Course No.	Course Title	L-P-T	Credits
MMAT2C002T	Cryptography	3-0-1	4

OBJECTIVES : The aim of this course is to teach the students the about the Encryption, Decryption, Authentication and Validations etc.

CO 01	Learn about the different types of Ciphers
CO 02	Understand the modular mathematics and their applications
CO 03	Learn and apply different symmetric key cryptography
CO 04	Use hash function for Authentications, digital signature
CO 05	Identify various Authentications systems and classifications

Course contents

Unit-1

Cryptography, Cryptosystem, Cryptanalysis, classical Cryptosystems: Hierarchy of Cipher Substitution Techniques, Monoalphabetic Cipher, Ceasar Cipher, Hill Cipher Playfair Transportation Techniques: Rail fence Cipher, Modern Ciphers: Block Ciphers Symmetric Ciphers, Asymmetric ciphers

Unit-2

Number Theory: Modular Arithmetic, Multiplicative Inverse, Relatively Prime, Extended Euclidean Algorithim, Finite Fields, Fermat's and Euler's Theorems, Euler's Totient Function and Euler,s Theorem, Galois Fields ($GF(P^n)$ & $GF(2^n)$), Polynomial Arthmetic: Addition, Multiplication and Division over Galois Fields, Miller –Rabin Algorithm, The Chinese Remainder Theorem.

Unit-3

Symmetric Key Cryptography: Data Encryption Standard(DES), Advanced Encryption Standard (AES) (IDEAS, Block Ciphers Modes of Operators . Public Key Cryptography Principles, Public Key Cryptography Algorithms, Diffier Hellman Key Exchange, RSA Algorithm Key Generation, Encryption and Decryption Processes.

Unit-4

Cryptographic Hash Functions: Application of Cryptographic Hash Functions, Requirements & Security, Secure Hash Algorithm, Message Authentication Functions, Message Digests: details of D4 and MD5 algorithms, SHA-1 and SHA-2 algorithms. Digital Signature Algorithm. Elliptic curve Cryptography.

Unit-5

Authentication System, Password Based Authentication, Dictionary Attacks (online and Offline) Challenge Response system, one way authentication, Mutual Authentication, Biometric System, Needham- Schroeder Scheme, Kerberos Protocol.

Reference Books:

1. W. Stallings, Cryptography and Network Security: Principles and Practice
2. William Stallings, Network Security Essentials: Applications and Standards
3. Matt Bishop, Computer Security, Art and Science.
4. Mark Stamp, Information Security: Principles and Practices
5. Bruce Schneider, Applied Cryptography: Theory and Practice
6. Douglas. R. Stinson. Cryptography: Theory and Practice
7. B.A Forouazan, Cryptography & Network Security, Tata Mc Graw Hill.

Shalaksh Kamlesh Kanwar