakley Key Determination Protocol:** Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security. Oakley is generic in that it does not dictate specific formats.

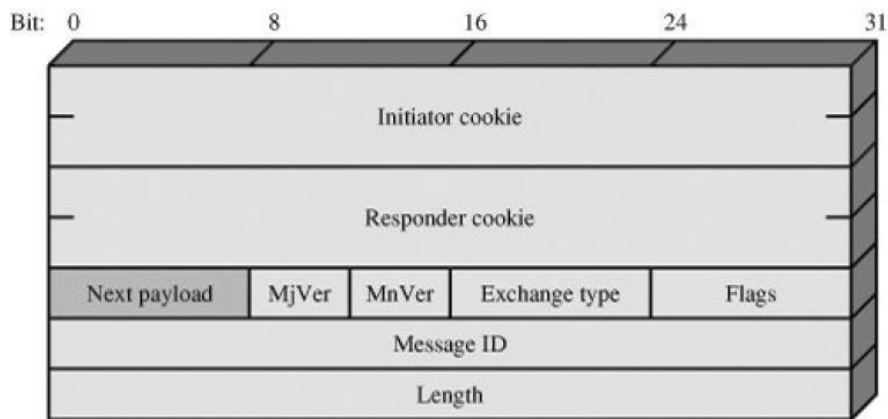
- **Internet Security Association and Key Management Protocol (ISAKMP):**
ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.

ISAKMP

ISAKMP defines procedures and packet formats to establish, negotiate, modify, and delete security associations. As part of SA establishment, ISAKMP defines payloads for exchanging key generation and authentication data.

ISAKMP Header Format

An ISAKMP message consists of an ISAKMP header followed by one or more payloads and must follow UDP transport layer protocol for its implementation. The header format of an ISAKMP header is shown below:



(a) ISAKMP header

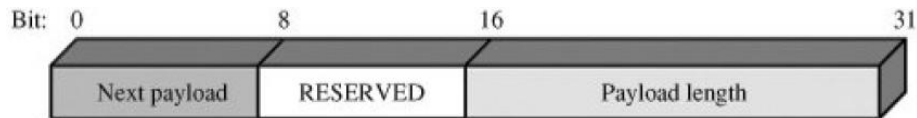
- Initiator Code (64 bits): Cookie of entity that initiated SA establishment, SA notification, or SA deletion.
- Responder Code (64 bits): Cookie of responding entity; null in first message from initiator.
- Next Payload (8 bits): Indicates the type of the first payload in the message
- Major Version (4 bits): Indicates major version of ISAKMP in use.
- Minor Version (4 bits): Indicates minor version in use.
- Exchange Type (8 bits): Indicates the type of exchange. Can be informational, aggressive, authentication only, identity protection or base exchange (S).
- Flag(8 bits): Indicates specific options set for this ISAKMP exchange. Two bits so far defined. The Encryption bit is set if all payloads following the header are encrypted

using the encryption algorithm for this SA. The Commit bit is used to ensure that encrypted material is not received prior to completion of SA establishment.

- Message ID (32 bits): Unique ID for this message.
- Length (32 bits): Length of total message (header plus all payloads) in octets.

ISAKMP Payload Types

All ISAKMP payloads begin with the same generic payload header shown below.



(b) Generic payload header

The Next Payload field has a value of 0 if this is the last payload in the message; otherwise its value is the type of the next payload. The Payload Length field indicates the length in octets of this payload, including the generic payload header. There are many different ISAKMP payload types. They are:

- a. The **SA payload** is used to begin the establishment of an SA.
- b. The **Proposal payload** contains information used during SA negotiation.
- c. The **Transform payload** defines a security transform to be used to secure the communications channel for the designated protocol.
- d. The **Key Exchange payload** can be used for a variety of key exchange techniques, including Oakley, Diffie-Hellman, and the RSA-based key exchange used by PGP.
- e. The **Identification payload** is used to determine the identity of communicating peers and may be used for determining authenticity of information.
- f. The **Certificate payload** transfers a public-key certificate.
- g. The **Hash payload** contains data generated by a hash function over some part of the message and/or ISAKMP state.
- h. The **Signature payload** contains data generated by a digital signature function over some part of the message and/or ISAKMP state.
- i. The **Nonce payload** contains random data used to guarantee aliveness during an exchange and protect against replay attacks.
- j. The **Notification payload** contains either error or status information associated with this SA or this SA negotiation.
- k. The **Delete payload** indicates one or more SAs that the sender has deleted from its database and that therefore are no longer valid.

