Name of Faculty	:	Faculty of Engineering & Technology
Name of Program	:	Master of Technology (M.Tech.) – Cyber Security
Course Code	:	2MCS01
Course Title	:	Wireless Network: Security & Privacy
Type of Course	:	Professional Core
Year of Introduction	:	2023-24

Prerequisite	:	logic and most importantly zeal to learn
Course Objective	:	To understand the fundamentals of computer programming.
Course Outcomes	:	At the end of this course, students will be able to:
	CO1	Develop Concept of Security needed in Communication of data through computers and networks along with Various Possible Attacks
	CO2	Understand Various Encryption mechanisms for secure transmission of data and management of key required for required for encryption
	CO3	Understand authentication requirements and study various authentication mechanisms
	CO4	Understand network security concepts and study different Web security mechanisms

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	
4	0	0	4	70	30	00	00	100

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

Course Content

Unit No.	Topics	Teaching Hours	Weightage	Mapping with CO
1	**INTRODUCTION:** Need for Security, Security Attacks, Services and Mechanisms, Network Security, Model	12	20%	CO1
2	**SYMMETRIC CIPHERS:** Substitution &Transposition Techniques, Block Cipher, DES, Triple DES, Stream Ciphers, RC4.	12	20%	CO2

3	**PUBLIC KEY CRYPTOGRAPHY** Need and Principles of Public Key Cryptosystems, RSA Algorithm, Key Distribution and Management, Diffie-Hellman Key Exchange, Digital Signatures	12	20%	CO2
4	**AUTHENTICATION:** Authentication Requirements, Message Authentication Codes, Hashes, MD5 & SHA, User Authentication: Password, Certificate based & Biometric Authentication, Kerberos	12	20%	CO3
5	**NETWORK SECURITY:** Authentication Requirements, Message Authentication Codes, Hashes, MD5 & SHA, User Authentication: Password, Certificate based & Biometric Authentication, Kerberos	12	20%	CO2 CO4

Suggested Distribution of Theory Marks Using Bloom's Taxonomy						
Level	Remembrance	Understanding	Application	Analyse	Evaluate	Create
Weightage	20	30	30	20	0	0

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

Suggested Learning Websites

Sr. No.	Name of Website
1	http://osou.ac.in/eresources/DCS-05-BLOCK-03.pdf
2	https://www.geeksforgeeks.org/wireless-security-set-1/
3	https://www.researchgate.net/publication/297364587_Privacy_and_Security_of_Wireless_Communication_Networks

Reference Books

Sr. No.	Name of Reference Books
1	"Cryptography & Network Security", PHI William Stalling
2	"Cryptography & Network Security", Mc Graw Hill Atul Kahate
3	"Cryptography & Network Security", PHI 4 Forouzan
4	Practical C Programming (Third Edition) by Steve Oualline