



---

|   |                    |
|---|--------------------|
| <b>Chapter 1 : Introduction to Information Security</b>                     | <b>1-1 to 1-22</b> |
| 1.1 Foundations of Security.....  | 1-1                |
| 1.2 Information Security Concepts (Computer Security Concepts) .....        | 1-3                |
| 1.2.1 Confidentiality .....   | 1-3                |
| 1.2.2 Integrity .....   | 1-4                |
| 1.2.3 Availability .....  | 1-4                |
| 1.3 Concept Building - Security Threats and Vulnerabilities.....            | 1-5                |
| 1.3.1 Security Threats.....   | 1-5                |
| 1.3.1(A) Comparison between Security Threats.....                           | 1-7                |
| 1.3.2 Security Vulnerabilities.....   | 1-7                |
| 1.4 Access Control and Attacks.....   | 1-8                |
| 1.4.1 STRIDE Model .....  | 1-10               |
| 1.5 Types of Security Attacks .....   | 1-11               |
| 1.5.1 Active Attacks .....  | 1-11               |
| 1.5.2 Passive Attacks.....  | 1-13               |
| 1.5.3 Comparison of Active and Passive Attacks.....                         | 1-14               |
| 1.6 OSI Model.....  | 1-15               |
| 1.6.1 The OSI Security Architecture.....                                    | 1-16               |
| 1.6.2 Security Services .....   | 1-17               |
| 1.6.3 Security Mechanisms.....  | 1-17               |
| 1.6.4 Placement of Security Services and Mechanisms.....                    | 1-18               |
| 1.7 Network Security Model .....  | 1-20               |
| <b>Chapter 2 : Symmetric Key Cryptography</b>                               | <b>2-1 to 2-39</b> |
| 2.1 Concept Building – Information Secrecy .....                            | 2-1                |
| 2.2 Concept Building - Introduction to Cryptography .....                   | 2-2                |
| 2.3 Classical Encryption Techniques.....                                    | 2-4                |
| 2.3.1 Substitution.....   | 2-4                |
| 2.3.1(A) Vignere Cipher .....   | 2-5                |
| 2.3.1(B) Playfair Cipher .....  | 2-7                |
| 2.3.1(C) Hill Cipher .....  | 2-15               |
| 2.3.1(D) Difference between Monoalphabetic and Polyalphabetic Ciphers ..... | 2-18               |
| 2.3.2 Transposition.....  | 2-19               |

---



|          |  |      |
|----------|--|------|
| 2.3.2(A) | Keyed Transposition Cipher .....   | 2-19 |
| 2.3.2(B) | Keyless Transposition Cipher.....  | 2-20 |
| 2.4      | Methods of Encryption.....   | 2-21 |
| 2.4.1    | Symmetric Key Encryption .....   | 2-21 |
| 2.4.2    | Asymmetric Key Encryption .....  | 2-22 |
| 2.4.3    | Comparison between Symmetric and Asymmetric Keys.....                              | 2-25 |
| 2.5      | Cryptanalysis (Attacks on Cryptosystems) .....                                     | 2-25 |
| 2.5.1    | Comparison between Differential and Linear Cryptanalysis.....                      | 2-26 |
| 2.6      | Concept Building - Types of Symmetric Algorithms (Ciphers) .....                   | 2-27 |
| 2.6.1    | Block Ciphers.....   | 2-27 |
| 2.6.2    | Stream Ciphers.....  | 2-27 |
| 2.6.3    | Comparison between Block and Stream Cipher .....                                   | 2-28 |
| 2.7      | Block Cipher Principles (for DES and other Ciphers).....                           | 2-28 |
| 2.8      | Data Encryption Standard (DES).....  | 2-29 |
| 2.8.1    | Block Diagram and Internals of DES.....  | 2-29 |
| 2.8.2    | Block Cipher Modes of Operation (for DES and other Block Ciphers in General) ..... | 2-31 |
| 2.8.3    | Comparison between Modes of Operation.....   | 2-33 |
| 2.8.4    | Double DES.....  | 2-34 |
| 2.8.5    | 3DES or Triple DES .....   | 2-35 |
| 2.9      | Advanced Encryption Standard (AES).....  | 2-35 |
| 2.9.1    | Block Diagram and Internals of AES.....  | 2-36 |
| 2.9.2    | Comparison between DES and AES.....  | 2-37 |

