CBCS SCHEME

USN □□□□□□□□□□

15TE71

Seventh Semester B.E. Degree Examination, Feb./Mar. 2022

Cryptography and Network Security

Time: 3 hrs. Max. Marks: 80

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

Module-1

1 a. Apply Extended Euclidean Algorithm to find GCD(1759, 550). **(06 Marks)**
b. Analyze Ceaser Cipher by encrypting "network security" with key = 4. **(06 Marks)**
c. Explain the various substitution ciphers in classical cryptography. **(04 Marks)**

OR

2 a. State and prove Euler's theorem. **(06 Marks)**
b. Analyze symmetric encryption of plain text "cryptography" using play fair cipher given key = security. **(06 Marks)**
c. Explain the general types of cryptanalytic attacks. **(04 Marks)**

Module-2

3 a. Apply RSA algorithm to encrypt and decrypt M = 88 given prime numbers 17 and 11 with public key {7, 187}. **(08 Marks)**
b. Analyze AES key generation algorithm with necessary diagram. **(08 Marks)**

OR

4 a. Apply Diffe-Hellman key exchange algorithm to generate secret key given 5 is a primitive root of 83 and users A and B use 6 and 10 as private keys respectively. **(08 Marks)**
b. Analyze DES encryption with a suitable diagram. **(08 Marks)**

Module-3

5 a. Describe the main loop and operation of MD5 Hash function. **(08 Marks)**
b. Explain discrete logarithm signature scheme with signature generation and verification process. **(08 Marks)**

OR

6 a. Explain SHA algorithm with its operation. **(08 Marks)**
b. Explain one-way Hash function MAC for stream ciphers with a diagram. **(08 Marks)**

Module-4

7 a. Explain connection and session parameters used in Secure Socket Layer (SSL). **(06 Marks)**
b. Analyze SSL handshake protocol action with timeline diagram. **(06 Marks)**
c. Explain SSH transport layer protocol packet formation. **(04 Marks)**

OR

8 a. Explain IEEE802.11 protocol stack with specific functions. **(06 Marks)**
b. Analyze the phases of operation of IEEE802.11i with suitable diagram. **(06 Marks)**
c. Explain connection initiation and connection closure in HTTPS. **(04 Marks)**

Module-5

9 a. Analyze the transmission and reception of PGP messages using flow diagrams. **(08 Marks)**
b. Explain: (i) Header fields in S/MIME (ii) Functions of S/MIME **(08 Marks)**

OR

10 a. Analyze the basic combinations of security associations in IPSec. **(08 Marks)**
b. Explain Transport and Tunnel mode services of IPSec for providing security to IP Packets. **(08 Marks)**

* * * * *