4/4 B.Tech. FIRST SEMESTER
INFORMATION SECURITY

CS7T5B **Credits: 4**

Elective – II

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

Course Context and Overview: Information Security is a comprehensive study of the principles and practices of computer system security including operating system security, network security, software security and web security. Topics include common attacking techniques such as virus, trojan, worms and memory exploits; the formalisms of information security such as the access control and information flow theory; the common security policies such as BLP and Biba model; the basic cryptography, RSA, cryptographic hash function, and password system; the real system implementations, with case study of UNIX, SE-Linux, and Windows; network intrusion detection; software security theory; web security; legal and ethical issues in computer security.

Prerequisites: C LANGUAGE, I/O ANALOG AND DIGITAL INTERFACING, AND PERIPHERALS

Learning Outcomes:

Ability to:

1. Identify both external and internal vulnerabilities to enterprise computer infrastructures and sensitive digital assets anddevise a mitigation plan against them.
2. Have comprehensive information about security policies, establishing necessary organizational processes /functions for information security and will be able to arrange necessary resources.
3. Understand, analyze and work on activities of fraud prevention, monitoring, investigation, reporting.
4. Differentiate among the models, architectures, challenges and global legal constraints of secure electronic commerce technologies used to ensure transmission, processing and storage of sensitive information.

UNIT I

Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internetwork security, Internet Standards and RFCs.

UNIT II

Conventional Encryption Principles, Conventional encryption algorithms, cipher block modes of operation, location of encryption devices, key distribution Approaches of Message Authentication, Secure Hash Functions and HMAC.

UNIT III

Public key cryptography principles, public key cryptography algorithms, digital signatures, digital Certificates, Certificate Authority and key management Kerberos, X.509 Directory Authentication Service.

UNITIV

Email privacy: Pretty Good Privacy (PGP) and S/MIME.

UNIT V

IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

UNIT VI

Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET).

UNIT VII

Basic concepts of SNMP, SNMPv1 Community facility and SNMPv3.

Intruders, Viruses and related threats.

UNIT VIII

Firewall Design principles, Trusted Systems. Intrusion Detection Systems.

Learning Resources

Text Books:

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.

Reference Books:

1. Hack Proofing your network by Ryan Russel, Dan Kaminsky, Rain Forest Puppy, Joe Grand, David Ahmad, Hal Flynn Ido Dubrawsky, Steve W. Manzuik and Ryan Permeh, Wiley Dreamtech.
2. Fundamentals of Network Security by Eric Maiwald (Dreamtech press)
3. Cryptography and network Security, Third edition, Stallings, PHI/Pearson
4. Principles of Information Security, Whitman, Thomson.
5. Introduction to Cryptography, Buchmann, Springer.