Program Name: M.Tech in Computer Science & Engineering

Specialization: Information Security

Aim:

With the ever increasing dependence of information for successful business operations, great emphasis is being laid on protecting business critical information. The scope of Information Security has been undefined and has been used in a customized manner in different contexts. This program aims to provide the basics of the complete end-to-end exposure from systems engineering, operating systems, computer networks and massive data mining, which will help the students to protect organization's business critical information from unauthorized external access.

Course Name: Cryptography Basics (3-1-0-0-8)

Unit 1:
NUMBER THEORY BASICS: Modular arithmetic, primes, GCD and Chinese reminder theorems
STREAM CIPHERS: Encryption and decryption with Stream ciphers, Shift-register based stream ciphers, DES, AES
BLOCK CIPHERS: ECB, CBC, OFB,CFB, CTR,GCM modes, Double and triple encryptions.

Unit 2:
PUBLIC KEY CRYPTOGRAPHY: RSA, ElGamal, Rabins encryption schemes, Diffe-Hellman Key exchange, practical digital signatures.
ELLIPTIC CURVE CRYPTOLOGY: definitions, group properties and basic algorithms for group operations.

Unit 3:
HASH FUNCTIONS: oneway, collision resistant, preimage resistant HASH functions, Real-world examples.
MESSAGE AUTHENTICATION CODES: MAC from Hash functions, MAC from block ciphers
KEY ESTABLISHMENT PROTOCOLS: Man -in-the-middle Attack, certificates, Public Key Infrastructure and PKI based crypto systems.

Text Books:

1. Christof Paar, Jan Pelzl, Understanding Cryptography, A text book for students and practitioners, Springer Verlag, India, 2010 { INDIAN EDITION}
2. Alfred Menezes. et al, Handbook of Applied Cryptography, CRC Press, USA. { Entire book available for free download in PDF form from authors homepage}