



| | | |
|--------------------|---|--------------------|
| Chapter 1 : | Introduction to Network Security & Cryptography | 1-1 to 1-48 |
| 1.1 | Computer Security and Network Security..... | 1-1 |
| 1.2 | Computer Security Concepts..... | 1-3 |
| 1.2.1 | Confidentiality | 1-4 |
| 1.2.2 | Integrity..... | 1-4 |
| 1.2.3 | Availability..... | 1-5 |
| 1.3 | Concept Building - Security Threats and Vulnerabilities..... | 1-6 |
| 1.3.1 | Security Threats..... | 1-6 |
| 1.3.1(A) | Comparison between Security Threats | 1-8 |
| 1.3.2 | Security Vulnerabilities | 1-8 |
| 1.4 | Access Control and Attacks..... | 1-9 |
| 1.4.1 | STRIDE Model..... | 1-11 |
| 1.5 | Types of Security Attacks (Mechanisms and Attacks)..... | 1-12 |
| 1.5.1 | Active Attacks | 1-12 |
| 1.5.2 | Passive Attacks..... | 1-14 |
| 1.5.3 | Comparison of Active and Passive Attacks | 1-16 |
| 1.6 | OSI Model..... | 1-16 |
| 1.6.1 | The OSI Security Architecture | 1-17 |
| 1.6.2 | Security Services..... | 1-18 |
| 1.6.3 | Security Mechanisms..... | 1-18 |
| 1.6.4 | Placement of Security Services and Mechanisms..... | 1-19 |
| 1.7 | Network Security Model | 1-21 |
| 1.8 | Concept Building – Information Secrecy..... | 1-23 |
| 1.9 | Concept Building - Introduction to Cryptography..... | 1-24 |
| 1.10 | Classical Encryption Techniques..... | 1-26 |
| 1.10.1 | Substitution | 1-26 |
| 1.10.1(A) | Vignere Cipher | 1-27 |
| 1.10.1(B) | Playfair Cipher | 1-29 |
| 1.10.1(C) | Hill Cipher..... | 1-38 |
| 1.10.1(D) | Difference between Monoalphabetic and Polyalphabetic Ciphers..... | 1-41 |
| 1.10.2 | Transposition..... | 1-41 |
| 1.10.2(A) | Keyed Transposition Cipher | 1-41 |
| 1.10.2(B) | Keyless Transposition Cipher | 1-43 |
| 1.11 | Introduction to Steganography | 1-44 |
| 1.11.1 | Uses of Steganography..... | 1-44 |
| 1.11.2 | Comparison between Cryptography and Steganography..... | 1-44 |



| Chapter 2 : Cryptography : Key Management, Distribution and User Authentication | | 2-1 to 2-64 |
|--|---|--------------------|
| 2.1 | Methods of Encryption | 2-1 |
| 2.1.1 | Symmetric Key Encryption | 2-2 |
| 2.1.2 | Asymmetric Key Encryption | 2-3 |
| 2.1.3 | Comparison between Symmetric and Asymmetric Keys..... | 2-5 |
| 2.2 | Cryptanalysis (Attacks on Cryptosystems) | 2-6 |
| 2.2.1 | Comparison between Differential and Linear Cryptanalysis..... | 2-7 |
| 2.3 | Concept Building - Types of Symmetric Algorithms (Ciphers) | 2-8 |
| 2.3.1 | Block Ciphers | 2-8 |
| 2.3.2 | Stream Ciphers | 2-8 |
| 2.3.3 | Comparison between Block and Stream Cipher | 2-9 |
| 2.4 | Block Cipher Principles (for DES and other Ciphers)..... | 2-9 |
| 2.5 | Data Encryption Standard (DES)..... | 2-10 |
| 2.5.1 | Block Diagram and Internals of DES..... | 2-10 |
| 2.5.2 | Block Cipher Modes of Operation (for DES and other Block Ciphers in General)..... | 2-12 |
| 2.5.3 | Comparison between Modes of Operation..... | 2-14 |
| 2.5.4 | Double DES..... | 2-15 |
| 2.5.5 | 3DES or Triple DES..... | 2-16 |
| 2.6 | Advanced Encryption Standard (AES) | 2-17 |
| 2.6.1 | Block Diagram and Internals of AES..... | 2-18 |
| 2.6.2 | Comparison between DES and AES | 2-19 |
| 2.7 | RC5 Algorithm | 2-19 |
| 2.7.1 | Major Attributes of RC5..... | 2-19 |
| 2.7.2 | Internals of RC5 Algorithm | 2-19 |
| 2.7.3 | Key Expansion | 2-19 |
| 2.7.4 | Encryption..... | 2-19 |
| 2.8 | Concept Building - Mathematics Behind Cryptography..... | 2-20 |
| 2.9 | Greatest Common Divisor (GCD)..... | 2-22 |
| 2.9.1 | Euclid's or Euclidean Algorithm | 2-23 |
| 2.9.2 | Solved Examples..... | 2-23 |
| 2.9.3 | Extended Euclidean Algorithm | 2-24 |
| 2.9.4 | Multiplicative Inverse using Extended Euclidean Algorithm | 2-28 |
| 2.10 | Public Key Cryptography | 2-30 |
| 2.10.1 | Principles of Public Key Cryptosystems..... | 2-30 |
| 2.10.2 | RSA Algorithm | 2-31 |
| 2.10.2(A) | Attacks on RSA | 2-35 |
| 2.11 | Message Authentication Requirements..... | 2-35 |
| 2.12 | Message Authentication Functions | 2-36 |
| 2.13 | Cryptographic Hash Functions..... | 2-37 |
| 2.13.1 | Introduction | 2-37 |



