NC5291 COMMUNICATION NETWORK SECURITY

DETAILED SYLLABUS

UNIT I INTRODUCTION AND NUMBER THEORY

Introduction to Information Security, Computer Security & Network Security. Need For Security. Security – Goals, Attacks, Security Services and Mechanisms, and Techniques. Number Theory and Mathematics for Symmetric Cryptography- Finite Arithmetic, Congruence Arithmetic-Linear Congruence and Quadratic Congruence. Mathematics for Asymmetric-Key Cryptography: Fermat‟s Theorem and Euler‟s Theorem, Primes, Primality Testing, Factorization, CRT, Exponentiation. Classical Symmetric-Key Ciphers –Substitution Ciphers, Transposition Ciphers.

UNIT II SYMMETRIC AND ASYMMETRIC CRYPTOSYSTEMS

Modern Symmetric-Key Cipher - Block Ciphers (DES, 3DES, AES and its mode of operations), Stream Ciphers, Asymmetric-Key Cryptosystem- RSA, ElGamal, ECC, Key Management - DiffieHellman (DH) Mechanism, Kerberos – Needham Schroeder Protocol.

UNIT III AUTHENTICATION, DIGITAL SIGNATURES AND CERTIFICATES

Message Integrity & Message Authentication - Message Authentication Code (MAC), Cryptographic Hash Functions – Birthday Attacks, Digital Signatures - Digital Signature Standards (FIPS 186-2), DSA (ANSI X9.30), RSA (ANSI X9.31) – Public Key Distribution – RSA schemes, Digital Certificates - PKI Certificates, PKI Life Cycle Management .

UNIT IV TRUSTED IDENTITY

Entity Authentication: Password System- Fixed and One time Passwords (S/Key) RFC 2289 – Callback System, Zero Knowledge, Challenge and Response Systems – RADIUS — ITU-T X.509.

UNIT V SECURITY AT LAYERS

Network Layer Security - IPSec, Transport Layer Security- SSL/TLS, SSH, Application Layer Security –PGP, S/MIME, Firewall - Concepts, Architecture, Packet Filtering, Proxy Services and Bastion Hosts.

OBJECTIVES :

The students should be made to:

Understand the need and concept of security

Learn cryptosystems

REFERENCES:

1. Behrouz A.Forouzan, “Cryptography and Network Security”, Special Edition, Tata McGraw Hill, 2007.

2. Bruce Scheneier, “Applied Cryptography”, John Wiley & Sons, 1994.

3. Charlie Kaufmann, Radia Perlman, Mike Speciner, "Network Security", Second Edition, Prentice Hall, 2002

4. Douglas R.Stinson, “Cryptography: Theory and Practice”, CRC Press Series on Discrete Mathematics and its Applications, 1995.

5. David M. Durton, “Elementary Number Theory”, Tata Mcgraw Hill, Sixth Edition, 2009.

6. William Stallings “Cryptography and Network Security: Principles and Practice”, 3rd Edition, Pearson Education, 2002.

7. William Stallings “Network Security Essentials: Applications and Standards”, 2nd Edition, Pearson Education, 2000.