CBCS SCHEME

USN | | | | | | | | | | |

17TE71

Seventh Semester B.E. Degree Examination, Feb./Mar. 2022
Cryptography and Network Security

Time: 3 hrs. Max. Marks: 100

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. Find the GCD (1160718174, 316258250) using Euclidean algorithm. **(05 Marks)**

b. For the group $G = \langle Z_{10}^*, X \rangle$

i) Find the order of the group
ii) Find the primitive roots in the group
iii) Show that the group is cyclic. **(07 Marks)**

c. Explain the types of cryptanalytic attacks on encrypted messages. **(08 Marks)**

OR

2 a. Find the multiplicative inverse of 550 in mod 1759. **(05 Marks)**

b. Find f(x) X g(x) in GF (2^8) with irreducible polynomial ($x^8 + x^4 + x^3 + x + 1$) if $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$. **(07 Marks)**

c. Encrypt using Hill Cipher for the plain text "PAY MORE MONEY" with the KEY

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$ **(08 Marks)**

Module-2

3 a. Write the difference between stream cipher and block cipher. **(05 Marks)**

b. What are the requirements a public key cryptosystem must full fill to be a secure algorithm? **(05 Marks)**

c. Explain the RSA Algorithm. In RSA system it is given P = 17, q = 31, e = 7, M = 2. Find the cipher text C. **(10 Marks)**

OR

4 a. Explain AES key generation algorithm with appropriate block diagram. **(10 Marks)**

b. Explain Man-in-middle attack on Diffie-Hellman algorithm. **(05 Marks)**

c. Consider the elliptic curve defined over E_{23} (1, 1). Let P = (3, 10) and Q = (9, 7). Find P + Q and 2P. **(05 Marks)**

Module-3

5 a. Define the hash function, mention the application of one-way hash function and describe the requirements for a hash function. **(10 Marks)**

b. Explain basic steps involved in generation of hash code using MD_5 algorithm with neat diagram. **(10 Marks)**

OR

6 a. Write a short note on HMAC. **(05 Marks)**

b. What is digital signature? List the requirements of digital signature. **(05 Marks)**

c. Describe the digital signature algorithm (DSA) and show signing and verification is done using DSS. **(10 Marks)**

Module-4

7 a. Explain the various phases of SSL handshake protocol with a neat diagram. **(10 Marks)**

b. List and explain all the parameters defined in SSL session and SSL connection states. **(10 Marks)**

OR

8 a. Explain the steps involved in operation of SSL record protocol with a neat diagram. **(10 Marks)**

b. Explain the IEEE 802.11 i phase of operation in detail. **(10 Marks)**

Module-5

9 a. What are the services provided by the PGP? Draw the appropriate diagram to explain it and mention the types of algorithm used for it. **(12 Marks)**

b. List and explain various functionality of S/MIME and also mention the header fields defined in MIME. **(08 Marks)**

OR

10 a. What is IPsec? Write the applications of IPsec and draw the IPsec scenario diagram. **(10 Marks)**

b. Explain the IP security architecture with the relevant diagram. **(10 Marks)**

* * * * *