# CRYPTOGRAPHY AND NETWORK SECURITY

**COURSE OUTCOMES**

At the end of the course, the student will develop ability to

1. Identify the security issues in the network and resolve it.
2. Compare and contrast different IEEE standards and electronic mail security.
3. Discuss on various types of attacks and their characteristics.
4. Explain the concept of digital signature and its applications.
5. Analyze and compare various cryptography techniques.
6. Design new strategies to secure data communication.

**UNIT I**

**Introduction**

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.

**Finite Fields:**

Groups, Rings, Fields-Modular arithmetic-Euclid’s algorithm-Finite fields- Polynomial Arithmetic logarithms. – DoS Attacks.

**UNIT II**

**Conventional Encryption**

Principles, Conventional encryption algorithms (DES, 3DES, AES), cipher block modes of operation, location of encryption devices, key distribution Approaches of Message Authentication, Secure Hash Functions and HMAC.

**UNIT III**

**Number theory**

Prime numbers- Fermat’s and Euler’s theorem-Testing for primarily -The Chinese remainder theorem- Discrete logarithms. Public key cryptography: principles, **public key cryptography algorithms:** D-H, RSA, digital signatures, digital Certificates, Certificate Authority and key management Kerberos, X.509 Directory Authentication Service.

**UNIT IV**

**Email privacy**

Pretty Good Privacy (PGP) and S/MIME.

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

**UNIT V**

**Web Security**

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

Basic concepts of SNMP, SNMPv1 Community facility and SNMPv3.

**UNIT VI**

**System Level Security**

Intrusion detection – password management – Viruses and related Threats – Virus Counter measures – Firewall Design Principles – Trusted Systems.

**TEXT BOOKS**

1. William Stallings, “Cryptography & Network Security”, Pearson Education, 4th Edition, 2010.
2. William Stallings and Lawrie Brown, “Computer Security: Principles and Practice”, PHI, 2008

**REFERENCE BOOKS**

1. Charlie Kaufman, Radia Perlman, Mike Speciner, “Network Security, Private communication in public world”, PHI, 2nd edition, 2002.
2. Bruce Schneier, Neils Ferguson, “Practical Cryptography”, Wiley Dreamtech India Pvt Ltd, 2003. Douglas R Simson “Cryptography – Theory and practice”, CRC Press, 1995.

**Web Links**

1. [www.williamstallings.com/Security2e.html](http://www.williamstallings.com/Security2e.html)
2. http://nptel.iitm.ac.in