MCA-303 **Information Security** L=3, T=1

Course Objectives: To understand how cryptography can be used as an effective tool in providing assurance concerning privacy and integrity of information. To recognize the concept of encryption/decryption. To describe the different types of ciphers along with the identification of the characteristics of a good cipher. To provide skills to design security protocols for solving security problems. To develop skills necessary to help organizations in designing, testing and implementing well-planned information security measures for information systems.

UNIT - I

Introduction: Security Attacks: Motives, vulnerabilities, Defense strategies and techniques, Various Attacks- DoS, DDoS, Session Hijacking and Spoofing, Phishing, Buffer Overflow, Format String Attacks, SQL Injection, Malicious Software, Prevention and Detection, Data Protection, Response, Recovery and Forensics.

Basics of Cryptography: Symmetric Cipher Model, Substitution Techniques, Transportation Techniques, Other Cipher Properties- Confusion, Diffusion, Block and Stream Ciphers

UNIT - II

Secret Key Cryptography: Data Encryption Standard (DES), Strength of DES, Block Cipher, Design Principles and Modes of Operations, Triple DES.

Public Key Cryptography: Principles of Public Key Cryptosystems, RSA Algorithm, DiffieHellman Key Exchange algorithm

UNIT - III

Cryptographic Hash Functions: Applications of Cryptographic Hash Functions, Secure Hash Algorithm, Message Authentication Codes – Message Authentication Requirements and Functions, HMAC, Digital signatures, Digital Signature Schemes, Authentication Protocols, Digital Signature Standards. Authentication Applications-Kerberos, Key Management and Distribution, X.509 Directory Authentication service, Public Key Infrastructure.

Electronic Mail Security-Pretty Good Privacy, S/MIME, Operating System Protection-Memory and Address protection, File Protection Mechanism, User Authentication. Database Security-Security Requirement, Reliability and Integrity, Sensitive data, Multilevel Databases.

UNIT - IV

IP Security: Overview, Architecture, Authentication Header, Encapsulating Security Payload, Combining security Associations, Internet Key Exchange, Web Security: Web Security Considerations, Secure Sockets Layer and Transport Layer Security, Electronic Payment.
Intrusion Detection Systems and Firewalls Intruders, Intrusion Detection, Password Management, Firewalls Need, Characteristics, Types of Firewalls, Placement of Firewalls, Firewall Configuration, Trusted systems.

Text Books:

1. 'Cryptography and Network Security- Principles and Practices' by William Stallings, 8th Edition, Prentice Hall Publication
2. 'Network security and Cryptography' by Bernard Menezes, 1 st Edition, Cengage Learning Publication
3. 'Computer Security- Principles and Practice' by William Stallings, 1 st Edition, Pearson Education

Reference Books:

1. 'Network Security Essentials' by William Stallings, 4th Edition, Pearson Publication
2. 'Applied Cryptography' by Bruce Schneier, Edition 2001, Wiley & Sons Inc
3. 'Cryptography and Network', 2nd edition, by Behrouz A Fourouzan, Debdeep Mukhopadhyay, TMH.

Course Outcomes:

By the end of the Course, Student will be able to:
CO1:understand a variety of generic security threats and vulnerabilities, and identify & analyze particular security problems for a given application
CO2: gain knowledge on the notions of various types cryptography techniques.
CO3:understand and analyze the various cryptography techniques, their principles and applications.
CO4:identify and analyze the applications of security techniques and technologies in solving real life security problems.
CO5:understand, analyze and evaluate the security of information systems.
CO6: analyze and interpret the mechanisms to provide security for communicating information.

NOTE: In Each theory paper. Nine questions are to be set. Two questions are to be set from each Unit and Candidate is required to attempt one question from each unit. Question number nine is Compulsory, which will be of short answer type with 5-10 parts, out of the entire syllabus. In all five questions are to be attempted.