UNIVERSITY OF MADRAS

MASTER OF COMPUTER APPLICATIONS (MCA) DEGREE PROGRAMME

SYLLABUS WITH EFFECT FROM 2023-2024

Title of the Paper	**Cryptography and Network Security**		
Elective -V Theory	II Year & III Semester	Credit:3	535E3B

Course Objectives

- To familiarize classical encryption techniques and advanced encryption standards

  To explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithms

  To recognize different encryption and decryption techniques to solve problems related to confidentiality and authentication

  To develop the ability to use existing cryptographic utilities to build programs for secure communication.

  To learn the need of digital signatures to secure the document with key management

Unit I: Overview: Computer Security Concepts – The OSI Security Architecture – Security Attacks – Security Services – Security Mechanisms –A Model for Network Security – Classical Encryption Techniques: Symmetric Cipher Model – Substitution Techniques – Transposition Techniques – Rotor Machines – Steganography.

Unit II: Block Ciphers and the Data Encryption Standard: Traditional Block Cipher Structure – The Data Encryption Standard – The DES Example – The Strength of DES – Block Cipher Design Principles –Basic Concepts in Number Theory and Finite Fields: Divisibility and the Division Algorithm – The Euclidean Algorithm – Modular Arithmetic – Groups, Rings, and Fields – Finite Fields of the Form GF(p) – Polynomial Arithmetic.

Unit III: Advanced Encryption Standard: Finite Field Arithmetic– AES Structure – AES Transformation Functions – AES Key Expansion –Block Cipher Operation: Multiple Encryption and Triple DES – Stream Ciphers – RC4 – Public-Key Cryptography and RSA: Principles of Public-Key Cryptosystems – The RSA Algorithm –Diffe-Hellman Key Exchange – Elgamal Cryptographic System – Elliptic Curve Arithmetic – Elliptic Curve Cryptography – Pseudorandom Number Generation Based on an Asymmetric Cipher.

Unit IV: Cryptographic Hash Functions: Applications of Cryptographic Hash Functions – Two Simple Hash Functions – Requirements and Security – Hash Functions Based on Cipher Block Chaining – Secure Hash Algorithm(SHA) – SHA-3 – Message Authentication Codes: Requirements – Functions – Security of MACs – MACs Based on Hash Functions: HMAC – MACs based on Block Ciphers: DAA and CMAC – Authenticated Encryption: CCM and GCM – Key Wrapping.

Unit V: Digital Signatures – Elgamal Digital Signature Scheme – Schnorr Digital Signature Scheme – NIST Digital Signature Algorithm – Elliptic Curve Digital Signature Algorithm – RSA-PSS Digital Signature Algorithm – Key Management and Distribution: Symmetric Key

Distribution Using Symmetric Encryption – Symmetric Key Distribution Using Asymmetric Encryption – Distribution of Public Keys – X.509 Certificates – Public-Key Infrastructure.

Text Books

1. William Stallings, "Cryptography and Network Security – Principles and Practices", Pearson Education / PHI, 7th Edition.
2. Behrouz A Forouzan, DebdeepMukhopadhyay, "Cryptography And Network Security", McGraw Hill Education, 3rd Edition.

Reference Books

1. Bernard Menezes, "Network Security and Cryptography", Cengage,1st Edition, 2010.
2. William Stallings, "Cryptography and Network Security", Pearson EducationIndia, Sixth Edition, 2016.
3. V.K. Jain, "Cryptography and Network Security", Khanna Book Publishing, New Delhi, 2016.
4. C.K. Shyamala, N. Harini, Dr. T. R. Padmanabhan, "Cryptography and Security", Wiley India Pvt. Ltd.,2011

Course Outcomes:

On the successful completion of the course, students will be able to

CO1	Comprehend and analyze the security concepts to apply and evaluate the encryption techniques in various models.	K1-K6
CO2	Understand and examine the various data encryption standards and number theory. Illustrate and evaluate the various techniques in different applications.	K1-K6
CO3	Grasp the knowledge of AES techniques and apply to evaluate the performance with different key types.	K1-K6
CO4	Comprehend and analyse the basics of hash function and MAC that helps to develop the encryption models in various application.	K1-K6
CO5	Understand and illustrate the need of digital signature to examine the method of providing good security to the document. And also learn the concept of key management.	K1-K6

K1- Remember, K2- Understand, K3- Apply, K4- Analyze, K5 Evaluate, K6- Create

Mapping with Programme Outcomes:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	M	S	-	L	M	S	M	M	-	S
CO2	M	S	-	M	M	L	M	S	-	M
CO3	S	S	-	M	S	M	S	M	-	S
CO4	S	M	L	S	M	L	S	M	-	M
CO5	M	S	M	L	S	L	M	S	-	S

S- Strong; M-Medium; L-Low