---

**Chapter 3 : Asymmetric Key Cryptography**
**3-1 to 3-30**

|       |   |      |
|-------|---|------|
| 3.1   | Mathematics Behind Cryptography.....                            | 3-1  |
| 3.2   | Greatest Common Divisor (GCD).....                              | 3-4  |
| 3.2.1 | Euclid's or Euclidean Algorithm .....                           | 3-4  |
| 3.2.2 | Solved Examples .....   | 3-4  |
| 3.2.3 | Extended Euclidean Algorithm .....                              | 3-5  |
| 3.2.4 | Multiplicative Inverse using Extended Euclidean Algorithm ..... | 3-9  |
| 3.2.5 | Euler's Theorem (Euler's Totient Function).....                 | 3-11 |
| 3.2.6 | Fermat's Theorem.....   | 3-13 |
| 3.2.7 | Chinese Remainder Theorem.....                                  | 3-13 |



|   |   |                    |
|---|---|--------------------|
| 3.3   | Asymmetric Key Ciphers (Public Key Cryptography) .....            | 3-18               |
| 3.3.1   | Principles of Public Key Cryptosystems .....                      | 3-18               |
| 3.4   | RSA.....  | 3-18               |
| 3.4.1   | Attacks on RSA.....   | 3-21               |
| 3.5   | Diffie-Hellman Key Exchange Algorithm.....                        | 3-22               |
| 3.6   | Elliptic Curve Arithmetic and Cryptography .....                  | 3-24               |
| 3.6.1   | How does it work? .....   | 3-25               |
| 3.7   | ElGamal Curve Arithmetic and Cryptography.....                    | 3-26               |
| 3.8   | Key Management.....   | 3-27               |
| 3.8.1   | Key States.....   | 3-28               |
| 3.8.2   | Cryptoperiod (Key Lifetime).....                                  | 3-29               |
| 3.8.3   | Key Management Principles.....                                    | 3-29               |
| <b>Chapter 4 : Data Integrity Algorithms and Web Security</b> |   | <b>4-1 to 4-50</b> |
| 4.1   | Message Authentication Requirements .....                         | 4-2                |
| 4.2   | Message Authentication Functions .....                            | 4-3                |
| 4.3   | Cryptographic Hash Functions.....                                 | 4-3                |
| 4.3.1   | Introduction (Applications of Cryptographic Hash Functions) ..... | 4-3                |
| 4.3.2   | How does this Work? .....   | 4-4                |
| 4.3.3   | Characteristics of Hash Functions.....                            | 4-5                |
| 4.4   | Hash Functions (Algorithms).....                                  | 4-6                |
| 4.4.1   | SHA-1 .....   | 4-7                |
| 4.4.2   | SHA-3 .....   | 4-8                |
| 4.4.3   | MD4.....  | 4-9                |
| 4.4.3(A)  | Major Attributes of MD4 .....                                     | 4-9                |
| 4.4.4   | MD5.....  | 4-9                |
| 4.4.4(A)  | Major attributes of MD5 .....                                     | 4-9                |
| 4.4.4(B)  | MD5 Algorithm Details .....                                       | 4-9                |
| 4.5   | Message Authentication Code (MAC).....                            | 4-10               |
| 4.5.1   | HMAC .....  | 4-11               |
| 4.5.2   | CBC-MAC.....  | 4-12               |
| 4.5.3   | CMAC.....   | 4-12               |
| 4.5.4   | Comparison between Hash and MAC.....                              | 4-13               |



