CBCS SCHEME

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

18EC744

Seventh Semester B.E. Degree Examination, Jan./Feb. 2023
Cryptography

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Draw and explain the model of symmetric cryptosystem. **(06 Marks)**

b. Encrypt the plaintext 'paymoremoney' using Hill chipher.

$$K = \begin{bmatrix} 17 & 17 & 15 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$ **(08 Marks)**

c. Encrypt the plaintext 'electronics and communication' using playfair cipher. Use the keyword 'VTUBGM'. **(06 Marks)**

OR

2 a. Find the GCD of 1160718174, 316258250 using Euclidian algorithm. **(08 Marks)**

b. Construct the Addition and Multiplication tables under Modulo 8 and write the table of additive and multiplication inverse module 8. **(07 Marks)**

c. Define the residue class under Mod n (z_n) write the residue class of Mod 4. **(05 Marks)**

Module-2

3 a. Draw and explain the Fiestel structure for encryption and decryption. **(12 Marks)**

b. With the help of neat figure, explain the DES encryption algorithm. **(08 Marks)**

OR

4 a. With the help of neat figure, explain the AES encryption process. **(12 Marks)**

b. With the help of neat figure, explain the AES key expansion. **(08 Marks)**

Module-3

5 a. Define Abelian group by mentioning the axioms. **(05 Marks)**

b. Perform addition, subtraction, multiplication and division on the polynomials $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$. **(08 Marks)**

c. Construct addition and multiplication tables in GF(7). Also write the table of additive and multiplicative inverses. **(07 Marks)**

OR

6 a. Define:
i) Prime Numbers
ii) Relatively Prime Numbers.
Give one example for each. **(04 Marks)**

b. State Fermat's theorem and Euler's theorem. Give one example for each. **(08 Marks)**

c. Explain Euler's Totient Function. Find the values of $\phi(37)$ and $\phi(35)$. **(08 Marks)**

Module-4

7 a. Explain the requirements of Public-key cryptography. **(06 Marks)**
b. Explain the RSA algorithm. **(06 Marks)**
c. Assuming p = 17, q = 11, find the public key and private keys. Perform encryption and decryption for plaintext message block M = 88. **(08 Marks)**

OR

8 a. Explain the Diffie-Hellman key exchange algorithm. Show that the keys generated at sender side and receiver side are same. **(08 Marks)**
b. Explain the Man-in-the-middle attack. **(08 Marks)**
c. Define primitive root. Give an example. **(04 Marks)**

Module-5

9 a. Explain the linear congruential generators. **(05 Marks)**
b. With a neat figure, explain the generalized Geffe generator. **(07 Marks)**
c. With neat figures explain
i) Beth-piper stop and go generator
ii) Alternating stop and go generator. **(08 Marks)**

OR

10 a. With neat figure, explain bilateral stop and go generator. **(08 Marks)**
b. Explain Giffort algorithm with relevant diagram. **(06 Marks)**
c. Explain Fish, Pike algorithms with relevant equations. **(06 Marks)**

* * * * *