CS502   Network Security

Prerequisites: MT104, CS302

Course contents:

Foundations of Cryptography and Security   **(10%)**
Ciphers and Secret Messages, Security Attacks and Services. Classical encryption techniques.

Mathematical Tools for Cryptography   **(5%)**
Substitutions and Permutations, Modular Arithmetic, Euclid's Algorithm, Finite Fields, Polynomial Arithmetic.

Design Principal of Block Ciphers   **(15%)**
Theory of Block ciphers, Feistel Cipher network Structures, DES and triple DES, Modes of Operation (ECB, CBC, OFB, CFB), Strength of DES., AES

Pseudo Random Numbers and Stream Ciphers   **(5%)**
Pseudo random sequences, Liner Congruential generators, Cryptographic generators, Design of stream Ciphers, RC4.

Public Key Cryptography   **(5%)**
Prime Numbers and testing for primality. Factoring large numbers, Discrete Logarithms.

Asymmetric Algorithms   **(15%)**
RSA, Diffie-Hellman,   ElGamal, Introduction of Ecliptics curve cryptosystems, Key Management, Key exchange algorithms, Public Key Cryptography Standards.

Hashes and Message Digests   **(10%)**
Message Authentication, MD5, SHA-3, HMAC

Digital Signatures, Certificate and Standards   **(10%)**
Digital signature standards (DSS and DSA), Public Key Infrastructures, Digital certificates and Basics of PKCS standards.

Authentication   **(5%)**
Kerberos , X509 Authentication Service

Web Security protocols   **(10%)**
 IP Security, Transport Layer Security (TLS)., Wireless Security,

System Security   **(10%)**
Intrusion detection , Password management. Firewalls management

Main Reading
1.   Stallings William, " Cryptography and Network Security: Principles and Practises", 5th edition, Prentice Hall
2.   Kahate Atul, "Cryptography and Network Security" Tata McGraw-Hill.

Supplementary Reading
1.   Menezes A. J., P.C. Van Oorschot and S.A. Vanstone, "Handbook of Applied Cryptrography"