Exam.Code:0918
Sub. Code: 33444

2056

B.E. (Computer Science and Engineering)

Sixth Semester

CS-602: Cryptography and Network Security

Time allowed: 3 Hours

Max. Marks: 50

NOTE: Attempt five questions in all, including Question No. I which is compulsory and selecting two questions from each Unit.

x-x-x

I. Answer the following:-

a) Define the term "Brute-force attack".

b) What is the key length used in the standard DES algorithm?

c) Distinguish between a Stream cipher and a Block cipher.

d) State Fermat's Little Theorem.

e) What is the purpose of the Euler Totient Function $\phi(n)$?

f) Mention two limitations of the Caesar Cipher.

g) What is a "Replay Attack" in network security?

h) Define "Diffusion" and "Confusion" in block cipher design.

i) What is the main difference between Monoalphabetic and Polyalphabetic ciphers?

j) Name the two primary modes of the Diffie-Hellman algorithm. (10x1)

UNIT - I

II. Explain the working of the Extended Euclidean Algorithm with a numerical example to find the Multiplicative inverse. (10)

III. Describe the Data Encryption Standard (DES) inner structure, focusing on the function of the S-boxes and the Feistel network. (10)

IV. Compare and contrast Vigenere Cipher and Vernam Cipher. Why is the Vernam Cipher Considered "unbreakable"? (10)

UNIT - II

V. Explain the architecture of IP Security (IPsec). Differentiate between Authentication Header (AH) and Encapsulating Security Payload (ESP). (10)

VI. Discuss the Secure Socket Layer (SSL) protocol stack and explain the handshake process between a client and a server. (10)

VII. What is a Firewall? Explain the different types of firewalls, including Packet Filtering and Application-level gateways. (10)

x-x-x