| | | |
|-----------|---|------|
| 2.13.2 | How does this Work?..... | 2-37 |
| 2.13.3 | Characteristics of Hash Functions..... | 2-39 |
| 2.14 | Hash Functions (Algorithms)..... | 2-41 |
| 2.14.1 | SHA-1..... | 2-41 |
| 2.14.2 | SHA-3..... | 2-42 |
| 2.15 | MAC (Message Authentication Code)..... | 2-43 |
| 2.15.1 | HMAC..... | 2-44 |
| 2.15.2 | CBC-MAC..... | 2-45 |
| 2.15.3 | CMAC..... | 2-45 |
| 2.15.4 | Comparison between Hash and MAC..... | 2-46 |
| 2.15.5 | Comparison between HMAC, CBC-MAC and CMAC..... | 2-46 |
| 2.15.6 | Comparison between Hash, MAC and Digital Signature..... | 2-46 |
| 2.16 | Security of Hash Functions and MAC..... | 2-47 |
| 2.16.1 | Security of Hash Functions..... | 2-47 |
| 2.16.2 | Attacks on Hash Functions and MAC..... | 2-48 |
| 2.17 | Digital Signature..... | 2-48 |
| 2.17.1 | How does this Work ?..... | 2-48 |
| 2.17.2 | Application and Use of Digital Signature..... | 2-49 |
| 2.17.3 | Properties of Digital Signature..... | 2-49 |
| 2.18 | PKI X.509 Certificate..... | 2-49 |
| 2.19 | Digital Signature Schemes..... | 2-51 |
| 2.19.1 | RSA Digital Signature Scheme..... | 2-51 |
| 2.19.1(A) | Key Generation..... | 2-51 |
| 2.19.1(B) | Message Signing..... | 2-51 |
| 2.19.1(C) | Signature Verification..... | 2-51 |
| 2.19.2 | Schnorr Digital Signature Scheme..... | 2-54 |
| 2.19.2(A) | Key Generation..... | 2-55 |
| 2.19.2(B) | Message Signing..... | 2-55 |
| 2.19.2(C) | Signature Verification..... | 2-55 |
| 2.19.3 | ElGamal Digital Signature Scheme..... | 2-55 |
| 2.19.3(A) | Key Generation..... | 2-55 |
| 2.19.3(B) | Message Signing..... | 2-55 |
| 2.19.3(C) | Signature Verification..... | 2-56 |
| 2.19.4 | Digital Signature Standard (DSS)..... | 2-56 |
| 2.19.4(A) | Digital Signature Algorithm (DSA)..... | 2-56 |
| 2.19.4(B) | Key Generation..... | 2-56 |
| 2.19.4(C) | Message Signing..... | 2-56 |
| 2.19.4(D) | Signature Verification..... | 2-57 |
| 2.20 | Authentication Applications (Remote user Authentication Protocols)..... | 2-57 |
| 2.20.1 | Kerberos..... | 2-57 |



| | | |
|--------|--------------------------------------|------|
| 2.20.2 | Problems Addressed by Kerberos | 2-57 |
| 2.20.3 | Components of Kerberos | 2-58 |
| 2.20.4 | How does it Work ? | 2-58 |
| 2.20.5 | Limitations of Kerberos..... | 2-60 |