ISAKMP Exchanges

ISAKMP provides a framework for message exchange, with the payload types serving as the building blocks. The specification identifies five default exchange types that should be supported.

- 1. Base Exchange:** allows key exchange and authentication material to be transmitted together. This minimizes the number of exchanges at the expense of not providing identity protection.
- 2. Identity Protection Exchange:** expands the Base Exchange to protect the users' identities.
- 3. Authentication Only Exchange:** used to perform mutual authentication, without a key exchange
- 4. Aggressive Exchange:** minimizes the number of exchanges at the expense of not providing identity protection.
- 5. Informational Exchange:** used for one-way transmittal of information for SA management.

INTRUSION DETECTION: OVERVIEW, APPROACHES FOR IDS/IPS, SIGNATURE BASED IDS, HOST BASED IDS/IPS (TEXT BOOK 2)

DEFINE INTRUDERS. WHAT ARE VARIOUS CLASSES OF INTRUDERS?

Intruder is generally referred as hacker or cracker. The intruders may cause serious threats to computer security.

Classes of Intruders:

- **Masquerader:** An individual who is not authorized to use the computer but he may gain access by exploiting a legitimate user's account. Generally masquerader is an outsider.
- **Misfeasor:** A legitimate user may access the data, programs or resources but not authorized to such access or authorized but misuses his or her privileges. Generally misfeasor is an insider.
- **Clandestine User:** An individual who seizes supervisory control of the system and uses this control for some misuse. Generally Clandestine user is an insider or outsider.

EXPLAIN ABOUT INTRUSION DETECTION TECHNIQUES (INTRUSION DETECTION TECHNIQUES)

An intrusion detection/prevention system (IDS/IPS) is employed to provide deep packet inspection at the entrance of important network. The Intrusion Detection System/Intrusion Prevention System is positioned behind the firewall. VPN is permitted to pass firewall and IDS/IPS since the traffic is usually encrypted and authenticated. The IDS/IPS provides deep packet inspection for the payload, IDS is based on out-of-band detection of intrusions and their reporting, and IPS is in-band filtering to block intrusions.

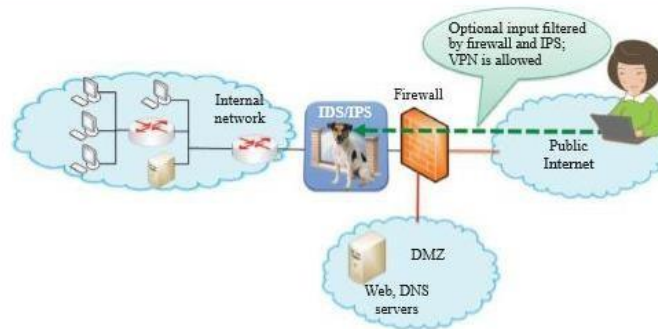


FIGURE 19.1 Positioning IDS/IPS in a system.

The following figure illustrates the difference between IDS and IPS. As indicated, IDS is performed through a wire tap, and is clearly an out-of-band operation. In contrast, IPS is performed inline. And by preventing intrusions, IPSs eliminate the need for keeping and reading extensive intrusion-incident logs, which contributes to IDSs’ considerable CPU, memory, and I/O overhead.

