



Chapter 1 : Introduction and Number Theory	1-1 to 1-57
1.1	Concept Building - Security - What is it really?..... 1-2
1.2	Concept Building - Information Security Concepts..... 1-4
1.2.1	Confidentiality..... 1-4
1.2.2	Integrity..... 1-5
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	Concept building - Access Control and Attacks..... 1-9
1.4.1	STRIDE Model..... 1-10
1.5	OSI Model..... 1-11
1.5.1	The OSI Security Architecture..... 1-12
1.5.2	Security Services..... 1-13
1.5.3	Security Mechanisms..... 1-13
1.5.4	Placement of Security Services and Mechanisms..... 1-14
1.6	Network Security Model..... 1-16
1.7	Types of Security Attacks..... 1-17
1.7.1	Active Attacks..... 1-17
1.7.2	Passive Attacks..... 1-19
1.7.3	Comparison between Active and Passive Attacks..... 1-20
1.8	Concept Building – Information Secrecy..... 1-21
1.9	Concept Building - Introduction to Cryptography..... 1-22
1.10	Classical Encryption Techniques..... 1-23
1.10.1	Substitution Cipher..... 1-23
1.10.1(A)	Vignere Cipher..... 1-24
1.10.1(B)	Playfair Cipher..... 1-26
1.10.1(C)	Hill Cipher..... 1-35
1.10.1(D)	Affine Cipher..... 1-36
1.10.2	Transposition Techniques..... 1-39
1.10.2(A)	Keyed Transposition Cipher..... 1-40
1.10.2(B)	Keyless Transposition Cipher..... 1-41



1.11	Methods of Encryption.....	1-41
1.11.1	Symmetric Key Encryption	1-42
1.11.2	Asymmetric Key Encryption.....	1-43
1.11.3	Comparison between Symmetric and Asymmetric Keys	1-45
1.12	Modular Arithmetic and Number Theory	1-46
1.13	Greatest Common Divisor (GCD)	1-48
1.13.1	Euclid's or Euclidean Algorithm	1-48
1.13.2	Extended Euclidean Algorithm	1-49
1.13.3	Multiplicative Inverse using Extended Euclidean Algorithm.....	1-53
Chapter 2 : Symmetric and Asymmetric Key Cryptography and Key Management		2-1 to 2-30
2.1	Concept Building - Types of Symmetric Algorithms (Ciphers)	2-2
2.1.1	Block Ciphers	2-2
2.1.2	Stream Ciphers.....	2-2
2.1.3	Comparison between Block and Stream Cipher	2-3
2.1.4	Block Cipher Principles.....	2-3
2.2	Data Encryption Standard (DES)	2-4
2.2.1	Block Diagram and Internals of DES	2-5
2.2.2	Block Cipher Modes of Operation (for DES and other Block Ciphers in General)	2-7
2.2.3	Comparison between Modes of Operation.....	2-8
2.2.4	Double DES.....	2-9
2.2.5	3DES or Triple DES	2-10
2.3	Advanced Encryption Standard (AES)	2-10
2.3.1	Block Diagram and Internals of AES.....	2-11
2.3.2	Comparison between DES and AES	2-12
2.4	Concept Building - Attacks on Cryptosystems.....	2-12
2.4.1	Comparison between Differential and Linear Cryptanalysis.....	2-13
2.5	Public Key Cryptography	2-13
2.5.1	Principles of Public Key Cryptosystems	2-14
2.5.2	RSA Algorithm	2-14
2.5.3	Knapsack Algorithm	2-17
2.6	Key Management Techniques.....	2-18
2.6.1	What is a Key?	2-18
2.6.2	Key States	2-19
2.6.3	Cryptoperiod (Key lifetime)	2-19



2.6.4	Key Management Principles.....	2-20
2.6.5	Symmetric Key Distribution.....	2-20
2.6.5(A)	Symmetric Key Distribution using Symmetric Encryption.....	2-20
2.6.5(B)	Symmetric Key Distribution using Asymmetric Encryption.....	2-21
2.6.6	Asymmetric Key Distribution (Distribution of Public Keys).....	2-22
2.6.7	Key Management using Diffie Hellman Key Exchange.....	2-23
2.7	Digital Certificate - X.509.....	2-26
2.8	Public Key Infrastructure (PKI).....	2-27
2.8.1	Components of PKI.....	2-27
2.9	Needham-Schroeder protocol.....	2-29
2.10	Kerberos : Kerberos Authentication protocol.....	2-29

Chapter 3 : Cryptographic Hash Functions**3-1 to 3-14**

3.1	Concept Building – Information Accuracy.....	3-1
3.2	Message Authentication Functions.....	3-2
3.3	Cryptographic Hash Functions.....	3-3
3.3.1	Introduction.....	3-3
3.3.2	How does this Work?.....	3-3
3.3.3	Characteristics / Properties of Secure Hash Functions.....	3-4
3.4	Hash Functions (Algorithms).....	3-6
3.4.1	SHA-1.....	3-7
3.4.2	SHA-3.....	3-8
3.4.3	MD5.....	3-9
3.4.3(A)	Major Attributes of MD5.....	3-9
3.4.3(B)	MD5 Algorithm Details.....	3-9
3.4.4	Comparison between SHA and MD5.....	3-10
3.5	MAC (Message Authentication Code).....	3-10
3.5.1	HMAC.....	3-11
3.5.2	CBC-MAC.....	3-12
3.5.3	CMAC.....	3-12
3.5.4	Comparison between Hash and MAC.....	3-13
3.5.5	Comparison between HMAC, CBC-MAC and CMAC.....	3-13
3.6	Security of Hash Functions and MAC.....	3-13
3.6.1	Security of Hash Functions.....	3-13
3.6.2	Attacks on Hash Functions and MAC.....	3-14



