Cryptography

Code: -

Credits: 4 **Maximum Marks:** 100

Description: This course will let student aware of basic concepts of Encryption techniques for information security.

Purpose: This course is intended as a comprehensive guide to introduce the role of cryptography in authentication mechanism, Network security, System level security and dealing with information breach.

Prerequisite:

- ✓ Students is expected to know basic operational knowledge of using computer
- ✓ Elementary Mathematical knowledge.
- ✓ Basics of Networking.

Recommended Study habit:

- ✓ Do observe the case studies and real world implementation.

Suggested Readings

1. William Stallings, “Cryptography And Network Security – Principles and Practices”, Prentice Hall of India, Third Edition,2003.
2. Atul Kahate, “Cryptography and Network Security”, TataMcGraw-Hill,2003.
3. Bruce Schneier, “Applied Cryptography”, John Wiley & Sons Inc,2001.
4. Charles B. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing”

UNIT – I

Theme	**Description**	**Lectures**
Introduction	• OSI Security Architecture • Classical Encryption techniques • Cipher Principles • Data Encryption Standard • Block Cipher Design Principles and Modes of Operation • Evaluation criteria for AES – AES Cipher – Triple DES • Placement of Encryption Function • Traffic Confidentiality	8

UNIT – II

Theme	**Description**	**Lectures**
Public Key Cryptography	• Key Management o Diffie-Hellman key Exchange • Elliptic Curve Architecture and Cryptography • Introduction to Number Theory • Confidentiality using Symmetric Encryption • Public Key Cryptography and RSA	8

UNIT – III

Theme	Description	Lectures
Authentication & Hash Function	• Authentication requirements, Authentication functions • Message Authentication Codes • Hash Functions: Security of Hash Functions and MACs • MD5 message Digest algorithm • Secure Hash Algorithm, RIPEMD, HMAC Digital Signatures • Authentication Protocols • Digital Signature Standard	8

UNIT – IV

Theme	Description	Lectures
Network Security	• Authentication Applications • Kerberos • X.509 Authentication Service • Electronic Mail Security • PGP – S/MIME • IP Security • Web Security.	12

UNIT – V

Theme	Description	Lectures
System Level Security	• Intrusion detection • Password management • Viruses and related Threats, Virus Counter measures • Firewall Design Principles • Trusted Systems.	10