---

|           |   |      |
|-----------|---|------|
| 4.5.5     | Comparison between HMAC, CBC-MAC and CMAC.....          | 4-13 |
| 4.5.6     | Comparison between Hash, MAC and Digital Signature..... | 4-13 |
| 4.6       | Security of Hash Functions and MAC.....                 | 4-14 |
| 4.6.1     | Security of Hash Functions .....                        | 4-14 |
| 4.6.2     | Attacks on Hash Functions and MAC.....                  | 4-14 |
| 4.7       | Digital Signature .....                                 | 4-15 |
| 4.7.1     | How does this Work? .....                               | 4-15 |
| 4.7.2     | Application and Use of Digital Signature.....           | 4-16 |
| 4.7.3     | Properties of Digital Signature.....                    | 4-16 |
| 4.8       | PKI X.509 Certificate - Digital Certificate .....       | 4-16 |
| 4.9       | Digital Signature Schemes.....                          | 4-17 |
| 4.9.1     | RSA Digital Signature Scheme .....                      | 4-17 |
| 4.9.1(A)  | Key Generation.....                                     | 4-17 |
| 4.9.1(B)  | Message Signing.....                                    | 4-17 |
| 4.9.1(C)  | Signature Verification .....                            | 4-18 |
| 4.9.2     | Schnorr Digital Signature Scheme.....                   | 4-21 |
| 4.9.2(A)  | Key Generation.....                                     | 4-21 |
| 4.9.2(B)  | Message Signing.....                                    | 4-21 |
| 4.9.2(C)  | Signature Verification .....                            | 4-21 |
| 4.9.3     | ElGamal Digital Signature Scheme .....                  | 4-21 |
| 4.9.3(A)  | Key Generation.....                                     | 4-21 |
| 4.9.3(B)  | Message Signing.....                                    | 4-21 |
| 4.9.3(C)  | Signature Verification .....                            | 4-22 |
| 4.9.4     | Digital Signature Standard (DSS).....                   | 4-22 |
| 4.9.4(A)  | Digital Signature Algorithm (DSA) .....                 | 4-22 |
| 4.9.4(B)  | Key Generation.....                                     | 4-22 |
| 4.9.4(C)  | Message Signing.....                                    | 4-22 |
| 4.9.4(D)  | Signature Verification .....                            | 4-23 |
| 4.10      | Web Security.....                                       | 4-23 |
| 4.10.1    | Secure Socket Layer (SSL).....                          | 4-23 |
| 4.10.2    | Overview of SSL Protocol .....                          | 4-24 |
| 4.10.2(A) | Session and Connection States.....                      | 4-24 |
| 4.10.2(B) | SSL Record Layer Protocol.....                          | 4-25 |

