CSCH 402 : Modern Cryptography

UNIT I

Introduction : Classical Cryptography and Modern Cryptography, The Setting of Private-Key Encryption, Historical Ciphers and Their Cryptanalysis, The Basic Principles of Modern Cryptography, **Perfectly-Secret Encryption :** Definitions and Basic Properties, The One-Time Pad (Vernam's Cipher), Limitations of Perfect Secrecy **Private-Key Cryptography:** Private-Key Encryption and Pseudorandomness, A Computational Approach to Cryptography, Defining Computationally-Secure Encryption, Pseudorandomness, Constructing Secure Encryption Schemes. **(16 hours)**

UNIT II

Message Authentication Codes and Collision-Resistant Hash Functions: Secure Communication and Message Integrity, Encryption vs. Message Authentication, Constructing Secure Message Authentication Codes, Collision-Resistant Hash Functions **Practical Constructions of Pseudorandom Permutations (Block Ciphers):** Substitution-Permutation Networks, Feistel Networks, DES – The Data Encryption Standard, AES – The Advanced Encryption Standard, **Public-Key (Asymmetric) Cryptography:** Number Theory and Cryptographic Hardness Assumptions, Preliminaries and Basic Group Theory. **(16 hours)**

UNIT III

Primes, Factoring, and RSA, Assumptions in Cyclic Groups, Cryptographic Applications of Number-Theoretic Assumptions, **Private-Key Management and the Public-Key Revolution:** Limitations of Private-Key Cryptography, A Partial Solution – Key Distribution Centers, The Public-Key Revolution, Diffie-Hellman Key Exchange, **Public-Key Encryption,** Hybrid Encryption, RSA Encryption, **Digital Signature Schemes:** RSA Signatures, The "Hash-and-Sign" Paradigm, Lamport's One-Time Signature Scheme, Public-Key Cryptosystems in the Random Oracle Model. **(16 hours)**

TextBooks :

(1). **"Introduction to Modern Cryptography"**, Jonathan Katz, Yehuda Lindell, Chapman & Hall/CRC, 2008

(2). **"Foundations of Cryptography - Basic Tools"**, Oded Goldreich, Cambridge University Press, 2004

(3). **"Foundations of Cryptography - Basic Applications"**, Oded Goldreich, Cambridge University Press, 2009