Chapter 3 : Malicious Software**3-1 to 3-30**

| | | |
|----------|--|------|
| 3.1 | Malicious Software (Malware) | 3-1 |
| 3.1.1 | Types of Malware..... | 3-2 |
| 3.1.2 | Virus and Worms..... | 3-4 |
| 3.1.3 | Types of Virus..... | 3-4 |
| 3.1.4 | Types of Worms..... | 3-8 |
| 3.1.5 | Trojans (Trojan Horses)..... | 3-9 |
| 3.1.6 | Logic Bombs | 3-9 |
| 3.1.7 | Botnets (Bots) (Zombie) | 3-10 |
| 3.1.7(A) | Components of Botnets | 3-11 |
| 3.1.7(B) | Botnet Architectures..... | 3-12 |
| 3.1.7(C) | Attacks Carried out by Botnets | 3-13 |
| 3.1.8 | Rootkits | 3-14 |
| 3.1.8(A) | Types of Rootkits..... | 3-14 |
| 3.1.8(B) | Detecting Rootkits | 3-15 |
| 3.1.9 | General Guidelines for Preventing Malware | 3-16 |
| 3.2 | Social Engineering | 3-17 |
| 3.2.1 | Social Engineering..... | 3-19 |
| 3.2.2 | Countermeasures against Social Engineering (and Phishing)..... | 3-21 |
| 3.3 | Keyloggers..... | 3-22 |
| 3.3.1 | Types of Keyloggers..... | 3-23 |
| 3.3.2 | Preventing Keylogging..... | 3-23 |
| 3.4 | DoS and DDoS (Flooding Attacks) | 3-23 |
| 3.4.1 | Types of DDoS Attacks | 3-25 |
| 3.4.2 | Preventing DDoS Attacks..... | 3-26 |
| 3.5 | Unsolicited Bulk Email (UBE) (SPAM)..... | 3-27 |
| 3.6 | Backdoors (Trapdoors)..... | 3-28 |
| 3.7 | Attack Agents | 3-28 |
| 3.8 | System Corruption and Information Theft..... | 3-28 |

Chapter 4 : IP Security, Transport Level Security and Email Security**4-1 to 4-32**

| | | |
|-------|---|-----|
| 4.1 | IP Security | 4-1 |
| 4.1.1 | IPv4 | 4-2 |
| 4.1.2 | IPv6 | 4-2 |
| 4.1.3 | Internet Protocol Security (IPSec)..... | 4-2 |
| 4.1.4 | Authentication Header (AH) | 4-5 |