---



---

|           |   |      |
|-----------|---|------|
| 4.10.2(C) | SSL Change Cipher Spec Protocol .....                                   | 4-26 |
| 4.10.2(D) | SSL Alert Protocol .....  | 4-26 |
| 4.10.2(E) | SSL Handshake Protocols .....   | 4-27 |
| 4.10.3    | Transport Layer Security (TLS).....                                     | 4-29 |
| 4.11      | HTTPS .....   | 4-29 |
| 4.11.1    | Comparison between HTTP and HTTPS.....                                  | 4-29 |
| 4.11.2    | Motivation / Benefits of using HTTPS .....                              | 4-30 |
| 4.11.3    | Format, Port Number and Representation.....                             | 4-30 |
| 4.12      | Secure Shell (SSH) .....  | 4-31 |
| 4.12.1    | Usage of SSH .....  | 4-32 |
| 4.12.2    | SSH Protocol .....  | 4-32 |
| 4.12.3    | Establishing SSH connection .....                                       | 4-34 |
| 4.13      | Email Security .....  | 4-35 |
| 4.13.1    | Pretty Good Privacy (PGP) .....   | 4-35 |
| 4.13.1(A) | Web of Trust .....  | 4-35 |
| 4.13.1(B) | PGP Services .....  | 4-36 |
| 4.13.1(C) | PGP Algorithms .....  | 4-38 |
| 4.13.2    | MIME .....  | 4-38 |
| 4.13.3    | S/MIME .....  | 4-38 |
| 4.13.3(A) | S/MIME Services.....  | 4-38 |
| 4.13.3(B) | S/MIME Algorithms.....  | 4-39 |
| 4.13.3(C) | S/MIME Cryptographic Message Syntax (CMS) .....                         | 4-39 |
| 4.13.3(D) | Comparison between PGP and S/MIME.....                                  | 4-40 |
| 4.14      | IP Security.....  | 4-40 |
| 4.14.1    | IPv4 .....  | 4-40 |
| 4.14.2    | IPv6 .....  | 4-41 |
| 4.14.3    | Internet Protocol Security (IPSec) .....                                | 4-41 |
| 4.14.4    | Authentication Header (AH) .....  | 4-43 |
| 4.14.5    | Encapsulating Security Payload (ESP) .....                              | 4-44 |
| 4.14.6    | Internet Security Association and Key Management Protocol (ISAKMP)..... | 4-45 |
| 4.14.7    | Internet Key Exchange (IKE) .....                                       | 4-46 |
| 4.14.8    | OAKLEY Key Determination Protocol.....                                  | 4-48 |

---



---

|   |                    |
|---|--------------------|
| <b>Chapter 5 : Network and System Security</b>  | <b>5-1 to 5-92</b> |
| 5.1 The OSI Security Architecture .....   | 5-1                |
| 5.2 Access Control.....   | 5-1                |
| 5.3 Denial of Service (DoS) and Distributed Denial of Service (DDoS) (Flooding Attacks) ..... | 5-2                |
| 5.3.1 Botnet .....  | 5-3                |
| 5.3.2 Types of DDoS Attacks .....   | 5-3                |
| 5.3.3 Preventing DDoS Attacks.....  | 5-4                |
| 5.4 Computer Intrusions and Intrusion Detection Systems (IDS/IPS) .....                       | 5-5                |
| 5.4.1 Introduction.....   | 5-5                |
| 5.4.2 Need for IDS.....   | 5-5                |
| 5.4.3 Types of IDS .....  | 5-6                |
| 5.4.4 Limitations and Challenges of IDS.....  | 5-7                |
| 5.5 Honeypot.....   | 5-7                |
| 5.6 Firewalls .....   | 5-8                |
| 5.6.1 Components of a Firewall Rule (Firewall Characteristics and Access Policy) .....        | 5-9                |
| 5.6.2 Classification of Firewalls.....  | 5-9                |
| 5.6.3 Challenges in Managing and Deploying Firewalls.....                                     | 5-11               |
| 5.7 DMZ Networks .....  | 5-12               |
| 5.8 Operating System Security.....  | 5-13               |
| 5.8.1 Memory and Address Protection .....   | 5-14               |
| 5.8.2 File Protection Mechanisms .....  | 5-19               |
| 5.9 Application Security.....   | 5-24               |
| 5.9.1 OWASP Top 10 .....  | 5-24               |
| 5.9.2 Linux and Windows Vulnerabilities .....   | 5-44               |
| 5.9.2(A) Vulnerabilities .....  | 5-44               |
| 5.9.2(B) File System Security .....   | 5-52               |
| 5.9.3 Security Maintenance.....   | 5-70               |
| 5.9.4 Need for Security at Multiple Levels .....  | 5-71               |
| 5.10 Access Control Policies and Models.....  | 5-73               |
| 5.10.1 Discretionary Access Control (DAC).....  | 5-74               |
| 5.10.2 Mandatory Access Controls (MAC) .....  | 5-76               |
| 5.10.2(A) Security Labels .....   | 5-76               |

