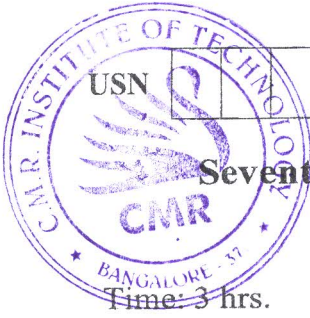


# CBGS SCHEME

18EC744



## Seventh Semester B.E. Degree Examination, Dec.2023/Jan.2024 Cryptography

Max. Marks: 100

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

### Module-1

- 1 a. Draw the model of symmetric crypto system and explain. (06 Marks)
- b. Explain rules used for playfair cipher and encrypt plain text "TECHNOLOGY" with keyword "ENCRYPT". (08 Marks)
- c. List the modular arithmetic operation properties. (06 Marks)

OR

- 2 a. Using Hill cipher technique encrypt and decrypt the plain text "ATTACK" using the key =  $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$ . (10 Marks)
- b. Explain extended Euclidean algorithm with an example. (04 Marks)
- c. Find GCD of (1970, 1066) using Euclidean algorithm. (06 Marks)

### Module-2

- 3 a. With a neat block diagram, explain DES encryption algorithm. (08 Marks)
- b. Explain with a neat diagram, AES encryption process. (08 Marks)
- c. With neat block diagram, describe ShiftRows transformation technique. (04 Marks)

OR

- 4 a. Describe the key expansion algorithm used in AES with neat diagram. (08 Marks)
- b. Illustrate the Feistel encryption and decryption process with its structure. (06 Marks)
- c. With neat block diagram, explain Mixed Columns Transformation technique. (06 Marks)

### Module-3

- 5 a. What are the Groups, Rings and Fields? Explain. (06 Marks)
- b. State and prove Fermat's and Euler's theorem. (10 Marks)
- c. Find whether 2 is primitive root of 11. (04 Marks)

OR

- 6 a. Define Euler's Totient Function. Determine the Euler's totient function of:  
(i) 37      (ii) 35      (iii) 600      (iv) 32      (v) 21 (07 Marks)
- b. For  $f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$  and  $g(x) = x^3 + x + 1$ , perform addition, subtraction, multiplication and division over GF(2). (08 Marks)
- c. Find the gcd of the given polynomials  $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$  and  $b(x) = x^4 + x^2 + x + 1$ . (05 Marks)

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-4**

- 7 a. Perform encryption and decryption using the RSA algorithm for the values  $p = 3$ ,  $q = 5$ ,  $e = 3$  and  $m = 4$ . (06 Marks)  
 b. Explain Diffie-Hellman key exchange algorithm with an example. (08 Marks)  
 c. Write a note on elliptic curve cryptography. (06 Marks)

**OR**

- 8 a. Show that 7 is a primitive root of 71, where  $q$  is common prime and 2 is primitive root used by Alice and Bob for Diffie-Hellman key exchange with  $q = 71$  and  $\alpha = 7$ .  
 (i) Find Bob's public key if Bob has private key 12? (10 Marks)  
 (ii) If Alice has a private key of 5, what is the shared key  $k$  with Bob? (10 Marks)  
 b. Which are the possible five approaches to attack RSA algorithm? (05 Marks)  
 c. Describe the RSA encryption and decryption algorithm. (05 Marks)

**Module-5**

- 9 a. Explain linear feedback shift register with necessary diagram. (08 Marks)  
 b. Describe the following with diagrams:  
 (i) Generalized Geffe generator (12 Marks)  
 (ii) Threshold Generator  
 (iii) Multispeed Inner-product generator

**OR**

- 10 a. Explain PKZIP data compression algorithm. (08 Marks)  
 b. Write notes on:  
 (i) Gifford  
 (ii) Algorithm M  
 (iii) Rambutan algorithms  
 (iv) Jennings generator (12 Marks)

\*\*\*\*\*