| U.S.N. | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|

# B.M.S. College of Engineering, Bengaluru-560019

**Autonomous Institute Affiliated to VTU**

## January / February 2025 Semester End Main Examinations

**Programme: B.E.** **Semester: V**

**Branch: CSE (IoT & Cybersecurity including Blockchain)** **Duration: 3 hrs.**

**Course Code: 23IC5PCCRP** **Max Marks: 100**

**Course: CRYPTOGRAPHY**

**Instructions**: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

**Important Note:** Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

| | | **UNIT - I** | *CO* | *PO* | **Marks** |
|---|---|---|---|---|---|
| 1 | a) | Distinguish between passive and active security attacks. List and explain passive and active attacks with examples. | *CO1* | *PO2* | **05** |
| | b) | Describe transposition ciphers. Apply transposition ciphers to encrypt the message "SECURITY" using a columnar transposition cipher with key 31254. Find the decryption key. | *CO1* | *PO1* | **07** |
| | c) | Encrypt the message "attack" using the Hill cipher with the key matrix $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$. Show the steps of encryption. | *CO1* | *PO1* | **08** |
| | | **OR** | | | |
| 2 | a) | Use Vigenere Cipher with key HEALTH to encrypt the message "Life is full of surprises" | *CO1* | *PO1* | **06** |
| | b) | Use the extended Euclidean algorithm to find the inverse of $(x^4 + x^3 + 1)$ in $GF(2^5)$ using the modulus $(x^5 + x^2 + 1)$. | *CO1* | *PO1* | **08** |
| | c) | Find all subgroups and cyclic generators of $G = <Z_{11}^*, \times>$. | *CO1* | *PO1* | **06** |
| | | **UNIT - II** | | | |
| 3 | a) | If a message of 3000 characters is encrypted using a block cipher with a 64-bit block size, determine:<br>i) The total number of blocks required.<br>ii) The amount of padding added when padding is done to the nearest block boundary.<br>iii) How many substitution and permutation operations are performed in a cipher using 10 rounds of a substitution-permutation network, assuming each round has 4 mixers and 2 swappers? | *CO2* | *PO2* | **06** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | b) | Distinguish between modern symmetric-key ciphers and traditional symmetric-key ciphers based on their schemes, strengths and weaknesses, and performance with examples. | *CO2* | *PO2* | **08** |
| | | c) | Demonstrate with a neat diagram the key generation process in DES. | *CO1* | *PO1* | **06** |
| | | | **OR** | | | |
| | 4 | a) | Write the pseudocode for the Shiftrows, InvSubBytes transformation in AES. | *CO1* | *PO1* | **06** |
| | | b) | AES supports three different numbers of rounds (10, 12, and 14) based on key size, while Triple DES uses a fixed 16 rounds applied three times. Compare the advantages and disadvantages of AES over Triple DES with respect to the number of rounds. How does this difference affect security, performance, and compatibility? | *CO2* | *PO2* | **08** |
| | | c) | Design and demonstrate an encryption and decryption system using the Output Feedback (OFB) mode of AES. | *CO3* | *PO3* | **06** |
| | | | **UNIT - III** | | | |
| | 5 | a) | Find the values of the following Euler's Totient Function:<br>(a)$\phi(17)$<br>(b)$\phi(36)$<br>(c)$\phi(72)$ | *CO1* | *PO1* | **06** |
| | | b) | Solve the following problems using Fermat's Little Theorem:<br>$a)\quad 7^{25} \mod 13$<br>$b)\quad 23^{56} \mod 19$ | *CO1* | *PO1* | **06** |
| | | c) | Determine whether the integers 73 and 103 pass the Miller-Rabin primality test using base 2. Show all steps and calculations. | *CO1* | *PO1* | **08** |
| | | | **OR** | | | |
| | 6 | a) | Apply CRT to find the integer x which leave a remainder of 6, 13, 9 and 19 when divided by 11, 16, 21 and 25 respectively. | *CO1* | *PO1* | **10** |
| | | b) | Explain the concepts of Quadratic Residues (QRs) and Quadratic Non-Residues (QNRs) .Find QN and QNR for $Z_{11}$*. | *CO1* | *PO1* | **10** |
| | | | **UNIT - IV** | | | |
| | 7 | a) | Differentiate between symmetric-key and asymmetric-key cryptosystems with suitable examples. | *CO2* | *PO2* | **05** |
| | | b) | Find d and Perform Encryption and Decryption using RSA algorithm with p=3, q=11, e=7 and Message=5. | *CO1* | *PO1* | **07** |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  |  | c) | Alice uses Bob’s RSA public key (e = 3, n = 35) and sends the ciphertext 22 to Bob. Show how Eve can find the plaintext using the cycling attack. | *CO2* | *PO2* | **08** |
|  |  |  | **OR** |  |  |  |
|  | 8 | a) | In ElGamal, given the prime p = 31:<br>a. Choose an appropriate e1 and d, then calculate e2.<br>b. Encrypt the following messages “H”, “E” , “L”; use 00 to 25 for encoding. | *CO1* | *PO1* | **08** |
|  |  | b) | Consider an elliptic curve $E_{11}(1,1)$ over a finite field 11 ,the generator Point G is G = (6,6) . Bob choose the private value n = 2.<br>1) Find the equation of the curve.<br>2) Find at least five points on the curve<br>3) find the Public Key of Bob over elliptic Curve $P_b$ = n G. | *CO1* | *PO1* | **12** |
|  |  |  | **UNIT - V** |  |  |  |
|  | 9 | a) | Identify and explain the types of attacks on digital signatures. provide a specific example scenario that illustrates how the above attack could be carried out on digital signatures. | *CO2* | *PO2* | **10** |
|  |  | b) | Explain the HMAC construction process with neat diagram. | *CO1* | *PO1* | **10** |
|  |  |  | **OR** |  |  |  |
|  | 10 | a) | Demonstrate the steps of Kerberos authentication protocol with the help of a neat diagram. | *CO1* | *PO1* | **06** |
|  |  | b) | In the Diffie-Hellman protocol, g = 7, p = 23, x = 3, and y = 5.<br>a. Solve the value of the symmetric key?<br>b. Solve the value of R1 and R2? | *CO1* | *PO1* | **06** |
|  |  | c) | Create a neat diagram that clearly illustrates the structure of an X.509 certificate. Label each part of the certificate and briefly describe its purpose. | *CO1* | *PO1* | **08** |

******