NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	Integrated B.Tech.(CSE)-MBA
Course Code:	CSI0902
Course Title:	Cryptography
Course Type:	(□ Core/ □ Value Added Course / √ **Department Elective** / □ Institute Elective/ □ University Elective/ □ Open Elective / □ Any other)
Year of Introduction:	2022-23

L	T	Practical Component				C
		LPW	PW	W	S	
3	-	2	-	-	-	4

Course Learning Outcomes (CLOs):

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

1. explain the classical and modern cryptography techniques (BL2)
2. solve various numerical problems related to cryptography (BL3)
3. compare the working of symmetric and asymmetric cryptography (BL4)
4. evaluate modern cryptographic techniques such as digital signatures and hashing (BL5)

Syllabus: **Total Teaching hours: 30**

Unit	Syllabus	Teaching hours
Unit-I	**Cryptography:** Basics of cryptography, OSI Security Architecture, Security attacks, services and mechanisms	03
Unit-II	**Ciphers**: Introduction, Classical encryption techniques, Block ciphers and data encryption standards, Modular arithmetic, Stream ciphers, AES algorithm, Multiple encryptions and Triple DES, different modes of block cipher operations	07
Unit-III	**Pseudorandom number generation and stream ciphers**: Principles of pseudorandom number generations, Pseudorandom number generators, Pseudorandom number generations using a block cipher, stream ciphers	03
Unit-IV	**Public key cryptosystem:** Principles of public key cryptosystem, The RSA algorithm, Fermat's and Euler's theorem, Elliptic Curve Cryptography, Elgamal, other public key cryptosystems	04
Unit-V	Cryptographic hash functions, Hash function based on Cipher Block Chaining, Secure Hash Algorithm, Message Authentication Codes, Digital Signature	10

Unit-VI	**Key Management and Distribution:** Symmetric key distribution using symmetric encryption, Symmetric key distribution using asymmetric encryption, distribution of public keys	03

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. Cryptography and Network Security Principles and Practices by William Stallings
2. Charlie Kaufman, Network Security: Private Communication in a Public World, PHI.
3. Aegean Park Pr, Basic Cryptanalysis, Field Manual, DoD, USA.
4. J. Katz and Y. Lindell., Introduction to Modern Cryptography, Taylor & Francis.
5. Bruce Schneier, Applied Cruptography, Wiley
6. Christof Paar, Understanding Cryptography, Springer
7. Basic Cryptanalysis Field Manual

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Implement Playfair Cipher, Rail fence Cipher and Affine Cipher.	04
2	Implement simplified DES encryption (and decryption).	02
3	Generate pseudorandom numbers using various techniques.	02
4	Finding the Greatest Common Divisor of 2 numbers using various methods, implement Euler's Method.	02
5	Implement the Chinese Remainder Theorem.	02
6	Implementation of RSA algorithm.	02
7	Implementation of Elliptic Curve Cryptography.	02
8	Implementing a Digital Signature scheme.	04

Suggested Case List: -NA-