## CORE COURSE XIV: 6B15CSC-A INFORMATION SECURITY

| SEMESTER | COURSE CODE | HOURS PER WEEK | CREDIT | EXAM HRS |
|---|---|---|---|---|
| 6 | 6B15CSC-A | 4 | 4 | 3 |

## COURSE OUTCOME

**CO1**: To understand the need of information security and to master information security Concepts, mechanisms and services as well as issues related to information Security.
**CO2**: To be familiar with cryptography and its categories.
**CO3:** Distinguish public and private key crypto systems and familiarize the rsa crypto System.
**CO4**: To attain the knowledge of digital signature and its security services.

**Unit I:**

Introduction to Information Security-The need for Security, Principles of security - confidentiality, Authentications, Integrity, Non-repudiation.Types of attacks-Passive attacks, Active attacks, Virus, Worm, Trojan horse.Introduction to Cryptography and Steganography.

**( 15Hrs)**

**Unit II:**

Symmetric Key Encipherment - Traditional symmetric Key Ciphers: Introduction-Kirchhoff's principle, cryptanalysis, categories of traditional ciphers; Substitution Ciphers- mono-alphabetic ciphers, polyalphabetic ciphers; Transposition Ciphers-key-less and keyed transposition ciphers, Stream and Block Ciphers.

**(20Hrs)**

**Unit III:**

DES: Data Encryption Standard:-Introduction, DES Structure-Initial and final permutations, DES function; Round Key Generation; Avalanche and completeness effect; Weak keys; Multiple DES- Double DES, Triple DES; Security of DES- Brute- force attack, Differential cryptanalysis, Linear cryptanalysis. Public key Cryptosystem: Principles of Public Key Cryptosystems; Applications of public Key Crypto systems, Requirement for Public Key Cryptosystem, Public Key Cryptanalysis. RSA Algorithm– Description of the Algorithm, The security of RSA

**(18Hrs)**

**Unit IV:**

Digital Signature:-Comparison between conventional and digital signature-Inclusion, Verification, Relationship, Duplicity; Process-needs for keys, signing the digest; Services-message authentication,message integrity, non-repudiation, confidentiality; Digital signature Forgery and types;Digital Signature Schemes-RSA digital signature scheme. **( 19Hrs)**

**Books for Study:**

1. Behrouz A. Forouzan and DebdeepMukhopadhyay, Cryptography And Network Security, 3rd Ed, McGraw Hill (Units I, II, IV)
2. William Stallings, Cryptography and Network Security - Principles and Practice Paperback, 7th Ed, Pearson (Unit III)

**Books for Reference:**

1. Bishop Matt, Introduction to Computer Security, Addison-Wesley,2004.
2. Pieprzyk Josef, Hardjono Thomas and Seberry Jennifer, Fundamentals of Computer Security, Springer, 2003.

**Marks including choice:**

| Unit | Marks |
|---|---|
| I | 10 |
| II | 20 |
| III | 15 |
| IV | 15 |