CRYPTOGRAPHY AND NETWORK SECURITY SYLLABUS

Module 1: Fundamentals of Number Theory

- Modular arithmetic
- Euclidean Algorithm
- Primality Testing
    - Fermat's Theorem
    - Euler's Theorem
- Chinese Remainder Theorem
- Discrete Logarithms

Module 2: Symmetric Encryption Algorithms

- Introduction to Stream Cipher
- Block Ciphers
    - DES
    - AES
    - IDEA
- Block Cipher Operation
- Random Bit Generation
- RC4

Module 3: Asymmetric Encryption Algorithms and Key Exchange

- Principles of Asymmetric Key Cryptography
- RSA
- ElGamal
- Elliptic Curve Cryptography
- Homomorphic Encryption
- Secret Sharing

- Key Distribution and Key Exchange Protocols
    - Diffie-Hellman Key Exchange
    - Man-in-the-Middle Attack

Module 4: Message Digest and Hash Functions

- Requirements for Hash Functions
- Security of Hash Functions
- Message Digest (MD5)
- Secure Hash Function (SHA)
- Birthday Attack
- HMAC

Module 5: Digital Signature and Authentication Protocols

- Authentication Requirements
- Authentication Functions
- Message Authentication Codes
- Digital Signature Authentication
- Authentication Protocols
- Digital Signature Standards
    - RSA Digital Signature
    - ElGamal-based Digital Signature
- Authentication Applications
    - Kerberos
    - X.509 Authentication Service
    - Public Key Infrastructure (PKI)

Module 6: Transport Layer Security and IP Security

- Transport-Layer Security
- Secure Socket Layer (SSL)
- TLS
- IP Security
    - Overview
    - IP Security Architecture
    - Encapsulating Payload Security

Module 7: E-mail, Web, and System Security

- Electronic Mail Security
    - Pretty Good Privacy (PGP)
    - S/MIME
- Web Security
    - Web Security Considerations
    - Secure Electronic Transaction Protocol
- Intruders
- Intrusion Detection
- Password Management
- Firewalls
    - Firewall Design Principles
    - Trusted Systems