| Roll No. | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

# PRESIDENCY UNIVERSITY

## BENGALURU

**Mid - Term Examinations – October 2025**

**Date:** 07-10-2025 **Time:** 02.00pm to 03.30pm

| | | |
|---|---|---|
| **School:** SOCSE | **Program:** B.Tech | |
| **Course Code:** IST2502 | **Course Name:** Foundations of Cryptography and Information Security | |
| **Semester**: V | **Max Marks**: 50 | **Weightage:**25% |

| **CO - Levels** | **CO1** | **CO2** | **CO3** | **CO4** |
|---|---|---|---|---|
| **Marks** | **24** | **26** | | |

**Instructions:**

*(i) Read all questions carefully and answer accordingly.*

*(ii) Do not write anything on the question paper other than roll number.*

## Part A

**Answer ALL the Questions. Each question carries 2marks.** **5Q x 2M=10M**

| | | | | |
|---|---|---|---|---|
| **1** | Define Cryptanalysis. | **2 Marks** | **L1** | **CO1** |
| **2** | List the two types of Passive Attacks. | **2 Marks** | **L1** | **CO1** |
| **3** | Name the AES transformation which performs a bitwise XOR operation with the round key. | **2 Marks** | **L1** | **CO2** |
| **4** | State two key issues that Public-Key Cryptography was developed to address. | **2 Marks** | **L1** | **CO2** |
| **5** | Define the purpose of the Diffie-Hellman key exchange algorithm. | **2 Marks** | **L1** | **CO2** |

## Part B

**Answer the Questions.** **Total Marks 40M**

| | | | | | |
|---|---|---|---|---|---|
| **6.** | **a.** | Classify the Classical Encryption Techniques of Substitution and Transposition Ciphers with suitable examples. | **10 Marks** | **L3** | **CO 1** |
| **Or** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **7.** | **a.** | Decrypt the following cipher text using Hill Cipher.<br>Key: $\begin{bmatrix} C & D \\ D & G \end{bmatrix}$<br>Ciphertext: FKMFIO | **10 Marks** | **L3** | **CO 1** |

| | | | | | |
|---|---|---|---|---|---|
| **8.** | **a.** | a) State Euler's Theorem and check the equality for *a*=3;*n*=10; ø(10)=4.<br>b) Demonstrate Euler Totient Function ø(n) | **10 Marks** | **L3** | **CO 1** |
| **Or** | | | | | |
| **9.** | **a.** | a) Encrypt the following text using the PLAYFAIR CIPHER.<br>Keyword: COMPARE<br>Plaintext: HIDDEN<br>b) Encrypt the following text using the Rail Fence cipher<br>d = 3<br>Plaintext: CRYPTOGRAPHY IS THE STUDY OF SECURE COMMUNICATION TECHNIQUES | **10 Marks** | **L3** | **CO 1** |

| | | | | | |
|---|---|---|---|---|---|
| **10.** | **a.** | Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 23 and a primitive root α = 5. If Bob has a public key YB = 10, calculate Bob’s private key XB? | **10 Marks** | **L3** | **CO 2** |
| **Or** | | | | | |
| **11.** | **a.** | Classify Single DES, 2-key Triple DES, and 3-key Triple DES. | **10 Marks** | **L3** | **CO 2** |

| | | | | | |
|---|---|---|---|---|---|
| **12.** | **a.** | Demonstrate the overall structure of the AES algorithm. | **10 Marks** | **L3** | **CO 2** |
| **Or** | | | | | |
| **13.** | **a.** | Perform RSA encryption and decryption for the given values: p = 7, q = 13, e = 11, M = 2 | **10 Marks** | **L3** | **CO 2** |