PUBLIC KEY INFRASTRUCTURE AND TRUST MANAGEMENT SYLLABUS

Module 1: Public Key Cryptography Basics

- Public Key Cryptography
  - Secret Key
  - Public Key
  - Public/Private Key Pair
- Services of Public Key Cryptography
- RABIN Cryptosystem
- ElGamal Cryptosystem
- Message Integrity and Authentication
  - Random Oracle Model
  - Message Authentication
  - Cryptographic Hash Functions

Module 2: Public Key Infrastructure

- Components and Architecture of Fully Functional Public Key Infrastructure (PKI)
  - Certification Authority
  - Certificate Repository
  - Certificate Revocation
  - Key Backup and Recovery
  - Automatic Key Update
  - Key History Management
  - Cross-Certification
  - Support for Non-Repudiation
  - Time Stamping
  - Client Software
  - Core PKI Services
  - PKI-Enabled Services

    - PKI Interoperability
    - Deployment and Assessment
- PKI Data Structures
- PKI Architectures
    - Single CA
    - Hierarchical PKI
    - Mesh PKI
    - Trust Lists
    - Bridge Certification Authority (CA)
    - Registration Authority (RA)
    - Simple PKI (SPKI)
- PKI Application
    - Smart Card Integration with PKIs

Module 3: Digital Certificates

- Introduction to Digital Certificates
- Certificate Structure and Semantics
- Alternative Certificate Formats
- Certificate Policies
- Object Identifiers
- Policy Authorities
- Certification Authority
- Key/Certificate Life Cycle Management
- Certificate Revocation
- Representing Certificates in Terms of S-Expressions
- Certificate Chain

Module 4: Access Control Mechanisms and Security Challenges

- Access Control Mechanisms
    - Discretionary Access Control (DAC)
    - Mandatory Access Control (MAC)

    - Role-Based Access Control (RBAC)
- Issues
    - Revocation
    - Anonymity
    - Privacy Issues
    - Entity Authentication
    - Passwords and Challenge Response
    - Zero-Knowledge Proofs
    - Biometrics
    - Key Management
    - Security Key Distribution
    - Kerberos
    - Symmetric Key Agreement
    - Public Key Distribution and Hijacking
    - Issues of Revocation
    - Anonymity and Privacy

Module 5: Trust Models

- Distributed Trust Architecture
    - Mesh Configuration
    - Hub-and-Spoke Configuration
    - Four-Corner Trust Model
    - Web Model
    - User-Centric Trust
- Cross-Certification
- Entity Naming
- Certificate Path Processing
    - Path Construction
    - Path Validation
- Trust Anchor Considerations
- Multiple Key Pairs
- Key Pair Uses
- Relationship Between Key Pairs and Certificates

Module 6: Trust Management Systems

- Social Network-Based Trust Management System
- Reputation-Based Trust Management System
    - DMRep
    - EigenRep
    - P2Prep
- Framework for Trust Establishment
- Risks Impact on E-Commerce and E-Business
    - Information Risk
    - Technology Business Risk

Module 7: Operational Considerations

- Client-Side Software
- Off-Line Operations
- Physical Security
- Hardware Components
- User Key Compromise
- Disaster Preparation and Recovery
- Relying Party Notification
- Preparation and Recovery
- Electronic Signature Legislation and Considerations