CBCS SCHEME

USN □□□□□□□□□□

15EC744

Seventh Semester B.E. Degree Examination, Jan./Feb. 2021

Cryptography

Time: 3 hrs. Max. Marks: 80

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. List all the axioms that should be obeyed by a field. Give suitable examples for fields. **(08 Marks)**

b. Find the GCD of the following pairs of numbers using Euclid's algorithm :
i) (24140, 16762) ii) (4655, 12075). **(08 Marks)**

OR

2 a. Explain the extended Euclid's algorithm to determine the multiplicative inverse of a given integer 'a' under modulo 'b'. Then determine 37^{-1} mod 49 using the algorithm. **(06 Marks)**

b. Find the GCD of the polynomials $x^8 + x^5 + x^4 + x + 1$ and $x^7 + x^6 + x^5 + x + 1$ using Euclidean algorithm. **(05 Marks)**

c. Prepare tables to demonstrate addition and multiplication operations for GF(5), and hence find the additive and multiplicative inverses modulo 5. **(05 Marks)**

Module-2

3 a. What are mono-alphabetic ciphers? Explain with an example. Discuss in brief the cryptanalysis of mono-alphabetic ciphers. **(06 Marks)**

b. State the rules used for encryption in PLAYFAIR cipher and encrypt the message "WATER SCARCITY" using the keyword "SAVE" using PLAYFAIR cipher. **(08 Marks)**

c. Decrypt the cipher text "zh 2100 phhw" using Caesar cipher. **(02 Marks)**

OR

4 a. Encrypt the message "HILLCIPHER" using the key $\begin{bmatrix} 3 & 2 \\ 8 & 5 \end{bmatrix}$ using Hill cipher. **(06 Marks)**

b. Encrypt the message "WORK IS WORSHIP" using the key "MOTIVATION" using vigenere cipher. **(04 Marks)**

c. With a neat block diagram, explain the various steps involved in encryption and key generation of DES algorithm. **(06 Marks)**

Module-3

5 a. Explain the AES encryption process with a neat flow diagram. **(08 Marks)**

b. Demonstrate the following operations in AES encryption given the input state 'S'

S =

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

and write the outcomes of each and transformation matrix is :

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

i) Shift rows ii) Mix columns. **(08 Marks)**

OR

6 a. Write briefly about :
i) Linear Congruential generators
ii) Galois - linear feedback shift register. **(06 Marks)**

b. With neat diagrams and necessary equations explain the working of :
i) Geffe generator
ii) Gellmann cascade generator. **(10 Marks)**

Module-4

7 a. If 'n' is a composite number and passes the Miller – Rabin test for the base 'a', then 'n' is called a strong pseudo – prime to the base 'a' show that 2047 is a strong pseudo – prime to the base 2. **(04 Marks)**

b. State Fermat's and Euler's theorems and bring out the differences between the two. Also find 9^{794} mod 73 using the most relevant of the two theorems. **(06 Marks)**

c. There is a number whose value is unknown. Repeatedly divided by 5 the remainder is 3; when divided by 7 the remainder is 1; and when repeatedly divided by 8 the reminder is 6. What is the number? (Hint : Use CRT). **(06 Marks)**

OR

8 a. Using the RSA algorithm, determine the private key 'd' (or PR) and the message 'M' given the cipher text C = 66, n = 119 and public key is PU = (e = 5, 119). **(05 Marks)**

b. Give the geometric and algebraic description of addition of 2 points $P(x_1, y_1)$ and $Q(x_2, y_2)$ on an elliptic curve $E_p(a, b)$ over prime numbers. **(06 Marks)**

c. Consider a Diffie – Hellman scheme with a common prime q = 11 and a primitive 'α' = 2.
i) If user 'A' has public key $Y_A = 9$, what is A's private key?
ii) If user 'B' has public key $Y_B = 3$, what is the shared secret key 'K'? **(05 Marks)**

Module-5

9 a. With neat diagrams and related equations explain a single operation of the Secure Hash Algorithm (SHA). Common on its security. **(08 Marks)**

b. Explain briefly the process of prime number generation in the DSA algorithm. **(08 Marks)**

OR

10 a. Define one way hash functions. Mention its properties. **(04 Marks)**

b. Describe briefly discrete logarithm signature schemes. **(06 Marks)**

c. Explain the operation of MD5, with neat diagrams and relevant equations. **(06 Marks)**

* * * * *