Faculty of Engineering & Technology
Master of Technology (M. Tech)
(W. E. F.: 2023-24)

Document ID: SUTEFETM-01

Name of Faculty	:	Faculty of Engineering & Technology
Name of Program	:	Master of Engineering (M. Tech)
Course Code	:	1MSE01
Course Title	:	Information & Network Security
Type of Course	:	Professional Core (PC)
Year of Introduction	:	2023-24

Prerequisite	:	Mathematical concepts: Random numbers, Number theory, finite fields
Course Objective	:	NA
Course Outcomes	:	At the end of this course, students will be able to:
	CO1	Define and analyse various security goals and understand the security policies such as the CIA triad of Confidentiality, Integrity and Availability.
	CO2	Understand and evaluate the mathematical formulations used in symmetric key and Asymmetric key cryptography to design various security solutions.
	CO3	Illustrate a basic symmetric key and modern symmetric key cryptography techniques, how it has evolved, and evaluate in today's world.
	CO4	Evaluate Asymmetric key encryption techniques, key distribution scenario and calculate public and private components of asymmetric key encryption techniques.

Teaching and Examination Scheme

Teaching Scheme (Contact Hours)			Credits	Examination Marks				
				Theory Marks		Practical Marks		Total Marks
L	T	P	C	SEE	CIA	SEE	CIA	
2	0	0	2	70	30	0	0	100

*Legends: **L**-Lecture; **T**–Tutorial/Teacher Guided Theory Practice; **P** – Practical, **C** – Credit, **SEE** – Semester End Examination, **CIA** - Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.))*

Course Content

Unit No.	Topics	Teaching Hours	Weightage	Mapping with CO
1	**Introduction** Security Goals, Attacks, Services and Mechanisms, Techniques	2	04%	CO1
2	**Mathematics of Cryptography** Integer Arithmetic, Modular Arithmetic, Matrices, Linear Congruence	2	06%	CO2
3	**Tradition Symmetric Key Ciphers** Introduction, Substitution Ciphers, Transposition Ciphers, Stream and block Ciphers	2	07%	CO1
4	**Introduction to Modern Symmetric Key Ciphers** Modern Block Ciphers, Modern Stream Ciphers	2	09%	CO3
5	**Data Encryption Standard** Introduction, DES Structure, DES Analysis, Multiple DES, Security of DES	3	11%	CO4
6	**Advanced Encryption Standard** Introductions, Transformations, Key Expansions, Ciphers, Examples, Analysis of AES	3	09%	CO2
7	**Mathematics of Cryptography** PRIMES, Preliminary Testing, Factorization, Chinese Remainder Theorem, Quadratic Congruence, Exponentiation and Algorithm	3	09%	CO3
8	**Asymmetric Key Cryptography** Introduction, RSA Cryptosystem, RABIN Cryptosystem, ELGAMAL Cryptosystem	3	09%	CO2
9	**Key Management** Symmetric Key Distribution, Kerberos, Symmetric Key agreement, Public Key Distribution	3	09%	CO2
10	**Security at the application layer: PGP and S/MIME** Email. PGP, S/MIME and Algorithm	3	09%	CO4
11	**Security at the transport layer: SSL and TSL** SSL Architecture, FOUR Protocols, SSL Message Formats, Transport Layer Security	2	09%	CO4
12	**E-commerce Security** Electronic Voting / Polling systems -Standards and Applications	2	09%	CO4

Suggested Distribution of Theory Marks Using Bloom's Taxonomy						
Level	Remembrance	Understanding	Application	Analyse	Evaluate	Create
Weightage	**40**	**20**	**30**	**-**	**-**	**10**

NOTE: This specification table shall be treated as a general guideline for the students and the teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Suggested Learning Websites

Sr. No.	Name of Website
1	http://www.interhack.net/pubs/network-security/

Reference Books

Sr. No.	Name of Reference Books
1	Behrouz A. Forouzan, “Cryptography and Network Security” , THM, ISBM: 978- 0-07-066046-5
2	Eric Cole, Ronald Krutz, “Network Security Bible”, Wiley - ISBN:81-2650576-1
3	Vijay K Bhargava, “Communications, Information and network Security”, Kluwer Academics Publication;ISBN-1-4020-7251-1
4	Bruce Scheneir: "Applied Cryptography", 2/E, John Wiley, 1996.
5	Menezes, Oorschot, Vanstone: "Handbook of Applied Cryptography", CRC Press, 1996.
6	D Stinson, "Cryptography: Theory and Practice", 2/E, Chapman & Hall, 2002