CBCS SCHEME

USN □□□□□□□□□□ 18CS744

Seventh Semester B.E. Degree Examination, Dec.2024/Jan.2025

Cryptography

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. Contrast between the following pair of terms:
   i) Cryptography and cryptanalysis
   ii) Monoalphabetic and polyalphabetic cipher
   iii) Substitution and transposition cipher
   iv) Symmetric and asymmetric key cipher
   v) Stream and block cipher. **(10 Marks)**

b. Decrypt the message "MTPAECNGHAQP" using keyword "COMPUTER" using playfair cipher. Explain play fair cipher and also listing the rules to be followed. Use I and J count as one letter [use in one box]. **(10 Marks)**

OR

2 a. Encrypt and decrypt the word "MUMBAI" by hill cipher using the key matrix

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$ **(10 Marks)**

b. Explain the DES encryption and decryption algorithm. **(10 Marks)**

Module-2

3 a. Explain the Public Key Cryptosystem and its applications. **(10 Marks)**

b. Perform encryption and decryption using RSA for the following values: P = 3, q = 11, e = 7 and M = 2. Also indicate public key and private key. **(10 Marks)**

OR

4 a. Explain Diffie-Hellman key exchange algorithm. **(10 Marks)**

b. In Diffie-Hellman key exchange algorithm common prime q = 71 and primitive root $\alpha = 7$, user A's private key $X_A = 5$ and user B's private key $X_B = 12$, find:
   i) Public key Y_A
   ii) Public key Y_B
   iii) Common key **(10 Marks)**

Module-3

5 a. Explain Elliptic Curve Cryptography [ECC] algorithm. **(10 Marks)**

b. Illustrate symmetric key distribution using asymmetric encryption. **(10 Marks)**

OR

6 a. Explain the following mechanisms of distribution of public keys.
   i) Public announcement
   ii) Publicly available directory
   iii) Public key authority. **(10 Marks)**

b. Explain the process of exchange of public key certificates and its requirements. **(10 Marks)**

Module-4

7 a. Explain X.509 certificate format. (10 Marks)

b. Explain Kerberos overview in detail. (10 Marks)

OR

8 a. How PGP can be used for exchange of message? (10 Marks)

b. What is S/MIME? Explain the functions provided by it. (10 Marks)

Module-5

9 a. What are IP security benefits, applications and IP services? (10 Marks)

b. Discuss the encapsulating security payload with respect to IP sec. (10 Marks)

OR

10 a. Differentiate between transport and tunnel mode security associations. (10 Marks)

b. Discuss basic combinations of security associations. (10 Marks)

* * * * *