Cryptography

Purpose and Scope:
Cryptography helps to protect data transmitted in the likely presence of an adversary. A cryptographic transformation of data is a procedure by which plaintext data is disguised, or encrypted (ciphertext) and does not reveal the original input. The original plaintext can be recovered from the ciphertext only by the corresponding decryption key. Cryptographic techniques have many applications in electronic data transmissions, financial transactions, identifications, etc. This course deals with fundamental concepts and design principles of various cryptographic techniques with specific examples and tutorials relevant to Banking and Financial Sector. It covers basics on number theory, secret key cryptography, public key cryptography and authentication and key agreement protocols. Every module includes examples and exercises to develop both theoretical and practical skills that handle various real life financial problems.

Pre-requisite : Nil

Contents :

Module A : Introduction to Number Theory
Groups, Rings, and Fields, Prime Numbers, Modular Arithmetic, Euclid's Algorithm, Finite Fields of the Form GF *(p),* Polynomial Arithmetic, Finite Fields of the Form GF (2"), Fermat's and Euler's Theorems, Testing for Primality, Random Number Generation, Integer Factorization, Discrete Logarithms.

Module B : Classical Encryption Techniques
Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Rotor Machines, Steganography, Block Cipher Principles, The Data Encryption Standard (DES), The Strength of DES, Block Cipher Design Principles, Stream Ciphers.

Module C : Contemporary Symmetric Ciphers & Advanced Encryption Techniques
Characteristics of Advanced Symmetric Block Ciphers, Triple DES, Advance Encryption Standards (AES), Evaluation Criteria for AES, Placement of Encryption Function, Traffic Confidentiality, Key Distribution, Differential and Linear Cryptanalysis.

Module D : Public Key Cryptography
Principles of Public-Key Cryptosystems, The Diffie-Hellman Key Exchange, Message Authentication Code (MAC), MD5 Message Digest Algorithm, Secure Hash Algorithm, HMAC, The RSA Algorithm, Elliptic Curve Cryptography (ECC).

Module E : Authentication & Key Agreement Protocols
Digital Signature Standard (DSS), Digital Signature Algorithm (DSA), ECDSA, Key Distribution and Management.

References :

1. A course in number theory and cryptography (2nd edn.), Koblitz, Neal.
2. An introduction to cryptography, Mollin, Richard A.
3. Applied cryptography: protocols, algorithms, and source code in C (2nd edn.) Schneier, Bruce
4. Basic methods of cryptography Van Der Lubbe, Jan C.A.
5. Cryptography and network security: principles and practice (3rd edn.) Stallings, William
6. Cryptography: theory and practice Stinson, Douglas R.
7. Handbook of applied cryptography, Alfred J.; Van Oorschot, Paul C.; Vanstone, Scott A.