MCPCC1012 Information Security		
Teaching Scheme	**Examination Scheme**	
Lectures : 03 Hrs/Week	**ISE I***	**20 Marks**
Tutorial :	**ISE II***	**20 Marks**
Credits : 03	**End Semester Examination**	**60 Marks**

Course Outcome - After studying this course, students will be able to

CO1: Identify and solve different information security issues.
CO2: Development of secure cryptosystem.
CO3: Design of basic biometric system application.
CO4: Development of biometric security algorithm.
CO5: Identify and investigate network security threats.

Course Contents

Unit No	Detailed Contents
1	**Information Security:** Introduction to IS, CIA model, computer security concepts, security attacks, security services, security mechanisms, a model for network security.
2	**Message Authentication codes:** Message Authentication requirements, Message Authentication functions, Digital Signature, Elgamal digital signature scheme, Hash Function, Cryptographic Hash Function, Secure Hash Algorithm (SHA) and Application of Cryptographic hash Functions.
3	**Cryptography:** Basics of Cryptography, Elementary Ciphers (Substitution, Transposition and Ceaser cipher), Random and Pseudorandom Numbers , Stream Ciphers and RC4 ,Cipher Block Modes of Operation, Block Cipher. Data Encryption Standard (DES), Introduction to Public Key, Advanced Encryption Standard (AES), Cryptosystem, Diffie-Hellman Key Exchange, RSA Cryptosystem.
4	**Network access control:** Transport layer security, secure shell (SSH)- transport layer protocol, user authentication protocol, connection protocol Electronic mail security – PGP, S/MIME.
5	**Biometrics security:** Biometric identification, verification, authentication, different biometric techniques, biometric design steps, face recognition system, fingerprint recognition system, biometric template security, fuzzy vault algorithm.

Text Books

1. Cryptography and Network Security, 5th Edition, William Stallings,Pearson.
2. Network Security and Cryptography, Bernard Menezes, Cengage, 2010.

Refernce Books

1. Information Security and cyber laws, Saurabh Sharma, Student series, Vikas publication
2. Network Security: The Complete Reference, Keith Strassberg, Mark Rhodes-Ousley, and Roberta Bragg.

E Books/ Online learning material

1. https://nptel.ac.in/courses/106/106/106106129/
2. https://bit.ly/3jAmS7k

Mapping of COs and POs

PO CO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO 1	1	2											1	1	
CO 2	1	2		2		1							1	1	1
CO 3	1	2	2										1	1	
CO 4	1	2	2										1	1	
CO 5	1	2		2	1			1					1	2	

Assessment Table

Assessment Tool	Course Outcomes				
	CO1	CO2	CO3	CO4	CO5
ISE I* (Class Test) 20 Marks	10	10	-	-	-
ISE II* 20 Marks	5	-	5	5	5
ESE Assessment 60 Marks	15	15	10	10	10

Assessment Pattern

Level No.	Knowledge Level	ISE I*	ISE II*	End Semester Examination
K1	Remember	10	5	20
K2	Understand	5	5	20
K3	Apply	5	-	10
K4	Analyze	-	5	5
K5	Evaluate	-	5	5
K6	Create	-	-	-
Total		20	20	60

Approved in BoS meeting held on 24/08/2023 and Approved by Chairman, Academic Council