

25MCST403	NETWORK SECURITY	Category	L	T	P	R	Credit	Year of Introduction
		VAC	4	0	0	0	4	2025

Preamble: The rapid growth of digital communication and connected systems has made information security an essential foundation for all computing applications. This minor course introduces the fundamental principles of cryptography and network security required for protecting data and ensuring secure communication. It provides an entry-level understanding of classical and modern encryption techniques, authentication mechanisms, network attacks, and basic protection strategies used in real-world systems.

Prerequisite: Nil

Course Outcomes: After the completion of the course, the student will be able to:

CO	Course Outcomes	Knowledge Level
CO1	Describe the fundamental principles of Network Security.	K2 Understand
CO2	Apply classical and modern cryptographic techniques for secure communication.	K3 Apply
CO3	Apply hashing, message authentication, and basic digital signature concepts to verify integrity and authenticity.	K3 Apply
CO4	Explain network security protocols and protection mechanisms.	K2 Understand

Mapping of course outcomes with program outcomes and program specific outcomes

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	2	1	–	–	–	2	3	–	–	–	2	1	–
CO2	2	1	1	–	2	–	2	–	–	–	2	–	1
CO3	2	1	2	2	2	–	2	–	–	–	2	–	1
CO4	2	1	1	–	2	2	3	–	–	–	2	1	–
Avg	2	1	1.33	2	2	2	2.5	–	–	–	2	1	1

Mapping of course outcomes with Knowledge and Attitude Profile (WK)

	WK1	WK2	WK3	WK4	WK5	WK6	WK7	WK8	WK9
CO1	*	*	*	*	*		*	*	*
CO2	*	*	*	*	*	*		*	*
CO3	*	*	*	*	*	*		*	*
CO4	*	*	*	*	*	*	*	*	*

Wks Mapped with the course

WK1	WK2	WK3	WK4	WK5	WK6	WK7	WK8	WK9
*	*	*	*	*	*	*	*	*

Mark Distribution:

Total Marks	CIE Marks	ESE Marks	ESE Duration
100	40	60	2.5 hrs

Continuous Internal Evaluation Pattern:

Attendance	: 5 marks
Continuous Assessment Test	: 20 marks
Continuous Assessment Assignment	: 15 marks

SYLLABUS**Module 1 (14 hrs)**

Introduction to Network Security, Need for Security in Modern Digital Systems, Security Goals, Confidentiality, Integrity, Availability (CIA Triad), Vulnerabilities, Threats and Attacks, Security Services and Mechanisms, Network security model, Symmetric cipher model, Steganography.

Module 2 (14 hrs)

Classical Cryptography, Modern Symmetric-Key Cryptography, Block ciphers and Stream ciphers, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Public Key crypto system, RSA algorithm, Key Management, Diffie–Hellman Key Exchange.

Module 3 (14 hrs)

Authentication functions, Message Authentication Codes (MAC), Hash functions, HMAC, CMAC, MD 5, SHA, Digital signatures: Properties, Attacks and forgeries, NIST Digital signature algorithm, Elgamal signature scheme.

Module 4 (14 hrs)

Secure Communication Protocols, SSL/TLS, HTTPS, secure web communication, IPsec – AH & ESP, Network Protection Mechanisms, Firewalls – types & basic rule, Intrusion detection, Antivirus & Malware Protection, Virtual Private Networks (VPN) – concept & benefits, Security in Modern Environments, Cloud security fundamentals, Basics of IoT Security.

Text Books:

1. Stallings, W. (2023). *Cryptography and network security: Principles and practice (8th ed.)*. Pearson Education.
2. Kahate, A. (2021). *Cryptography and network security (3rd ed.)*. McGraw-Hill Education.
3. Forouzan, B. A., & Mukhopadhyay, D. (2020). *Cryptography and network security (3rd ed.)*. McGraw-Hill Education.

Reference Books:

1. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2020). *Handbook of applied cryptography*. CRC Press.
2. Stamp, M. (2021). *Information security: Principles and practice (2nd ed.)*. Wiley.
3. Schneier, B. (2000). *Applied cryptography: Protocols, algorithms, and source code in C (2nd ed.)*. Wiley.

END SEMESTER EXAMINATION – MODEL QUESTION PAPER

Course Code	25MCST403
Course Name	NETWORK SECURITY
Max. Marks: 60	Duration: 2.5 Hours

Part A <i>(Answer all questions. Each question carries 3 marks)</i>				
Qn No.	Question	Marks	CO	BL
1	Describe CIA Triad with a neat sketch.	3	1	L2
2	Explain symmetric cipher model with a diagram.	3	1	L2
3	Encrypt the message $M = 7$ using $p = 11$, $q = 13$ and public key $e = 7$ using RSA Algorithm.	3	2	L3
4	Apply shift row and inverse shift row transformations in the following state of AES algorithm with suitable comments.	3	2	

		63	C9	FE	30				L3
		F2	F2	63	26				
		C9	82	24	FA				
		D4	18	7D	0D				
5	Identify two known weaknesses of MD5 that make it unsuitable for security-critical applications, citing their practical impact.						3	3	L3
6	Compare SHA-1 and SHA-256 in terms of digest size, block size, and current security status.						3	3	L3
7	Explain about cloud security.						3	4	L2
8	Differentiate between HTTP and HTTPS.						3	4	L2
Part B <i>(Answer any one full question from each Module. Each carry 9 marks)</i>									
Module I									
Qn No.	Question						Marks	CO	BL
9.a	Explain Network security model with a neat diagram.						5	1	L2
9.b	Explain steganography with example.						4	1	L2
OR									
10	Describe the different types of security services with examples.						9	1	L2
Module II									
Qn No.	Question						Marks	CO	BL
11	Given two prime numbers $p = 13$ and $q = 19$, generate the RSA public and private keys. Choose a suitable public exponent e , compute the corresponding private key exponent d , and encrypt the message $M = 12$ using the generated public key. Show all calculations.						9	2	L3
OR									
12	Using the Diffie–Hellman Key Exchange Protocol, calculate the shared secret key for the following parameters: $q = 13$, $\alpha = 2$, User A's private key $X_a = 5$, and User B's private key $X_b = 9$. Determine the public keys and the common secret key.						9	2	L3
Module III									
Qn No.	Question						Marks	CO	BL
13	Using Elgamal digital signature scheme, generate and verify the signature with the following data. $M=14$, $q=19$, $X_A = 16$, $K=5$, $\alpha = 10$.						9	3	L3
OR									

14	Derive the HMAC construction from a generic hash function H. Prove informally that HMAC is secure if H is a pseudo-random function.	9	3	L3
Module IV				
Qn No.	Question	Marks	CO	BL
15.a	Describe Authentication header (AH) in IP security with necessary diagrams.	5	4	L2
15.b	Explain the functionalities of SSL Record protocol.	4	4	L2
OR				
16	Explain any two network protection mechanisms.	9	4	L2
