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

UNIT 3

UNIT 4

UNIT 5

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 α = 7. If the user A has private key XA=5, what is A's public key YA?. 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)