Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada.

3/4 B.Tech. SECOND SEMESTER

IT6T4 CRYPTOGRAPHY AND NETWORK SECURITY Credits: 4

Lecture: 4 periods/week Internal assessment: 30 marks
Tutorial: 1 period /week Semester end examination: 70 marks

Objectives:

- To explain the objectives of information security.
- To discuss the tradeoffs inherent in security.
- To explain the importance and applications of confidentiality, integrity, and availability.
- To explain the basic categories of threats to computers and networks.
- To discuss issues for creating security policy for a large organization.
- To defend the need for protection and security, and the role of ethical considerations.
- To describe the enhancements made to IPv4 by IPSec.
- To discuss the fundamental ideas of public-key cryptography and simple extensions of cryptographic protocols.

Outcomes :

Student will be able to

- Understand Intrusions and intrusion detection
- Design a security solution for a given application.
- Analyze a given system with respect to security of the system.

Syllabus:

UNIT-I
INTRODUCTION:
The OSI security architecture, security attacks, security services, security mechanisms, a model for network security.

UNIT-II
CLASSICAL ENCRYPTION TECHNIQUES:
Symmetric cipher model, Substitution techniques, Transposition techniques, rotor machines, steganography.

UNIT-III
BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD:
Block cipher principles, the data encryption standard, the strength of DES, differential and linear cryptanalysis, and block cipher design principals.

UNIT-IV
PUBLIC-KEY CRYPTOGRAPHY AND RSA:
Principals of Public Key Cryptosystems, the RSA algorithm.

UNIT-V
KEY MANAGEMENT OTHER PUBLIC KEY CRYPTOSYSTEMS:
Key management, Diffie-Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography.

UNIT-VI
AUTHENTICATION APPLICATIONS:
Kerberos, X.509 authentication services, public-key infrastructure.

UNIT-VII
ELECTRONIC MAIL SECURITY & IP SECURITY:
Pretty good privacy, S/MIME, IP security overview, IP security architecture.

UNIT-VIII
INTRUDERS, MALICIOUS SOFTWARE & FIREWALLS:
Intruders, intrusion detection, viruses and related threats, virus countermeasures, firewall design principles, trusted systems.

Text Book:

1. William Stallings**, "**Cryptography and network security"**,** Fourth edition, Pearson Education.

Reference books:

1. Behrouz A.Forouzen, "Cryptography & Network Security", TMH.
2. Kaufman, Perlman, Speciner, "NETWORK SECURITY", 2nd Edition, (PHI / Eastern Economy Edition)
3.Trappe & Washington, "Introduction to Cryptography with Coding Theory",2/e, Pearson.