Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – MAY/ JUNE 2025

Date: 02-06-2025 **Time:** 01:00 pm – 04:00 pm

School: SOCSE	**Program:** B. Tech-CBC	
Course Code : CSE3169	**Course Name:** Modern Cryptography	
Semester: IV	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	CO1	CO2	CO3	CO4	CO5
Marks	32	28	20	20	-

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.	Differentiate between substitution and transposition ciphers, highlighting their primary differences.	**2 Marks**	**L2**	**CO1**
2.	Identify and explain the security principle that ensures a sender or receiver cannot deny their participation in a communication.	**2 Marks**	**L1**	**CO1**
3.	Examine the key differences between mono-alphabetic and poly-alphabetic ciphers, providing a suitable example.	**2 Marks**	**L2**	**CO1**
4.	Explain the concept of cryptanalysis and its significance in breaking cryptographic systems.	**2 Marks**	**L2**	**CO2**
5.	Compute $7^{100} \pmod{40}$ using Euler's Theorem.	**2 Marks**	**L1**	**CO2**
6.	Explain what is meant by the term "deterministic" in the context of hashing.	**2 Marks**	**L2**	**CO1**
7.	Differentiate between a collision-resistant and a non-collision-resistant hash function.	**2 Marks**	**L1**	**CO2**
8.	Describe the concept of cryptojacking and how it affects system performance.	**2 Marks**	**L2**	**CO1**
9.	Analyze how a Man-in-the-Middle (MiTM) attack compromises communication security.	**2 Marks**	**L1**	**CO2**
10.	What is Firesheep and what role did it play in raising awareness of session hijacking?	**2 Marks**	**L2**	**CO1**

Part B

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

11.	**a.**	Explain the significance of safeguarding data in motion and at rest. How do encryption techniques contribute to ensuring data security?	**10 Marks**	**L2**	**CO1**
	b.	Demonstrate the process of setting up a VPN on a Windows system, outlining each step involved and explaining the purpose of key configuration settings.	**10 Marks**	**L3**	**CO2**

		Or			
12.	**a.**	Examine the concept of security services as defined by the ITU-T X.800 standard. Provide real-world examples illustrating how these services protect data from potential security threats.	**10 Marks**	**L2**	**CO2**
	b.	Describe the TLS handshake and TLS record protocols, and illustrate the flow of communication using suitable diagrams.	**10 Marks**	**L3**	**CO4**
13.	**a.**	Identify different cryptographic techniques used for securing data. Demonstrate your understanding of substitution and transposition ciphers by explaining their mechanisms and providing relevant examples.	**10 Marks**	**L2**	**CO2**
	b.	Explain the role of hashing in message authentication, and discuss how MAC and HMAC provide integrity and authenticity.	**10 Marks**	**L3**	**CO3**
		Or			
14.	**a.**	Discuss the concept of a Trusted Third Party (TTP) in the context of Public Key Infrastructure (PKI). Assess the role of PKI in enhancing secure communication, emphasizing its impact on authentication and trust.	**10 Marks**	**L2**	**CO2**
	b.	Compare the GDPR and CCPA data privacy regulations, focusing on aspects such as consumer rights, regulatory scope, and enforcement mechanisms	**10 Marks**	**L3**	**CO3**
15.	**a.**	Investigate various cyber threats that specifically target data security. Propose and justify effective strategies that organizations can implement to mitigate these threats.	**10 Marks**	**L2**	**CO1**
	b.	Demonstrate the step-by-step process of generating a digital signature, and highlight the underlying cryptographic techniques.	**10 Marks**	**L3**	**CO3**
		Or			
16.	**a.**	Explain the Affine Cipher and demonstrate its encryption process with an example where $\alpha = 5$ and $\beta = 8$, and the plaintext is "HELLO".	**10 Marks**	**L2**	**CO1**
	b.	Outline the major components and objectives of HIPAA, and evaluate its effectiveness in safeguarding patient health information (PHI)	**10 Marks**	**L3**	**CO3**
17.	**a.**	Define Non-Repudiation in cybersecurity and describe its importance. Illustrate how digital signatures help achieve non-repudiation with a relevant example.	**10 Marks**	**L2**	**CO1**
	b.	Explain how encryption can be exploited in malware and ransomware attacks, and analyze their implications for cybersecurity defense strategies.	**10 Marks**	**L3**	**CO4**
		Or			
18.	**a.**	Given the RSA encryption system with prime numbers $p = 23$ and $q = 17$, and public encryption key $e = 3$: a) Compute the decryption key d using appropriate mathematical steps. b) Demonstrate the decryption of the ciphertext C=165 using modular exponentiation, ensuring a clear breakdown of each step in the computation.	**10 Marks**	**L2**	**CO1**
	b.	Describe how Pretty Good Privacy (PGP) ensures confidentiality, integrity, and authenticity in email communications.	**10 Marks**	**L3**	**CO4**