INFORMATION SECURITY

(Professional Elective-V)

Course Code : 15IT1107

L	T	P	C
3	0	0	3

PRE-REQUISITES:

Computer Networks.

Course Outcomes:

At the end of the Course, the Student will be able to:

CO 1 Specify the Security Architecture.

CO 2 Analyze different Public-Key Cryptography Algorithms and Hash Functions.

CO 3 Discuss key management, distribution and authentication techniques.

CO 4 Analyze transport level security and electronic mail security.

CO 5 Determine the Security at IP layer.

UNIT-I (12 Lectures)

OVERVIEW OF SECURITY:

OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A model for Internetwork security.

CLASSICAL ENCRYPTION TECHNIQUES:

Symmetric Cipher Model, Substitution Techniques, Transposition Techniques. Block Cipher Principles, Data Encryption Standard, DES Example, Strength of DES , Multiple Encryption and Triple DES, Advanced Encryption Standard, Stream Ciphers, RC4.

UNIT-II (12 Lectures)

PUBLIC-KEY CRYPTOGRAPHY:

Public-Key Cryptography and RSA, Other Public-Key Cryptosystems(Diffie-Hellman Key Exchange, Elliptic Curve Cryptography.

CRYPTOGRAPHIC HASH FUNCTIONS:

Applications of Cryptographic Hash Functions, Secure Hash Algorithm (SHA).

MESSAGE AUTHENTICATION CODES:

Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MACs, MACs Based on Hash Functions: HMAC , Digital Signature Standard.

UNIT-III (9 Lectures)

KEY MANAGEMENT AND DISTRIBUTION:

Symmetric Key Distribution using Symmetric Encryption, Symmetric Key Distribution using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates, Kerberos.

UNIT-IV (8 Lectures)

TRANSPORT-LEVEL SECURITY:

Web Security Issues, Secure Sockets Layer (SSL), Transport Layer Security (TLS), HTTPS

ELECTRONIC MAIL SECURITY:

Pretty Good Privacy, S/MIME

UNIT-V (9 Lectures)

IP SECURITY:

IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange, Intruders, Malicious Software, Firewalls.

TEXT BOOK:

William Stallings, “Cryptography and Network Security Principles and Practices”, 6thEdition, PHI/Pearson, 2014.

REFERENCES:

1. William Stallings, “Network Security Essentials: Applications and Standards”, 5thEdition, PearsonEducation,2013.
2. Whitman, “Principles of Information Security”, 4thEdition, Thomson, 2012.

WEB REFERENCE:

http://nptel.ac.in/courses/106105031/