CSE 802 Information Security and Cryptography

Information and Network Security Concepts: Cybersecurity, Information Security and Network Security, CIA triad, Security Attacks, Services and mechanism, Various types of threats and Cryptanalysis. Symmetric Encryption: Symmetric Cipher Model, Classical Substitution and Transposition Ciphers, Block Cipher Design Principles and Data Encryption Standard, Strength of DES, Different variants of DES like 2DES, 3DES. Attack of 2DES, AES. Asymmetric Encryption: Principles of Pubic Key Cryptosystems, RSA, Discrete Logarithm, Diffie-Hellman Key Exchange, Man-in-the- middle attack on Diffie-Hellman. Hash Functions: Applications of cryptographic hash functions, Hash function requirements, Secure Hash Algorithm (SHA), Digital Signatures. Key and Identity Management including certificate management: Key exchange and random numbers, key/identity management, Symmetric key distribution using Symmetric and Asymmetric Encryption, Public Key Distribution, X.509 Certificates, PKI Architecture. User Authentication: Password based authentication, Token based authentication, Biometric authentication, Remote user authentication, security issues for user authentication, AI/ML for security systems.

Textbook and Reference:

Textbook:
– *Willam Stallings*, **Cryptography and Network Security Principles and Practice**, 8th Edition.