22-382-0302 - CRYPTOGRAPHY AND NETWORK SECURITY

UNIT I (9 Hours)

Classical cryptography: Shift cipher, Substitution cipher, Affine cipher, Vigenere cipher, Hill cipher, Permutation cipher, Stream ciphers, Product Ciphers: Playfair Cipher. LFSR, Cryptanalysis on Classical Ciphers.

UNIT II (10 Hours)

Block ciphers: Substitution Permutation Networks, Feistel cipher, Data Encryption Standard, Cryptanalysis: Differential Cryptanalysis and Linear Cryptanalysis, Multiple encryption: 3-DES, Advanced Encryption Standard, Analysis of AES, Block Cipher Modes of operation.

UNIT III (13 Hours)

Public Key Cryptosystems: Integer factorization problem, Discrete logarithm problem, RSA cryptosystem, Attacks on RSA, Diffie-Hellman Key agreement Protocol, ElGamal cryptosystem, Elliptic curve cryptography,Homomorphic Encryption, Secret Sharing Schemes

UNIT IV (6 Hours)

Pseudo Random Number Generators(PRNG): LCRNG, RSA, BBS. Cryptographic Hashes for Integrity, Hash functions: MD5, Secure Hash Algorithm(SHA1, SHA512, SHA1024), Message Authentication Code(MAC),Signature schemes: RSA signature, ElGamal signature, ECDSA.

UNIT V (7 Hours)

Network Security protocols:SSL,TLS,IPSec.Application Layer Security Protocols: PGP,S/MIME,SET.