CBCS SCHEME

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

Seventh Semester B.E. Degree Examination, June/July 2025

Cryptography

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Explain the play fair cipher algorithm. Using the keyword "SAVE", decrypt the play fair cipher "ADRBOEDSOGNOZY". **(10 Marks)**

b. Construct multiplication and addition tables modulo 8. **(10 Marks)**

OR

2 a. For a particular one time pad, the key used is a steam of random numbers between 0 and 26. For example , if the key is 3 19 5 - - - - , then the first letter of plain test is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters and so on.

i) Encrypt the plain text "sendmoremoney" with the key stream –
9 0 1 7 23 15 21 14 11 11 2 8 9

ii) Using the cipher text produced in part(a), find a key so that the cipher text decrypts to the plaintext "cashnotneeded". **(10 Marks)**

b. Explain the extended Euclid's algorithm for determining the GCD and multiplicative inverse of two integers. Compute the multiplicative inverse of 11 in Z_{26}. **(10 Marks)**

Module-2

3 a. With relevant block diagram, explain the details of single round of DES. **(10 Marks)**

b. Explain the overall structure of the AES encryption process with relevant diagram. **(10 Marks)**

OR

4 a. With relevant block diagram, explain the Data Encryption Standard (DES). **(10 Marks)**

b. Differentiate the following terms :

i) SubBytes and subword
ii) ShiftRows and RotWord
iii) ShiftRows and MixColumns
iv) Confusion and Diffusion. **(10 Marks)**

Module-3

5 a. Define cyclic subgroups. Compute the cyclic subgroups that can be formed from the group, $G = \{Z_{10}^{*}, X\}$. **(10 Marks)**

b. Compute multiplicative inverse of the following using Fermat's little theorem :

i) 8^{-1} mode 17
ii) 60^{-1} mod 101 **(10 Marks)**

OR

6 a. Using Miller Rabin algorithm check whether 53 is a prime number? Also describe the algorithm. **(10 Marks)**

b. State and prove Euler's theorem. Compute the following :
$\phi(21)$, $\phi(12)$, $\phi(240)$, $\phi(13)$. **(10 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. Explain the principles involved in providing confidentiality and authenticity using public key cryptography. **(10 Marks)**

b. Perform encryption and decryption using RSA algorithm. Given p = 17, q = 11, e = 7 and m = 88. **(10 Marks)**

OR

8 a. In Diffie-Hellman key exchange algorithm q = 71, its primitive root $\alpha = 7$. A's private key is 5 and B's private key is 12 compute :

i) Public key of A
ii) Public key of B
iii) Shared secret key 'k' **(10 Marks)**

b. Compute (P + Q) and 2P for the elliptic curve $E_{23}(1, 1)$ with P(3, 10) and Q(9, 7). **(10 Marks)**

Module-5

9 a. Discuss the analysis of stream ciphers with respect to linear complexity and correlation immunity. **(10 Marks)**

b. Discuss the features of feedback shift registers and Linear Feedback Shift Registers (LFSRs) used in cryptography. **(10 Marks)**

OR

10 a. Explain LFSR based Jennings generator and Beth-Piper stop and – Go generator. **(10 Marks)**

b. Discuss the LFSR based Geffe generator and generalized Gefffe generator. **(10 Marks)**

* * * * *