Code No: **R1641051** **R16** **Set No. 1**

IV B.Tech I Semester Advanced Supplementary Examinations, May - 2022

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any FOUR questions from Part-B

*****

PART–A *(14 Marks)*

1. a) Define Primality Test. [2]
   b) Write about cipher block chaining mode of operation. [3]
   c) Define Euler's totient function or phi function and their applications? [2]
   d) How keys are exchanged in Diffie-Hellman algorithm? [2]
   e) In SSL and TLS, why is there a separate change cipher spec protocol, rather than including change cipher spec message in the handshake protocol? [3]
   f) What is the role of compression function in hash function? [2]

PART–B *(4x14 = 56 Marks)*

2. a) i. Differentiate between passive attacks and active attacks. [7]
      ii. List and Determine the security services required to counter various types of active and passive attacks.
   b) i. What are the two approaches to attacking a cipher? [7]
      ii. Describe various security mechanisms.

3. a) Compare the substitution method in DES and AES. Why do we need only one substitution table in AES, but several in DES? [7]
   b) Explain the Fiestel cipher structure with a neat sketch. And also explain its importance. [7]

4. a) Enumerate Diffie-Hellman Key exchange for encryption and decryption with suitable examples. [7]
   b) Given p=19, q=23, and e=3 Use RSA algorithm to find n, $\phi(n)$ and d. [7]

5. a) List the main features of SHA-512 cryptographic hash function. What kind of compression function is used in SHA-512? [7]
   b) i. Compare Direct and Arbitrated digital signature. [7]
      ii. Explain the challenges/ response approach in mutual authentication.

6. a) What is SSL? Explain about SSL record protocol format. [7]
   b) What is the need for security services at transport layer of Internet Protocol? [7]

7. a) Explain the challenges/ response approach in mutual authentication. [7]
   b) Describe the architecture of IPSec. [7]