CBCS SCHEME

USN □□□□□□□□□□ **17EC744**

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. Prove that [(a mod n) + (b mod n)]mod n = (a + b) mod n. **(07 Marks)**

b. Consider $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$.

Find : i) $f(x) + g(x)$ ii) $f(x) * g(x)$ iii) $\frac{f(x)}{g(x)}$. **(07 Marks)**

c. State the axioms of groups and rings. **(06 Marks)**

OR

2 a. List and explain the properties of modular arithmetic. **(07 Marks)**

b. Define the term divisibility. State the properties of divisibility for integers. **(07 Marks)**

c. Find gcd[$a(x_2)$, $b(x_1)$] for $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 x + 1$ and $b(x) = x^4 + x^2 + x + 1$. **(06 Marks)**

Module-2

3 a. With an example, explain playfair cipher. **(10 Marks)**

b. With a block diagram, explain Fiestal encryption and decryption. **(10 Marks)**

OR

4 a. With an example, explain how transposition technique when applied on the plaintext. **(10 Marks)**

b. With a neat diagram, explain DES encryption and decryption and key generation. **(10 Marks)**

Module-3

5 a. Explain how to design and analyze, stream cipher with respect to linear complexity and correlation immunity. **(10 Marks)**

b. With schematic of AES structure, explain the operation of AES. **(10 Marks)**

OR

6 a. Design and explain the stream cipher using the following LF – SR.
i) Geffe generators
ii) Bilateral Stop and Go-generator. **(10 Marks)**

b. With neat diagram, explain the AES key expansion. **(10 Marks)**

Module-4

7 a. State Fermat's theorem. Prove that $a^{p-1} \equiv 1 (\text{mod } p)$. (07 Marks)
b. Write an elaborate note on Man-in-the-Middle attack. (07 Marks)
c. Define what is an Abelian Group. (06 Marks)

OR

8 a. State and prove Euler's theorem. (06 Marks)
b. Explain Diffie – Hellman key exchange. (07 Marks)
c. Write a note on elliptic curve over real numbers. (07 Marks)

Module-5

9 a. Explain digital signature algorithm. (10 Marks)
b. Explain in detail how N-Hash function is obtained. (10 Marks)

OR

10 a. Explain in detail secure Hash algorithm. (10 Marks)
b. Explain in detail MD5 hash function. (10 Marks)

* * * * *