NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	Master of Computer Application (2-Years Programme)
Course Code:	3MCAD352
Course Title:	Data Encryption
Course Type:	Departmental Elective
Year of Introduction:	2021-22

Credit Scheme

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

Course Learning Outcomes (CLO):

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

1. identify the role of symmetric and asymmetric cryptographic techniques
2. relate the mathematical foundations with the modern cryptographic techniques
3. apply the concepts of pseudorandom number generation for various cryptographic activities
4. examine modern cryptographic techniques such as digital signatures and hashing

Syllabus: **Total Teaching hours: 45**

Unit	Syllabus	Teaching hours
Unit-I	**Cryptography:** Basics of cryptography, Services, Mechanisms and Attacks, The OSI Security Architecture.	04
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	04
Unit-IV	**Pseudorandom number generation and stream ciphers:** Principles of pseudorandom number generation, pseudorandom number generators, pseudorandom number generation using a block cipher, stream ciphers.	06
Unit-V	**Public key cryptosystem:** Principles of public key cryptosystem, the RSA algorithm, Fermat's and Euler's theorem, Elliptic Curve Cryptography	06
Unit-VI	**Cryptographic hash functions:** Requirements and applications of cryptographic hash functions, hash function based on cipher block chaining, secure hash algorithm	04
Unit-VII	**Message Authentication Codes:** Requirements and applications of message authentication codes, MACs based on hash function, MACs based on block ciphers	04
Unit-VIII	**Digital Signatures:** Requirements and applications of digital signatures, different digital signature schemes	04
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 semester. Around 10% of the questions will be asked from self-study contents.

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, PHI.
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.	Title	Hours
1.	To study and perform a C Program using your own logic to encrypt and decrypt the given data. [Perform your encryption on string entered by the user as well as on given text file through command prompt].	02
2.	To study and perform a C Program to implement Caesar Cipher algorithm of data encryption. Apply the algorithm to a given file. Extend your program for generalized Caesar Cipher logic.	02
3.	To study and implement Breaking the Shift Cipher. Hint: Apparently, the system is easily broken if the total number of distinct secret keys is small, that is the key space K is small. In this experiment, we work with a well-known historical encryption scheme, namely the shift cipher, which has a very small key space. Your task is to break the shift cipher. Specifically, given (only) the cipher text in some instance of a shift cipher, you need to find the plaintext and the secret key.	02
4.	To study and implement one of the multiple-letter encryptions cipher (Playfair) algorithm.	04
5.	To study and Read one text file (data.txt), applying Hill Cipher algorithm, encrypt the data.txt file and store it into encrypt.txt file. Apply decryption logic and store decrypted text into decrypt.txt file.	04
6.	To study and Use Vigenere cipher algorithm to encrypt and decrypt the content of given data file.	02
7.	To study and implement simple rail fence technique of transposition cipher. Also make scheme complex by writing message in rectangle form.	02
8.	To study and implement Steganography concept on text file/image file.	04
9.	To study and implement Symmetric key Data Encryption Standard algorithm.	04

	10.	To study and design a program to store User ID, Password and other important secret information into "encrypt" file. Content stored into the encrypt file must be stored using more than one encryption algorithm.	04
Suggested Case List:	-NA-		