FMCE1002 CRYPTOGRAPHY (3-1-0)

Module-I (14 Hours)

Some simple Cryptosystems, Symmetric and Asymmetric Cryptosystems, Cryptanalysis, Block ciphers, Multiple Encryption, The use of block Ciphers, Stream Ciphers, The Affine Cipher, Matrices and Linear Maps, Affine Linear Block Ciphers, Vigenere, Hill and Permutation Ciphers Cryptanalysis of Affine Linear Block Ciphers, Secure cryptosystems.

Module-II (12 Hours)

The idea of public key cryptography, RSA, Rabin Encryption, Diffie-Hellman Key Exchange, ElGamal Encryption. Trial Division, p-1 Method, Quadratic sieve, Analysis of the Quadratic sieve, Efficiencency of Other Factoring Algorithms.

Module-III (14 Hours)

Discrete Logarithms: The DL Problem, Enumeration, Shanks Baby-Step giant-Step Algorithm, The Pollard ρ - Algorithm, Generalization of the Index Calculus Algorithm

Hash Functions and Compression Functions, Birthday attack, Compression Functions from Encryption Functions, Digital Signatures: Security, RSA Signatures, Signatures from Public –Key Systems, ElGamal Signatures, Blind Signatures.

Text book

1. Johannes A. Buchmann: Introduction to Cryptography, 2nd Edition , Springer

Chapters: 3, 8, 9, 10, 11(11.1-11.4), 12

Reference book

1. Neal Koblitz: A Course In number theoretic Cryptography, Springer Veriag, GTM No. 114; 1987).

2. A. J. Menezes. P. C. Van Oorschot and Scoff A. Vanstone, Hand Book of Applied Cryptography, CRC Press (1997).