**IV/IV B. TECH. FIRST SEMESTER**
**INFORMATION SECURITY(Required)**

**Course Code: CS 7T3** **Credits: 3**
**Lecture:3 periods/week** **Internal assessment: 30 Marks**
**Tutorial: 1period/week** **Semester end examination: 70 Marks**

**Prerequsites: Program Design, Computer Graphics**

**Course Objectives:**

The main goal of this course is to provide background, foundation, and insight into the many dimensions of information security. This knowledge will serve as basis for further deeper study into selected areas of the field, or as an important component in further studies and involvement in computing as a whole. The primary objectives of the course are as follows. Understand information security's importance in our increasingly computer-driven world. Master the key concepts of information security and how they "work." The course will be organized around a few broad themes:

1. Foundations: security mindset, essential concepts (policy, CIA, etc.)
2. Software security: vulnerabilities and protections, malware, program analysis
3. Practical cryptography: encryption, authentication, hashing, symmetric and asymmetric crypto Networks: wired and wireless networks, protocols, attacks and countermeasures.

**Course Outcomes:**

At the end of this course student will:

CO1) Understand the need of security over the network and define the cryptographic mechanism

CO2) Apply appropriate symmetric key algorithms

CO3) Apply appropriate Asymmetric key algorithms

CO4) Attribute the security mechanism in network transmission

CO5) Understand various vulnerabilities on system security

**Syllabus:**

**UNIT 1**
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 2**
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 3**
Public key cryptography principles, public key cryptography algorithms: RSA,Diffie-Hellmen key exchange algorithms, digital signatures, digital Certificates, Certificate Authority and key management Kerberos, X.509 Directory Authentication Service. Email privacy: Pretty Good Privacy (PGP) and S/MIME.

**UNIT 4**
IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management. Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET).

**UNIT 5**
Basic concepts of SNMP, SNMPv1 Community facility and SNMPv3. Intruders, Viruses and related threats. Firewall Design principles, Trusted Systems. Intrusion Detection Systems.

**Learning Resource**

**Text Books**

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

**References**

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.