

25UCST413	CRYPTOGRAPHY AND NETWORK SECURITY	Category	L	T	P	R	Credit	Year of Introduction
		PEC	3	0	0	0	3	2025

Preamble: This course introduces the fundamental concepts of information and network security. It covers basic cryptographic principles, security mechanisms, and protection techniques used in communication systems. The course provides an overview of how data confidentiality, integrity, and authentication are ensured in digital environments. Overall, it helps students understand the importance of securing modern information systems.

Prerequisite: Nil

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

CO	Course Outcomes	Knowledge Level
CO1	Explain network security fundamentals, classical encryption, security services, and security mechanisms.	K2 Understand
CO2	Apply cryptographic techniques to secure data in communication systems.	K3 Apply
CO3	Apply authentication functions, MAC, hashing techniques, and digital signature schemes for data integrity and authentication.	K3 Apply
CO4	Describe Kerberos, E-mail security, IP security, web security, and firewall 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	3	2	–	–	–	1	-	–	–	–	1	2	1
CO2	3	3	2	1	–	–	1	–	–	–	1	3	2
CO3	3	3	2	1	–	–	1	–	–	–	1	3	2
CO4	3	2	1	–	1	–	-	–	–	–	1	3	1
Avg	3	2.5	1.6	1	1	1	1	–	–	–	1	2.75	1.5

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 (10 hrs)

Need for information security, goals of security. Types of attacks: passive & active. Classical ciphers: substitution and transposition techniques, Security services: confidentiality, integrity, authentication, non-repudiation, Security Mechanisms: specific and pervasive.

Module 2 (10 hrs)

Symmetric key encryption, block vs stream ciphers, Basic idea of Data Encryption Standard (DES) & Advanced Encryption Standard (AES). Public-key cryptography: RSA Algorithm, Diffie-Hellman key exchange.

Module 3 (10 hrs)

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

Module 4 (12 hrs)

User authentication principles, Kerberos, Transport level security: Secure socket layer (SSL) Transport layer security (TLS), Email security: Pretty good privacy (PGP), IP security overview, Firewalls.

Text Books:

1. Stallings, W. (2023). *Cryptography and network security: Principles and practice (8th ed.)*. Pearson Education.
2. Kahate, A. (2016). *Cryptography and network security (3rd ed.)*. McGraw-Hill Education.
3. Forouzan, B. A., & Mukhopadhyay, D. (2015). *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. (Widely used as a reference in cryptography)
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	25UCST413
Course Name	CRYPTOGRAPHY AND NETWORK SECURITY
Max. Marks: 60	Duration: 2.5 Hours

Part A																				
(Answer all questions. Each question carries 3 marks)																				
Qn No.	Question	Marks	CO	BL																
1	Differentiate between active and passive attack.	3	1	L2																
2	Explain the need for Information security.	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. <table><tr><td>63</td><td>C9</td><td>FE</td><td>30</td></tr><tr><td>F2</td><td>F2</td><td>63</td><td>26</td></tr><tr><td>C9</td><td>82</td><td>24</td><td>FA</td></tr><tr><td>D4</td><td>18</td><td>7D</td><td>0D</td></tr></table>	63	C9	FE	30	F2	F2	63	26	C9	82	24	FA	D4	18	7D	0D	3	2	L3
63	C9	FE	30																	
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	Describe the uses and types of firewalls.	3	4	L2
8	Explain Kerberos.	3	4	L2
Part B (Answer any one full question from each Module. Each carry 9 marks)				
Module I				
Qn No.	Question	Marks	CO	BL
9	Explain any three substitution ciphers with example.	9	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	Using Diffie-Hellman key exchange protocol solve the following problem. Let common prime $q=11$ and primitive root $\alpha = 2$. 1. If user A has public key $Y_A = 9$. Find private key X_A . 2. If User B has public key $Y_B = 3$. Find the shared secret key K . 3. Prove that 2 is the primitive root of 11.	9	2	L3
OR				
12	Given two primes $p = 17$ and $q = 11$, perform complete RSA key generation. Verify that your chosen public exponent e is valid, compute the private key d using the Extended Euclidean Algorithm (show all steps), and confirm that $ed \equiv 1 \pmod{\phi(n)}$.	9	2	L3
Module III				
Qn No.	Question	Marks	CO	BL
13	Using Elgamal digital signature scheme, develop 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	Explain Secure Socket Layer (SSL) with necessary diagrams .	9	4	L2
OR				
16	Describe Pretty Good Privacy (PGP).	9	4	L2
