NETWORK SECURITY

Paper Code	**CEN-805**
Course Credits	**4**
Lectures / week	**3**
Tutorial / week	**1**
Course Description	**UNIT – I**

The need for security, Security approaches, Principles of security, Types of Attacks, Services and Mechanisms, Algorithm types and Modes. Secret Key Cryptography: Block Encryption, DES rounds, S-Boxes ,IDEA: Overview, comparison with DES, Key expansion, IDEA rounds, Uses of Secret key Cryptography; ECB, CBC, OFB, CFB, Multiple encryptions DES. Advance Encryption Standard AES.

UNIT- II

Kanpsack, RSA, Defiie-Hellman, use of public key cryptography Digital signature, Confidentiality and Non-repudiation, Public Key Infrastructure Algorithms, RSA: keys generating , encryption and decryption. Other Algorithms: PKCS, Diffie-Hellman, El-Gamal, Elliptical curve cryptography, DSS, Zero-knowledge signatures.

UNIT- III

Length of HASH, uses, Message Digest 4 and 5: algorithm (padding, stages, digest computation.) SHA: Overview, padding, stages. Message Authentication Codes (MACs).

UNIT- IV

Authentication Methods, Passwords, Single sign on, Authentication Protocol,

Kerberos: purpose, authentication, serer and ticket granting server, keys and tickets, use of AS and TGS, replicated servers. Kerberos V4: names, inter-realm authentication, Key version numbers., KDC's Certification Revocation, Inter domain, groups, delegation. Authentication of People: Verification techniques, passwords, length of passwords, password distribution.

UNIT – V

Electronic mail security, IP security, Network management security. Security for electronic commerce: Secure Socket Layer. Secure Electronic Transaction, Pretty Good Privacy, IP Security, Intruders and Viruses, Firewalls, Intrusion Detection system. Securing a Wireless Network.

References / Text Books:

- Stallings, W., Cryptography and Network Security: Principles and Practice, 3rd ed., Prentice Hall Print.,2003
- Atul Kahate, Cryptography and Network Security, McGraw Hill.Jochen Schiller, Mobile Communications, Pearson Education 2012.
- Kaufman, c., Perlman, R., and Speciner, M., Network Security, Private Communication in a public world, 2nd ed., Prentice Hall Print, 2002.
- Behrouz A Forouzan, Cryptography and Network Security, 2nd Edition 2010, McGraw Hill.

Computer Usage / Software Requires:

C++/ PYTHON /JAVA