Xavier Institute of Engineering
Mahim, Mumbai 400016
Department of Computer Engineering
(Affiliated to University of Mumbai)

Lesson Plan 2024-25

Class : TE **Subject** : Cryptography and System Security (CSC602) **Semester** : VI

Course Objectives:
1. To introduce classical encryption techniques and concepts of modular arithmetic and number theory.
2. To explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithms.
3. To explore the design issues and working principles of various authentication protocols, PKI standards and various secure communication standards including Kerberos, IPsec, and SSL/TLS.
4. To develop the ability to use existing cryptographic utilities to build programs for secure communication.

CO	CO Statement	PO Mapped
1	Apply classical encryption techniques and the mathematics behind cryptography.	PO1, PO2, PO3, PO4, PO5, PO10
2	Compare and apply different modern encryption and decryption techniques to solve problems related to confidentiality and authentication.	PO1, PO2, PO3, PO4, PO5, PO10, PO12
3	Review different message digest algorithms to achieve integrity.	PO1, PO2, PO3, PO4, PO5, PO10, PO12
4	Explain different authentication protocols and digital signature schemes to achieve authentication.	PO1, PO2, PO3, PO4, PO5, PO10, PO12
5	Explore network security basics, different attacks and software vulnerabilities.	PO1, PO2, PO3, PO4, PO5, PO10, PO12
6	Understand recent trends and research in cryptography technologies and their future.	PO1, PO2, PO3, PO4, PO5, PO10, PO12

Text Books:

1. **William Stallings, "Cryptography and Network Security, Principles and Practice", 6th Edition, Pearson Education, March 2013.**
2. **Behrouz A. Ferouzan, "Cryptography & Network Security", Tata McGraw Hill**
3. **Behrouz A. Forouzan & Debdeep Mukhopadhyay, "Cryptography and Network Security" 3rd Edition, McGraw Hill**

Refernce Books:

1. **Bruce Schneier, "Applied Cryptography, Protocols Algorithms and Source Code in C", Second Edition, Wiley.**
2. **Atul Kahate, "Cryptography and Network Security", Tata McGraw-Hill Education, 2003.**
3. **Eric Cole, "Network Security Bible", Second Edition, Wiley, 2011.**

Resource Links:

1. **https://github.com/cmin764/cmiN/blob/master/FII/L3/SI/book/W.Stallings%20-%20Cryptography%20and%20Network%20Security%206th%20ed.pdf**
2. **https://docs.google.com/file/d/0B5F6yMKYDUbrYXE4X1ZCUHpLNnc/view**

Module No.	Session No.	Topic	Planned Date	CO	Assessment Methods
1	1	Syllabus, Cos, Security Goals, Attacks	07/01/2025	CO1	IAT-1, MCQ-1
	2	Services, Mechanisms and Techniques	09/01/2025		
	3	Modular Arithmetic: Modulus, Congruence, Multiplicative Inverse, Euclidean Algorithm, Extended Euclidean Algorithm	10/01/2025		
	4	Modular Arithmetic: Fermat's theorem	14/01/2025		
	5	Modular Arithmetic: Euler's theorem	16/01/2025		
	6	Introduction to terms in cryptography, Cryptanalysis Attacks	17/01/2025		
	7	types of ciphers, types of classical cuphers, monoalphabetic vs polyalphabetic subsitution ciphers	21/01/2025		

	8	Monoalphabetic Ciphers: Additive cipher, Multiplicative cipher, Affine cipher, Simple Substitution Cipher	23/01/2025		
	9	Polyalphabetic Ciphers: Autokey Cipher, Vigenere Cipher, Playfair Cipher	24/01/2025		
	10	Example of playfair cipher, OTP-Vernam Cipher	28/01/2025		
	11	Hill Cipher (2 by 2 key matrix)	30/01/2025		
	12	Example of Hill Cipher	31/01/2025		
	13	Keyless Transposition Cipher	04/02/2025		
	14	Keyed Transposition Cipher	06/02/2025		
2	15	Difference between Stream and block cipher, traditional and modern cipher, components of modern block cipher, confusion and diffusion	07/02/2025	CO2	IAT-1, MCQ-2
	16	DES Cipher	11/02/2025		
	17	2-DES and 3-DES, Modes of operations of modern block cipher	13/02/2025		
	18	AES Cipher	14/02/2025		
	19	RC4 Algorithm	18/02/2025		
	20	Symmetric-key vs asymmetric-key algorithm, RSA Algorithm	20/02/2025		
	21	The Knapsack Cryptosystem	21/02/2025		
	22	KDC, Needham-schroeder Protocol	04/03/2025		
	23	Kerberos	06/03/2025		
	24	Diffie-Hellman Key Exchange with example	07/03/2025		
	25	Digital Certificate: X.509, PKI	11/03/2025		

3	26	Cryptographic hash functions, Properties of secure hash function	13/03/2025	CO3	IAT-2, MCQ-3
	27	Hash Function - MD5	18/03/2025		
	28	Hash Function - SHA1	20/03/2025		
	29	MAC - HMAC, CMAC	21/03/2025		
4	30	Message Authentication: Various techniques	25/03/2025	CO4	IAT-2, MCQ-4
	31	User Authentication, Entity Authentication, Digital Signature - RSA	27/03/2025		
	32	Example on RSA Digital Signature	28/03/2025		
5	33	Network security basics: TCP/IP vulnerabilities (Layer wise), Network Attacks: Packet Sniffing, ARP spoofing, port scanning, IP spoofing	29/03/2025	CO5	IAT-2, MCQ-5
	34	Denial of Service: DOS attacks, ICMP flood, SYN flood, UDP flood, Distributed Denial of Service	01/04/2025		
	35	SSL	03/04/2025		
	36	IPSec	04/04/2025		
	37	PGP	05/04/2025		
	38	IDS, firewall	15/04/2025		
6	39	Buffer Overflow, malicious Programs: Worms and Viruses, SQL injection	17/04/2025	CO5	IAT-2, MCQ-6
	40	Recent trends and research in cryptography or security.	19/04/2025	CO6	Expert Lecture

Faculty in-Charge **Head of Department**