| | | |
|---|---|--------------------|
| 4.1.5 | Encapsulating Security Payload (ESP)..... | 4-5 |
| 4.1.6 | Internet Security Association and Key Management Protocol (ISAKMP)..... | 4-6 |
| 4.1.7 | Internet Key Exchange (IKE)..... | 4-8 |
| 4.1.8 | OAKLEY Key Determination Protocol..... | 4-9 |
| 4.2 | Web Security..... | 4-10 |
| 4.3 | Secure Socket Layer (SSL)..... | 4-10 |
| 4.3.1 | Overview of SSL Protocol..... | 4-11 |
| 4.3.1(A) | Session and Connection States..... | 4-11 |
| 4.3.1(B) | SSL Record Layer Protocol..... | 4-12 |
| 4.3.1(C) | SSL Change Cipher Spec Protocol..... | 4-13 |
| 4.3.1(D) | SSL Alert Protocol..... | 4-14 |
| 4.3.1(E) | SSL Handshake Protocols..... | 4-15 |
| 4.3.2 | Transport Layer Security (TLS)..... | 4-16 |
| 4.4 | HTTPS..... | 4-17 |
| 4.4.1 | Comparison between HTTP and HTTPS..... | 4-17 |
| 4.4.2 | Motivation / Benefits of using HTTPS..... | 4-18 |
| 4.4.3 | Format, Port Number and Representation..... | 4-18 |
| 4.5 | Secure Shell (SSH)..... | 4-20 |
| 4.5.1 | Usage of SSH..... | 4-20 |
| 4.5.2 | SSH Protocol..... | 4-20 |
| 4.5.3 | Establishing SSH connection..... | 4-23 |
| 4.6 | Email Security..... | 4-23 |
| 4.6.1 | Pretty Good Privacy (PGP)..... | 4-23 |
| 4.6.1(A) | Web of Trust..... | 4-23 |
| 4.6.1(B) | PGP Services..... | 4-24 |
| 4.6.1(C) | PGP Algorithms..... | 4-26 |
| 4.6.2 | MIME..... | 4-27 |
| 4.6.3 | S/MIME..... | 4-27 |
| 4.6.3(A) | S/MIME Services..... | 4-27 |
| 4.6.3(B) | S/MIME Algorithms..... | 4-27 |
| 4.6.3(C) | S/MIME Cryptographic Message Syntax (CMS)..... | 4-28 |
| 4.6.3(D) | Comparison between PGP and S/MIME..... | 4-28 |
| 4.7 | VPN (Transport Level Security)..... | 4-29 |
| 4.7.1 | Types of VPN..... | 4-29 |
| 4.7.2 | Challenges of using VPN..... | 4-30 |
| Chapter 5 : Network Management Security and Network Access Control | | 5-1 to 5-26 |
| 5.1 | Introduction to Networking Components..... | 5-1 |
| 5.2 | Network Management Security - SNMPv3..... | 5-7 |
| 5.2.1 | What is SNMP?..... | 5-7 |
| 5.2.2 | How SNMP Works?..... | 5-7 |



| | | |
|-------|--|------|
| 5.2.3 | SNMP Management Information Base (MIBs)..... | 5-8 |
| 5.2.4 | SNMP Versions | 5-10 |
| 5.2.5 | Comparison between SNMP Versions..... | 5-11 |
| 5.2.6 | Security Enhancements in SNMPv3 | 5-11 |
| 5.2.7 | Architecture Change in SNMPv3 for Security | 5-11 |
| 5.2.8 | The SNMPv3 Engine..... | 5-12 |
| 5.2.9 | SNMPv3 Applications..... | 5-13 |
| 5.3 | User-based Security Model (USM)..... | 5-13 |
| 5.3.1 | Common Terms Used by USM | 5-13 |
| 5.3.2 | SNMPv3 Packet Format..... | 5-14 |
| 5.3.3 | SNMPv3 User Attributes | 5-16 |
| 5.4 | View-based Access Control Model (VACM) | 5-16 |
| 5.4.1 | How VACM Works?..... | 5-18 |
| 5.5 | Network Access Control (NAC)..... | 5-19 |
| 5.5.1 | Principal Elements of NAC | 5-20 |
| 5.5.2 | Principal NAC Enforcement Methods..... | 5-22 |
| 5.5.3 | Use Cases for Network Access Control (NAC) | 5-23 |
| 5.5.4 | Types of Network Access Control (NAC) | 5-23 |
| 5.5.5 | How to Implement NAC Solutions? | 5-24 |

Chapter 6 : System Security**6-1 to 6-10**

| | | |
|-------|---|-----|
| 6.1 | Computer Intrusions and Intrusion Detection and Prevention Systems (IDS/IPS)..... | 6-1 |
| 6.1.1 | Introduction..... | 6-1 |
| 6.1.2 | Need for IDS..... | 6-2 |
| 6.1.3 | Types of IDS..... | 6-2 |
| 6.1.4 | Limitations and Challenges of IDS | 6-3 |
| 6.2 | Firewalls..... | 6-4 |
| 6.2.1 | Classification of Firewalls..... | 6-5 |
| 6.2.2 | Challenges in Managing and Deploying Firewalls | 6-8 |
| 6.3 | DMZ Networks (Firewall Design Principles) | 6-9 |

□□□