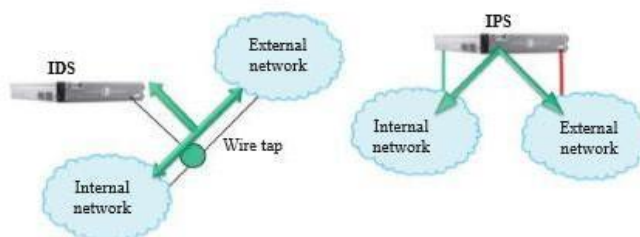


FIGURE 19.2 An illustration of out-of-band IDS vs. in-band IPS.

Explain about Signature based IDS/IPS.

Signature-based detection is used to detect patterns of specific known exploits and vulnerabilities. The exploits include patterns of codes, scripts, registration-key-modification and buffer overflow. The vulnerabilities include payload content or requests to a known vulnerability, which is used to create vulnerability-based signatures. Content signature is often a string of characters that appear in the payload of packets as part of the attack. Once

a new vulnerability is disclosed, signatures are developed by researchers to counter threats. Signature-based systems take a look at the payload and identify whether it contains a matched signature.

While this signature-based detection usually has a lower false positive rate, it may not detect zero-day and mutated attacks. Malware can be stealthy by embedding its communications into protocols that are likely to be present in normal network operations or incorporate polymorphism and metamorphism to avoid a fixed signature. A Botnet might coordinate with its C&C at irregular intervals and at low rates to avoid generating significant anomalies. The big challenges to signature-based IDS/IPS are the size of signature database, and the processing time of packets against all entries in the signature database. These can make the IDS vulnerable to DoS attacks. Some IDS evasion tools flood signature-based IDSs with too many packets, thus making the IDS drop packets and fail detection.

Explain about Host based IDS/IPS.

Many host security products contain integrated host-based IDS/IPS systems (HIDS/HIPS), anti-malware and a firewall. These HIDS/HIPS systems have both advantages and weaknesses. They are capable of protecting mobile hosts from an attack when outside the protected internal network, and they can defend local attacks, such as malware in removable devices. They also protect against attacks from network and encrypted attacks in which the encrypted data stream terminates at the host being protected. They have the capability of detecting anomalies of host software execution, e.g., system call patterns. On the negative side of the ledger, if an attacker takes over a host, the HIDS/HIPS and NAC agent software can be compromised and disabled, and the audit logs are modified to hide the malware. In addition, HIDS/HIPS has only a local view of the attack, and host-based anomaly detection has a high false alarm rate. For example, OSSEC is an open source host-based intrusion detection system. It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Windows, Linux, MacOS X, FreeBSD, Solaris, HP-UX and AIX. With some modification of the host's kernel, HIDS/HIPS can monitor all of the system calls and evaluate system calls against either known attack signatures or anomaly rules.

The HIDS/HIPS detect and prevent attacks on host computers, including Web servers and database servers. The inputs to HIDS/HIPS are network packets, system logs, system events and hardware information.

Combined signature- and anomaly-based methods detect and block abnormal activity patterns, and generate the system alarms and event reports. The time window of an event may be different due to its characteristics. HIDS/HIPS can update the system profiles based on the newly observed network patterns and system calls in order to improve the false alarm rate. HIDS/HIPS builds a dynamic database of system objects that can be monitored. Then an analysis and comparison of a number of items is performed with respect to the database. These items include system calls and the sequence of these calls, logs and their modification, system binaries modifications, password files, access control lists, shell commands and backdoor software installations. HIDS/HIPS inspects packet content after decrypting received VPN, P2P or SSL packets, and uses anti-malware software for decrypting or emulating malware that employs mutations. In contrast, NIDS/NIPS cannot inspect encrypted traffic and detect mutated malware. Hence, both NIDS/NIPS and HIDS/HIPS are deployed for optimal protection, in which the combination is greater than the sum of its individual parts. This approach yields a more accurate result for quarantining hosts and blocking/filtering traffic as well as providing the basis for NAC/NAP products. A trusted platform module (TPM) on the motherboard, which is external to the CPU thus making it much harder for an intruder to corrupt its object and checksum databases, can be used to protect the integrity of the database used for inspection.