CBCS SCHEME

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

18EC744

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

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. Draw the model of symmetric cryptosystem and explain in detail. **(08 Marks)**

b. Using Hill Cipher technique encrypt and decrypt the plain tent "Pay more money". Using the key. $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ **(12 Marks)**

OR

2 a. Explain Euclidean algorithm for determining of GCD. If a = 24140, b = 16762 solve using. Euclidean algorithm to find GCD (a, b). **(08 Marks)**

b. Mention the modular arithmetic operation properties and prove the same. **(08 Marks)**

c. Find 11^7 mod 13 using modular Arithmetic. **(04 Marks)**

Module-2

3 a. With a neat diagram, explain fiestal encryption and decryption model. **(08 Marks)**

b. With a neat diagram, explain DES encryption algorithm. **(08 Marks)**

c. List the design features of fiestal network. **(04 Marks)**

OR

4 a. Explain with a neat diagram AES encryption and decryption process. **(08 Marks)**

b. Explain AES key expansion algorithm write the Pseudo code for the same. **(08 Marks)**

c. Describe the AES shift Rows Transformation. **(04 Marks)**

Module-3

5 a. What are Groups? Explain in detail with respect to its properties. **(06 Marks)**

b. Write a note on finite field of the form GF (P). **(06 Marks)**

c. Find the additive and multiplicative inverse of GF (8). **(08 Marks)**

OR

6 a. State and prove Fermat's Theorem. Also find 7^{18} mod 19 using it. **(08 Marks)**

b. With suitable explanation prove Euler's Theorem. **(07 Marks)**

c. Explain discrete logarithms for modular Arithmetic. **(05 Marks)**

Module-4

7 a. With a neat diagram, explain public-key cryptosystem secrecy and Authentication. (10 Marks)

b. Explain the steps involved for encryption and Decryption for RSA Algorithm. (06 Marks)

c. Perform encryption using RSA algorithm for p = 5, q = 11, e = 3, m = 9. (04 Marks)

OR

8 a. Explain Diffie-Hellman key exchange algorithm. (07 Marks)

b. Explain Elliptic curve over real numbers. (07 Marks)

c. Explain Elliptic curve cryptography. (06 Marks)

Module-5

9 a. Write an explanatory note on Liner Feedback shift registers. (10 Marks)

b. Explain the following with necessary diagrams :

i) Generalized Geffe Generator

ii) Threshold Generator

iii) Alternating stop and go generator. (10 Marks)

OR

10 a. Explain Additive Generators. Also explain fish and pike Additive Generator. (10 Marks)

b. With a neat diagram, explain the concept of Gifford. (06 Marks)

c. Write a short note on A5. (04 Marks)

* * * * *