CBCS SCHEME

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

18EC744

Seventh Semester B.E. Degree Examination, June/July 2023
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. Define the following terminologies:
(i) Plaintext (ii) Ciphertext (iii) Encryption
(iv) Decryption (v) Cryptanalysis (vi) Brute force attack **(06 Marks)**

b. Encrypt the plaintext "VACCINATION" using a play fair cipher with a key "INDIA", also give rules for encryption. **(08 Marks)**

c. Mention the modular arithmetic operation properties and prove the same. **(06 Marks)**

OR

2 a. Draw the model of symmetric cryptosystem and explain it. **(08 Marks)**

b. Encrypt the plaintext "Hard Work" using Hill Cipher with key $\begin{vmatrix} 7 & 8 \\ 19 & 3 \end{vmatrix}$ and decrypt the same. **(08 Marks)**

c. Find the GCD of (2740, 1760) using Euclid's algorithm. **(04 Marks)**

Module-2

3 a. With neat diagram, explain AES encryption process. **(10 Marks)**

b. Explain the AES key expansion. **(10 Marks)**

OR

4 a. Draw the single round DES algorithm and explain the process in detail. **(10 Marks)**

b. Briefly explain the major transformations in AES algorithm. **(10 Marks)**

Module-3

5 a. Find the GCD [a(x), b(x)] for $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $b(x) = x^4 + x^2 + x + 1$. **(07 Marks)**

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

c. State and prove Fermat's theorem. **(07 Marks)**

OR

6 a. Find the GCD of [a(x), b(x)] for $a(x) = x^8 + x^4 + x^3 + x + 1$, $b(x) = x^5$. **(08 Marks)**

b. Define the following terms:
(i) Abelian group (ii) Integral domain (iii) Fields **(06 Marks)**

c. State and prove Euler's theorem. **(06 Marks)**

Module-4

7 a. Differentiate between a conventional encryption and public-key encryption. **(06 Marks)**

b. Mention the requirements for public key cryptography. **(06 Marks)**

c. Perform an encryption and decryption using RSA algorithm for p = 3, q = 11, e = 7 and m = 5. Find the cipher text 'c' and decrypt 'c' to get plaintext. **(08 Marks)**

OR

8 a. With a neat diagram explain public key cryptography. **(08 Marks)**

b. Explain in brief the Diffie Hellman key exchange algorithm. **(05 Marks)**

c. Write a note on elliptic curve arithmetic on the elliptic curve E23(1, 1) = P = (3, 10) and Q(9, 7). Find : (i) P + Q (ii) 2P **(07 Marks)**

Module-5

9 a. Explain linear feedback shift registers with necessary diagrams. **(08 Marks)**

b. Write a note on linear congruential generates. **(06 Marks)**

c. Explain the following with necessary diagrams:
   (i) Generalized Geffe Generator
   (ii) Threshold Generator **(06 Marks)**

OR

10 a. Explain the following with necessary diagrams:
   (i) Self decimated generators
   (ii) Gollmann cascade **(10 Marks)**

b. Write short notes on:
   (i) NANOTEQ
   (ii) RAMBOTAN
   (iii) GIFFORD Algorithms **(10 Marks)**

* * * * *

CMRIT LIBRARY
BANGALORE - 560 037
VTU 05-06-2023 01:13:49pm CR - CR - CR - CR - CR - CR
05-06-2023 01:34:28pm CR - CR - CR - CR - CR - CR