---



|  |  |                    |
|--|--|--------------------|
| 5.10.2(B)                                  | Clearance Level .....  | 5-77               |
| 5.10.2(C)                                  | Access Decisions in MAC .....  | 5-77               |
| 5.10.3                                     | Role-Based Access Control (RBAC) .....                               | 5-78               |
| 5.10.4                                     | Attribute-Based Access Control (ABAC) .....                          | 5-80               |
| 5.10.4(A)                                  | Attributes .....   | 5-80               |
| 5.10.4(B)                                  | Policy .....   | 5-80               |
| 5.10.4(C)                                  | Access Decision in ABAC .....  | 5-81               |
| 5.11                                       | Concepts of Trusted System and Trusted Computing .....               | 5-82               |
| 5.11.1                                     | Bell-LaPadula (BLP) Model .....                                      | 5-82               |
| 5.11.2                                     | Biba Model .....   | 5-86               |
| <b>Chapter 6 : Cybersecurity and Tools</b> |  | <b>6-1 to 6-39</b> |
| 6.1  | Legal System and Cybercrime .....                                    | 6-1                |
| 6.1.1                                      | Introduction, Definition and Origin .....                            | 6-2                |
| 6.1.2                                      | Cybercrime and Information Security .....                            | 6-2                |
| 6.1.3                                      | Cloud Computing and Cybercrime .....                                 | 6-4                |
| 6.1.4                                      | Characteristics of Cloud Computing that Attract Cybercriminals ..... | 6-5                |
| 6.1.5                                      | Lifecycle of a Cybercrime with Cloud Computing .....                 | 6-6                |
| 6.1.6                                      | Typical Uses of Cloud Computing in Cybercrime .....                  | 6-6                |
| 6.1.7                                      | Acceptable Use Policy .....  | 6-7                |
| 6.1.8                                      | Categories of Cybercrimes .....                                      | 6-9                |
| 6.1.9                                      | Classification of Cybercrimes .....                                  | 6-10               |
| 6.1.10                                     | The Legal Perspectives of Cybercrimes .....                          | 6-11               |
| 6.2  | Categories of Cybercrime .....                                       | 6-21               |
| 6.2.1                                      | Social Engineering .....   | 6-21               |
| 6.2.2                                      | Social Engineering – The Attack Cycle .....                          | 6-23               |
| 6.2.3                                      | Countermeasures against Social Engineering (and Phishing) .....      | 6-25               |
| 6.3  | Cyberstalking .....  | 6-25               |
| 6.3.1                                      | Cyberstalking Harassments .....                                      | 6-25               |
| 6.3.2                                      | Types of Stalkers .....  | 6-26               |
| 6.3.3                                      | How cyberstalking works ? .....                                      | 6-27               |
| 6.3.4                                      | How to safeguard yourself from stalking ? .....                      | 6-28               |
| 6.3.5                                      | Provisions in the Indian Jurisdiction for Stalking .....             | 6-29               |



---

---

|       |  |      |
|-------|--|------|
| 6.4   | Proxy Servers .....                            | 6-29 |
| 6.4.1 | Security Benefits Provided by Proxies .....    | 6-29 |
| 6.4.2 | Anonymizers .....                              | 6-30 |
| 6.4.3 | Security Benefits Provided by Anonymizers..... | 6-31 |
| 6.4.4 | Comparison between Proxy and Anonymizer .....  | 6-31 |
| 6.5   | Password Cracking .....                        | 6-31 |
| 6.5.1 | Password Cracking Techniques.....              | 6-32 |
| 6.5.2 | Password Cracking Tools .....                  | 6-34 |
| 6.5.3 | Preventing Password Cracking.....              | 6-34 |
| 6.6   | Keyloggers .....                               | 6-35 |
| 6.6.1 | Types of Keyloggers.....                       | 6-36 |
| 6.6.2 | Preventing Keylogging.....                     | 6-36 |
| 6.7   | Spywares.....                                  | 6-36 |
| 6.7.1 | Types of Spyware.....                          | 6-36 |
| 6.7.2 | Preventing Spyware.....                        | 6-37 |