25UCST415	SECURITY IN COMPUTING	Category	L	T	P	R	Credit	Year of Introduction
		PEC	3	0	0	0	3	2025

Preamble: This course explores the algorithms used to ensure data confidentiality, integrity, authentication, and non-repudiation while analyzing system attacks and their defenses. From classical encryption and symmetric/public-key systems to key distribution and authentication, the curriculum covers the mechanics of securing data against intruders, malware, and DDoS attacks. Ultimately, learners gain the practical expertise to apply cryptographic tools and countermeasures to protect real-world applications.

Prerequisite: Nil

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

CO	Course Outcomes	Knowledge Level
CO1	Explain the fundamentals of network security and basic cryptographic techniques.	K2 Understand
CO2	Apply symmetric and public key cryptographic techniques for secure communication.	K3 Apply
CO3	Describe message integrity and authentication methods in a secure communication scenario.	K2 Understand
CO4	Explain key concepts of network and system security 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	2	–	–	–	–	–	–	–	–	–	2	–
CO2	3	3	2	1	2	–	–	–	–	–	–	2	3
CO3	2	2	–	–	1	–	–	–	–	–	–	2	–
CO4	2	2	–	–	1	–	1	–	–	–	–	2	1
Avg	2.25	2.25	2	1	1.33	–	1	–	–	–	–	2	2

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 (12 hrs)

Introduction: Security basics - Aspects of network security - Attacks Different types - Security attacks - Security services and mechanisms. Cryptography: Basic Encryption & Decryption -Classical encryption techniques - symmetric encryption, substitution ciphers:Caesar cipher ,Monoalphabetic Cipher, Playfair Cipher, Polyalphabetic cipher,Vigenère,Cipher, Transposition ciphers : Rail Fence cipher, Row Transposition Ciphers

Module 2 (10 hrs)

Modern Block Ciphers - Fiestel Networks , DES Algorithm - Avalanche Effect. Public key Cryptography:- Principles of Public key Cryptography Systems, RSA algorithm, Key Management , Diffie-Hellman Key Exchange,Elgamal Crypto System .

Module 3 (10 hrs)

Message Authentication-Requirements- Authentication functions- Message authentication codes-Hash functions- Secure Hash Algorithm(SHA 512) , MD5, Digital signatures- protocols- Digital signature standards, Elgamal digital signature scheme.

Module 4 (10 hrs)

Network Security: Electronic Mail Security, Pretty Good Privacy, IP Security Overview, IP Security

Architecture, Web Security: Web Security considerations- Secure Socket Layer -Transport layer Security, Secure electronic transaction, System Security: Intruders, Intrusion Detection, Password Management, Viruses and Related Threats, Virus Countermeasure.

Text Books:

1. Stallings, W. (2023). *Cryptography and network security: Principles and practice (8th ed.).* Pearson Education.
2.Kahate, A. (2020). *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. (2023). *Handbook of applied cryptography. CRC Press.*
2.Stamp, M. (2022). *Information security: Principles and practice (2nd ed.).* Wiley.
3.Schneier, B. (2021). *Applied cryptography: Protocols, algorithms, and source code in C (2nd ed.).* Wiley.

END SEMESTER EXAMINATION – MODEL QUESTION PAPER

Course Code	**25UCST415**
Course Name	**SECURITY IN COMPUTING**
Max. Marks: 60	**Duration: 2.5 Hours**

Part A

(Answer all questions. Each question carries 3 marks)

Qn No.	Question	Marks	CO	BL
1	Identify the type of security attack in each of the following cases. Justify your answer. a) A hacker gains access to a company's server and copies confidential customer data without altering anything. b) A disgruntled employee deletes important files from the company's database before quitting.	3	1	L2
2	Distinguish between symmetric and asymmetric encryption.	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	Explain public cryptosystem.	3	2	L2
5	Differentiate MAC and Hash function.	3	3	L2
6	Explain the requirements of Message Authentication Code.	3	3	L2
7	Describe three different classes of Intruders.	3	4	L2
8	Explain the phases of virus.	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 attacks with examples.	9	1	L2
Module II				
Qn No.	**Question**	**Marks**	**CO**	**BL**
11	Using Diffie-Hellaman 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	Consider an Elgamal cryptographic scheme with a common prime q=71 and primitive root $\alpha = 7$. 1. If B has a public key $Y_B = 3$ and A choose the random integer k = 2. Find the cipher text of the message M=30. 2. If A now choose a different value of k, so that the encoding of M = 30 is C = (59, C2). Find the value of C2.	9	2	L3
Module III				
Qn No.	**Question**	**Marks**	**CO**	**BL**
13	Explain Digital Signature Algorithm (DSA).	9	3	L2
OR				
14	Demonstrate the working of SHA 512 with necessary diagrams.	9	3	L2
Module IV				
Qn No.	**Question**	**Marks**	**CO**	**BL**
15	Differentiate between statistical anomaly detection and rule-based intrusion detection.	9	4	L2
OR				
16. a	Explain the services offered by Pretty Good Privacy (PGP).	4	4	L2
16. b	Describe Secure Electronic transaction with necessary diagrams.	5	4	L2

******