Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – MAY 2025

Date: 27-05-2025 **Time:** 09:30 am – 12:30 pm

School: SOIS	**Program:** BCA/BCADS/BCAAIML	
Course Code: CSA3027	**Course Name:** Cryptography and Network Security	
Semester: VI	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	CO1	CO2	CO3	CO4
Marks	24	26	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. **10Q x 2M=20M**

1.	What is plaintext and ciphertext?	**2 Marks**	**L1**	**CO1**
2.	Explain the importance of key management.	**2 Marks**	**L1**	**CO1**
3.	Define modular arithmetic with an example.	**2 Marks**	**L1**	**CO2**
4.	What is discrete logarithm problem?	**2 Marks**	**L1**	**CO2**
5.	Define Euler's totient function with example.	**2 Marks**	**L1**	**CO2**
6.	What is a digital certificate?	**2 Marks**	**L1**	**CO3**
7.	Define HMAC and its purpose.	**2 Marks**	**L1**	**CO3**
8.	What is the main idea behind RSA algorithm?	**2 Marks**	**L1**	**CO3**
9.	What is PGP in email security?	**2 Marks**	**L1**	**CO4**
10.	What is cryptographic hash function?	**2 Marks**	**L1**	**CO4**

Part B

Answer the Questions. **Total Marks 80M**

11.	**a.**	Differentiate authentication and authorization.	**4 Marks**	**L2**	**CO1**
	b.	Describe the model of network security.	**8 Marks**	**L2**	**CO1**
	c.	Explain monoalphabetic cipher with suitable example.	**8 Marks**	**L2**	**CO1**
		Or			
12.	**a.**	Explain stream cipher structure.	**4 Marks**	**L2**	**CO1**
	b.	Encrypt 'DATA' using Caesar cipher with key 3.	**8 Marks**	**L3**	**CO1**
	c.	Discuss OSI security layers.	**8 Marks**	**L2**	**CO1**

13.	**a.**	Explain Euclidean and Extended Euclidean algorithm.	**4 Marks**	**L2**	**CO2**
	b.	Explain the working of DES with diagram.	**8 Marks**	**L2**	**CO2**
	c.	Solve GCD(60,13) using Extended Euclidean Algorithm.	**8 Marks**	**L3**	**CO2**
		Or			
14.	**a.**	What is modular inverse? Explain with example.	**4 Marks**	**L2**	**CO2**
	b.	Describe AES structure and steps.	**8 Marks**	**L2**	**CO2**
	c.	State and prove Fermat's Little Theorem briefly.	**8 Marks**	**L2**	**CO2**

15.	**a.**	List applications of cryptographic hash functions.	**4 Marks**	**L2**	**CO3**
	b.	Perform RSA encryption (p=3, q=11, e=7, m=9).	**8 Marks**	**L3**	**CO3**
	c.	Explain digital signature generation and verification.	**8 Marks**	**L2**	**CO3**
		Or			
16.	**a.**	Define RSA algorithm steps.	**4 Marks**	**L2**	**CO3**
	b.	Compare SHA-1 and MD5 algorithms.	**8 Marks**	**L2**	**CO3**
	c.	Explain Diffie-Hellman Key Exchange protocol.	**8 Marks**	**L2**	**CO3**

17.	**a.**	Describe email security through S/MIME.	4 Marks	**L2**	**CO4**
	b.	Define Kerberos and explain its purpose.	**8 Marks**	**L2**	**CO4**
	c.	Explain IP Security (IPSec) architecture.	**8 Marks**	**L2**	**CO4**
		Or			
18.	**a.**	Explain Web security issues and solutions.	**4 Marks**	**L2**	**CO4**
	b.	What are SSL and TLS protocols?	**8 Marks**	**L2**	**CO4**
	c.	Describe components of PKI system.	**8 Marks**	**L2**	**CO4**