Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – October 2025

Date: 08-10-2025 **Time:** 02.00pm to 03.30pm

School: SOIS	**Program:** BCA	
Course Code: CSA3027	**Course Name:** Cryptography and Network Security	
Semester: V	**Max Marks**: 50	**Weightage**: 25%

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

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.	Name the three key security goals defined in the OSI security architecture.	2	L1	CO1
2.	What is the primary purpose of the Feistel network structure?	2	L1	CO1
3.	Compare active and passive attacks.	2	L2	CO1
4.	What is the purpose of Euclidean Algorithm?	2	L1	CO2
5.	List the differences between DES and AES.	2	L1	CO2

Part B

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

6.	**a.**	Explain active and passive attacks with suitable examples.	10	L2	CO1
	b.	Illustrate the following services with examples: Authentication, Access Control, Data Confidentiality, Data Integrity, and Non-repudiation.	10	L2	CO1
OR					
7.	**a.**	Apply Feistel structure principles to show how encryption and	10	L3	CO1

		decryption are similar in design.			
	b.	List and explain the three fundamental concepts of the OSI security architecture.	10	L1	CO1

8.	**a.**	Explain the structure of DES with a neat diagram and describe its working principle.	10	L2	CO2
	b.	Compare and contrast the DES and AES algorithms in detail.	10	L2	CO2
OR					
9.	**a.**	Explain the properties of modular arithmetic with suitable examples.	10	L2	CO2
	b.	Explain the steps of AES encryption process (SubBytes, ShiftRows, MixColumns, AddRoundKey) in detail.	10	L2	CO2