

## UNIT 1

Challenges in network security: 6-7

Legal Security: 8-9

Model for Network Security and OSI Architecture: 13-23

Threat: 24

Attack: 25

Security Attack: 26-32

Security Service: 33-34

Security Mechanism: 35-36

Classical Encryption Technique:

Symmetric Cipher Model: 39-41

Block vs stream Cipher: 43

Classical Encryption Technique: (Main) 45-

Basic Terminology: 46-48

1.Symmetric Cipher Model: 49-52,55

Cryptanalysis and Brute-force Attack: 53-54

2.Substitution technique: 56-80

a. Caesar Cipher: 57-58

b. Monoalphabetic Cipher: 59

c. Polyalphabetic Cipher: 60-65

d. Playfair Cipher: 66-70

e. One-Time Pad: 71-72

f. Hill Cipher: 73-75

Transposition Cipher: 76-78

Product Cipher: 79-80

Rotor Machine, Steganography: 82-85

Simple Substitution cipher: 86

Adding a rotor: 87-90

Steganography: 91-97

## UNIT 2

Confidentiality Using Symmetric Encryption: 2-

Placement of Encryption Function (Link Encryption): 3-14

Traffic Confidentiality: 15-20

Key Distribution (Hierarchical key, Session key, Transparent key, Decentralized key, Controlling key) : 21-49

Random Number Generation: 50-79

Pseudorandom number generators: 55-56

Linear Congruent Generators: 57-63

Cryptographical Generated Random numbers: 64-76

True Random number generator: 77-79

## UNIT 3

Number Theory and problems (divisibility, Arithmetic): 4-16

The Division algorithm: 8-14

Corollary-17

Congruence and Hash function: 18

Congruence and Pseudorandom number Generator: 19

Congruence and Cryptography: 20

Primes: 21-24

Greatest common divisor: 25-30

The Euclidean Algorithm: 31-38

Linear Congruence: 39-42

Chinese Remainder Theorem: 43-45

Fermat's Little Theorem: 46

Public Key Cryptography and RSA Cryptography: 47-48

Traditional Cryptography: 49

Public Key Cryptography: 50

RSA Cryptography: 51-57

Key Management: 59-83

Public-Key Authority: 63-66

Secret Key: 69-72

Hybrid Key Distribution: 73

Diffie-Hellman Key: 74-81

Attack Example: 82

Key Exchange Protocol: 83

#### UNIT 4

Message Security Requirements: 3

Message Authentication: 4

Message Encryption: 5-6

Hash function: 7-13

Message Authentication Code (MAC): 14-17

HMAC: 18-20

Authentication Application: 21

Kerberos: 22-27

X.509 Authentication Service: 28-34, 39

Authentication Procedures: 35-38

#### UNIT 5

Email Security Enhancement: 2

Pretty Good Privacy: 3-24

S/MIME (Secure/Multipurpose Internet Mail Extension): 25-34

IP Security: 35-47

Transport vs Tunnel Mode ESP: 43-44, 46, 61

Security Association: 48-52, 62, 64

Authentication Header: 53-56,

Encapsulation Security Payload (ESP): 54, 57-58

Anti-Replay Service: 59-60

Authentication plus confidentiality: 63

Key Management: 65

Internet Key Exchange (IKE): 66-67

Web: 59

Secure Socket Layer (SSL): 70-74

Cookies: 76-79

Web content, Java, Spyware, Active X, Authenticate: 80-89

Intruders: 90-106

Firewalls: 107-131

Malware: Malicious Software: 132-151

#### Assignment 1

Explain elaborately the Hill cipher with neat example. (Use Assignment answer sheet)

#### Assignment 2

Explain elaborately the Message Digest with neat Diagram. (Use Assignment answer sheet)

#### CAE 1

Explain the model for network security with neat diagram. (CAE 1 – Mohnish Devaraj)

What is random number. Explain Blum Blum shub generator with example. (CAE 1 – Mohnish Devaraj)

What is DES? Elaborate the working of DES with necessary diagrams. (UNIT 2 \_ PPT\_ The Data Encryption Standard)

#### CAE 2

In a public key system using RSA, you intercept the cipher text  $C=10$  sent to a user with an algorithm description whose public key is  $e=5$ ,  $n=35$ . What is the plain text? Explain the above problem (CAE 2 – Mohnish Devaraj)

Users A and B use the Diffie-Hellman Key exchange technique with a common prime  $q=71$  and a primitive root  $\alpha = 7$ . If the user A has private key  $X_A=5$ , what is A's public key  $Y_A$ ?. Justify your answer. (39110373\_HARIHARAN B P\_NET SEC 2)

What is authentication? Explain the MD5 with neat diagram (CAE 2 – Mohnish Devaraj)

Explain x.509 certificate in detail. What is the cryptographic method used in x.509 certificate (UNIT 4\_X.509 Authentication\_ME)