

CBCS SCHEME

USN

--	--	--	--	--	--	--	--	--	--

MMCH311C

Third Semester MCA Degree Examination, June/July 2026 Cryptography and Network Security

Time: 3 hrs.

Max. Marks: 100

*Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M : Marks , L: Bloom's level , C: Course outcomes.*

		Module – 1	M	L	C
Q.1	a.	Explain the fundamental goals of computer security. Describe Confidentiality, Integrity, and Availability (CIA Triad) with suitable examples. Also explain the need for security in modern computer systems.	10	L2	CO1
	b.	Classify security attacks into passive and active attacks. Given the following scenarios, identify the type of attack and justify: i) An attacker secretly reads confidential emails ii) A website is flooded with fake requests iii) A message is altered during transmission iv) A fake login page is used to steal credentials	10	L3	CO1
OR					
Q.2	a.	Describe the OSI Security Architecture proposed by ISO. Clearly describe i) Security Attacks ii) Security Services iii) Security Mechanisms and show how they are related using a neat diagram.	10	L2	CO1
	b.	Explain the Rail Fence Transposition Cipher. Encrypt the plaintext "CRYPTOGRAPHY AND NETWORK SECURITY" using 3 rails and show all steps. Analyze how transposition differs from substitution in terms of security strength.	10	L3	CO1
Module – 2					
Q.3	a.	Explain the following block cipher modes of operation with suitable diagrams: • Electronic Codebook (ECB) • Cipher Block Chaining (CBC) • Cipher Feedback (CFB) • Output Feedback (OFB)	10	L2	CO1

	b.	Explain the concept of Multiple Encryption and describe the working of Triple DES (3DES) with encryption and decryption equations. Highlight how 3DES improves security over DES.	10	L2	CO2
OR					
Q.4	a.	With a neat diagram, explain the DES encryption process and illustrate a DES example showing how plaintext is transformed into cipher text through the 16 rounds.	10	L2	CO2
	b.	Explain stream ciphers and RC4 cipher. Describe the key scheduling algorithm (KSA) and pseudo-random generation algorithm (PRGA) of RC4, and discuss its security issues.	10	L2	CO2
Module – 3					
Q.5	a.	Explain Euler's Totient Function. Find $\phi(40)$ and hence evaluate $3^{20} \bmod 40$ using Euler's theorem	10	L3	CO3
	b.	Describe the RSA algorithm with key generation, encryption, and decryption steps. Given $p = 11$, $q = 17$, and $e = 7$, Compute the public and private keys Encrypt the message $M = 9$ Decrypt the cipher text to verify correctness	10	L3	CO3
OR					
Q.6	a.	Apply Chinese Remainder Theorem (CRT) to solve the simultaneous congruences: $x \equiv 2 \pmod{3}$ $x \equiv 3 \pmod{4}$ $x \equiv 1 \pmod{5}$	10	L3	CO3
	b.	Explain the Diffie-Hellman key exchange protocol with a neat diagram. Given $p = 23$, $g = 5$, - Alice chooses $a = 6$, Bob chooses $b = 15$ - Compute the public values exchanged - Determine the shared secret key	10	L3	CO4

Module – 4					
Q.7	a.	Write short notes among the following a) Security of MAC b) Difference between HMAC & MAC	10	L2	CO4
	b.	Explain how CBC-MAC and HMAC operate with neat diagram and Compare their performance, security, and suitable applications.	10	L2	CO4
OR					
Q.8	a.	Explain the working principle of Message Authentication Codes (MACs). Demonstrate how a MAC is generated and verified using a shared secret key with a suitable example.	10	L3	CO4
	b.	Explain the Secure Hash Algorithm (SHA) in detail. Describe the major steps involved in SHA-1 or SHA-256 and explain how message digest is generated	10	L2	CO4
Module – 5					
Q.9	a.	Explain the concept of Digital Signatures. Describe the requirements and properties of a secure digital signature system. Illustrate the generic digital signature process with a neat diagram.	10	L2	CO4
	b.	Apply the concept of Public Key Infrastructure (PKI) to explain how secure communication is established in an organization. Describe the roles of CA, RA, and certificate repositories with a neat diagram.	10	L3	CO5
OR					
Q.10	a.	Explain the ElGamal Digital Signature Scheme. Describe the key generation, signature generation, and signature verification steps in detail.	10	L2	CO5
	b.	Illustrate how symmetric and asymmetric key distribution differ in steps and security with proper example	10	L3	CO5