NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	Integrated B.Tech.(CSE)-MBA
Course Code:	CSI0703
Course Title:	Information Security
Course Type:	Core
Year of Introduction:	2021-22

Credit Scheme

L	T	Practical Component				C
		LPW	PW	W	S	
3	1	0	-	-	-	4

Course Learning Outcomes (CLO):

At the end of the course, students will be able to –

1. illustrate principles and problems of cryptosystems for encryption, digital signing and authentication
2. infer the role of mathematics of cryptography
3. choose appropriate cryptographic technique for developing a secured network
4. implement the cryptographic algorithms

Syllabus: **Total Teaching hours: 30**

Unit	Syllabus	Teaching hours
Unit-I	**Security Overview:** Significance of Information and network security, what are the hurdles in achieving the same, introduction to Cryptography	02
Unit-II	**Classical Encryption Techniques**: Caesar Cipher, Monoalphabetic substitution, Playfair Cipher, Polyalphabetic substitution, Transposition Techniques	06
Unit-III	**Symmetric Ciphers:** Block Ciphers and DES, Advanced Encryption Standard (AES), Block Cipher Operations, Key Distribution	05
Unit-IV	**Mathematics:** Pseudo Random Number Generation and Stream Ciphers, Mathematical Background (Fermat's Little Theorem, Euler Totient Function, Euler's Theorem Chinese Remainder Theorem etc.)	10
Unit-V	**Public Key Cryptography:** RSA, Elliptic Curve Cryptography, Diffie Helman Key Exchange, Digital Signatures, Key Distribution	05
Unit -VI	Overview of Hash and MAC Functions and Digital Signature Standards	02

Self-Study: The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents

Suggested Readings/ References:

1. William Stallings, "Cryptography and Network Security: Principles and Practice, Pearson
2. D. R. Stinson: Cryptography: Theory and Practice (Discrete Mathematics and Its Applications), CRC Press.
3. B. Schneier: Applied cryptography: protocols, algorithms, and source code in C, John Wiley & Sons.
4. Bernard Menezes: Network Security & Cryptography, 1st Edition

Suggested List of Experiments: -NA-

Suggested Case List: -NA-