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: 07/10/2026 **Time:** 09:30 AM - 11:00 AM

Course Code: CBD2504 **Course Name:** Data Security and Cryptography

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	Explain what symmetric cryptography is and how it works.	2	CO1	BT2
2	What is a masquerade attack?	2	CO1	BT1
3	Write Euclid's GCD Algorithm.	2	CO1	BT1
4	What is the purpose of the S-box in DES?	2	CO2	BT2
5	Differentiate between properties confusion and diffusion .	2	CO2	BT2

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	Explain Hill Cipher . Use Hill Cipher to encrypt the plaintext, "EXAM" using the key, "HILL".	10	CO1	BT3
7	Write Euler's theorem. Find multiplicative inverse of 7 mod 15.	10	CO1	BT3

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	Explain the different types of passive and active security attacks with suitable examples. For each type, clearly indicate which security goal (confidentiality, integrity, or availability) is primarily affected and suggest one appropriate countermeasure.	10	CO1	BT3
9	Explain the working principle of the Playfair Cipher, including the rules for constructing the key matrix and performing encryption. Using the key “MONARCHY”, encrypt the plaintext “INSTRUMENTS” using the Playfair Cipher. Show all the steps clearly.	10	CO1	BT3

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
10	Explain the working of the Data Encryption Standard (DES), including the implementation of its rounds.	10	CO2	BT2
11	Explain the four functions used in Advanced Encryption Standard.	10	CO2	BT2

PART E: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT

PTO (Please Turn Over)

12	Illustrate the Diffie Hellmann Key exchange process with suitable diagram	10	CO2	BT3
13	Explain the RSA algorithm with the help of the following parameters. Let p = 17, q = 11 and e = 7. 1. Generate the public key and private key. 2. Using the obtained keys, encrypt the plaintext, M = 8 3. Decrypt the resulting ciphertext and verify that the original plaintext is recovered.	10	CO2	BT3