Roll No: | | | | | | | | | | | |

PRESIDENCY UNIVERSITY

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

Presidency University Act, 2013 of the Karnataka Act No. 41 of 2013 | Established under Section 2(f) of UGC Act, 1956
Approved by AICTE, New Delhi | Approved By BCI
Bengaluru

Mid Term Examinations - October 2026

Date: 06/10/2026 **Time:** 11:45 AM - 01:15 PM

Course Code: CSS2502 **Course Name:** Cryptography and Network Security

Semester: Fifth Semester **Max. Marks:** 50 **Weightage:** 50%

CO - Levels	CO1	CO2
Marks	46	44

PART A: Answer Following Questions. 10 M

Q.N.	Questions	M	CO	BT
1	List the five ingredients of a symmetric encryption model.	2	CO1	BT1
2	Mention any two characteristics of cryptography.	2	CO1	BT1
3	Who is a cryptanalyst?	2	CO1	BT1
4	What is a stream cipher?	2	CO2	BT1
5	What are diffusion and confusion?	2	CO2	BT1

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	Explain the Caesar cipher mathematically with encryption and decryption procedures. Illustrate with an example.	10	CO1	BT2
7	Explain the Hill cipher encryption and decryption process with the support of the following example. Example: Key= HILL Plaintext=exam	10	CO1	BT2

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	Explain the Playfair cipher algorithm with its key matrix and encryption rules. Encrypt the follwing message "Balloon" by using the keyword "MONARCHY.	10	CO1	BT2
9	Explain the Vigenère cipher and discuss its security characteristics.	10	CO1	BT2

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
10	Explain the Feistel cipher structure with a neat diagram. Discuss its design elements.	10	CO2	BT2
11	Explain the AES structure and encryption process with a neat diagram.	10	CO2	BT2

PART E: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
12	Explain the Chinese Remainder Theorem (CRT) and find X for the given set of congruent equations using CRT $X \equiv 2 \pmod 3$ $X \equiv 3 \pmod 5$ $X \equiv 2 \pmod 7$.	10	CO2	BT2

13	Explain the Extended Euclidean Algorithm and its application in finding multiplicative inverses.	10	CO2	BT2