Cryptography and Network Security

1. Introduction to Cryptography and Network Security

1.1 Security Trends - Legal & Ethical Aspects of Security
1.2 Need for Security at Multiple Levels
1.3 Model of Network Security
1.4 Security Attacks
1.5 Types of Security Attacks
1.6 Security Services
1.7 Security Mechanism
1.8 OSI Security Architecture
1.9 Cryptography
1.10 Classical Encryption Techniques
1.11 Substitution Techniques
1.12 Transposition Techniques
1.13 Steganography
1.14 Cryptanalysis

2. Symmetric Key Cryptography

2.1 Modular Arithmetic
2.2 Polynomial Arithmetic
2.3 Finite Fields
2.4 Simple DES
2.5 Data Encryption Standard (DES)
2.6 Block Cipher Design Principles
2.7 Stream Cipher
2.8 Confusion and Diffusion
2.9 Block Cipher Modes of Operation
2.10 Advanced Encryption Standards (AES)
2.11 Blowfish
2.12 RC4

3. Public Key Cryptography

3.1 Mathematics of Asymmetric Key Cryptography
3.2 Euler's Totient Function
3.3 Fermat's and Euler's Theorem
3.4 Chinese Remainder Theorem
3.5 Exponentiation and Logarithm
3.6 Euclid's Algorithm
3.7 Asymmetric Key Ciphers
3.8 RSA Cryptosystem
3.9 Key Management and Distribution
3.10 Diffie-Hellman Key Exchange
3.11 ElGamal
3.12 Elliptic Curve Arithmetic
3.13 Elliptical Curve Cryptography

4. Message Authentication and Integrity

4.1 Authentication and Authorization
4.2 MAC
4.3 Hash Function
4.4 SHA
4.5 HMAC
4.6 CMAC
4.7 Digital Signature
4.8 Authentication Protocol
4.9 Entity Authentication
4.10 Authentication Applications: Kerberos
4.11 X. 509 Authentication Services

5. Security Practice and System Security

5.1 Electronic Mail Security
5.2 Overview of IPSec
5.3 IP Security Architecture
5.4 Authentication Header (AH)
5.5 Encapsulating Security Payload (ESP)
5.6 Combining Security Association
5.7 Key Management of IPsec
5.8 Web Security
5.9 System Security: Intruders
5.10 Intrusion Detection