NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	MTech CSE (Cyber Security)
Course Code:	6CS403CC25
Course Title:	Cryptography Essentials
Course Type:	Core
Year of Introduction:	2025-26

L	**T**	**Practical Component**				**C**
		LPW	**PW**	**W**	**S**	
3	0	2	-	-	-	4

Course Learning Outcomes (CLOs):

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

1. explain the fundamentals of classical and advanced cryptography techniques (BL2)
2. apply the mathematical foundations to modern cryptographic techniques (BL3)
3. analyse various security mechanisms for application development (BL4)
4. evaluate numerical examples related to Galois field, symmetric and asymmetric cryptographic techniques. (BL5)

Unit	**Contents**	**Teaching Hours (Total 45)**
Unit-I	**Cryptography:** Basics of cryptography, OSI Security Architecture, Security attacks, services and mechanisms	03
Unit-II	**Symmetric Ciphers**: Introduction, Classical encryption techniques, Block ciphers and data encryption standards, Basic cryptanalysis, Modular arithmetic, Stream ciphers, AES algorithm	08
Unit-III	**Block Cipher operations**: Multiple encryptions and Triple DES, different modes of block cipher operations	04
Unit-IV	**Pseudorandom number generation and stream ciphers**: Principles of pseudorandom number generations, Pseudorandom number generators, Pseudorandom number generators using a block cipher, stream ciphers	04
Unit-V	**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	05
Unit-VI	**Cryptographic hash functions**: Requirements and applications of cryptographic hash functions, Hash function based on Cipher Block Chaining, Secure Hash Algorithm	05
Unit-VII	**Message Authentication Codes**: Requirements and applications of Message Authentication Codes, MACs based on Hash function, MACs based on Block ciphers	05
Unit-VIII	**Digital Signatures**: Requirements and Applications of Digital Signatures, different digital signature schemes	06
Unit-IX	**Key Management and Distribution:** Symmetric key distribution using symmetric encryption, Symmetric key distribution using asymmetric encryption, distribution of public keys.	05

Self-Study:

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

Suggested Readings/ References:

1. W. Stallings, Cryptography and Network Security: Principles and Practices, Prentice Hall
2. Charlie Kaufman, Network Security: Private Communication in a Public World, Prentice Hall
3. Aegean Park Pr, Basic Cryptanalysis, Field Manual, DoD, USA
4. J. Katz and Y. Lindell., Introduction to Modern Cryptography, Taylor & Francis
5. A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of Applied Cryptography, Taylor & Francis.

Suggested List of Experiments:

Sr. No.	Name of Experiments/Exercises	Hours
1	Implement Playfair Cipher, Rail fence Cipher, and Transposition technique	04
2	Implement simplified DES encryption (and decryption)	02
3	Generate pseudorandom numbers using various techniques	04
4	Finding the Greatest Common Divisor of 2 numbers using various methods, implement Euler's Method, the Chinese Remainder Theorem	02
5	Implementation of RSA algorithm	02
6	Implementation of ElGamal Algorithm	02
7	Implementation of Elliptic Curve Cryptography	02
8	Implementation of stream cipher technique using RC4	04
9	Implementing a Digital Signature scheme	04
10	Implement a small application to carry out Confidentiality, Authentication, Integrity, Access Control, and Digital Signatures.	04