Chapter 4 : Authentication Protocols and Digital Signature Schemes	4-1 to 4-18
4.1 User and Entity Authentication	4-1
4.1.1 Types of Authentication Methods.....	4-2
4.1.2 Comparison between the Authentication Types.....	4-6
4.2 Factors of Authentication	4-6
4.3 One-way and Mutual Authentication Schemes.....	4-7
4.3.1 Needham Schroeder Authentication Protocol (Challenge Response Based Authentication).....	4-7
4.3.1(A) The Needham–Schroeder Symmetric Key Based Authentication Protocol.....	4-7
4.3.1(B) The Needham–Schroeder Asymmetric Key Based Authentication Protocol.....	4-8
4.3.2 Kerberos Authentication Protocol.....	4-9
4.3.2(A) Problems Addressed by Kerberos.....	4-10
4.3.2(B) Components of Kerberos	4-10
4.3.2(C) How does it work?.....	4-10
4.3.2(D) Limitations of Kerberos.....	4-12
4.4 Digital Signature.....	4-12
4.4.1 How does this work?.....	4-12
4.4.2 Application and use of Digital Signature.....	4-13
4.4.3 Properties of Digital Signature.....	4-13
4.5 Attacks on Digital Signature	4-13
4.6 RSA Digital Signature Scheme	4-13
Chapter 5 : Network Security and Applications	5-1 to 5-39
5.1 Network Security Basics.....	5-2
5.2 TCP/IP Vulnerabilities (Layer Wise).....	5-2
5.2.1 Packet Sniffing.....	5-3
5.2.2 ARP Spoofing.....	5-4
5.2.3 Port Scanning.....	5-5
5.2.3(A) Port Scanning Techniques	5-6
5.2.4 IP Spoofing.....	5-7
5.2.5 Denial of Service (DoS) and Distributed Denial of Service (DDoS).....	5-7
5.2.5(A) Botnet.....	5-8
5.2.5(B) Types of DDoS Attacks	5-9
5.2.5(C) Preventing DDoS Attacks	5-10
5.3 Internet Security Protocols.....	5-10



5.3.1	Secure Socket Layer (SSL)	5-11
5.3.1(A)	Overview of SSL Protocol	5-12
5.3.1(B)	SSL Record Layer Protocol	5-13
5.3.1(C)	SSL Change Cipher Spec Protocol	5-14
5.3.1(D)	SSL Alert Protocol	5-14
5.3.1(E)	SSL Handshake Protocol	5-15
5.3.2	Transport Layer Security (TLS)	5-17
5.3.3	Internet Protocol Security (IPSec)	5-19
5.3.3(A)	Security Association	5-20
5.3.3(B)	Modes of Operation	5-21
5.3.3(C)	Applications / Benefits / Usage of IPSec	5-21
5.3.3(D)	How does IPSec work?	5-22
5.3.3(E)	Security Protocols/ Services Provided by IPSec	5-22
5.4	Secure Email	5-26
5.4.1	Pretty Good Privacy (PGP)	5-26
5.4.1(A)	PGP Services	5-28
5.4.1(C)	PGP Algorithms	5-30
5.4.2	S/MIME	5-30
5.4.2(A)	S/MIME Services	5-30
5.4.2(B)	S/MIME Algorithms	5-31
5.4.2(C)	S/MIME Cryptographic Message Syntax (CMS)	5-31
5.4.3	Firewalls	5-31
5.4.3(A)	Components of a Firewall Rule	5-32
5.4.3(B)	Classification of Firewalls	5-32
5.4.3(C)	Challenges in Managing and Deploying Firewalls	5-35
5.4.4	Intrusion Detection Systems (IDS)	5-35
5.4.4(A)	Introduction	5-36
5.4.4(B)	Need for IDS	5-36
5.4.4(C)	Types of IDS	5-36
5.4.4(D)	Limitations and Challenges of IDS	5-37

Chapter 6 : System Security**6-1 to 6-37**

6.1	Software Vulnerabilities	6-1
6.2	Buffer Overflow	6-3
6.2.1	Causes of Buffer Overflow and Suggested Protection Mechanism	6-6



6.2.1(A)	Low-level Programming Languages.....	6-7
6.2.1(B)	Unsafe Libraries	6-7
6.2.1(C)	Poor Coding Practices.....	6-8
6.2.1(D)	Lack of Secure Code Review and Analysis.....	6-8
6.2.1(E)	Lack of Penetration Testing.....	6-10
6.2.1(F)	No Specific Buffer Overflow Protection in Place.....	6-10
6.2.2	Specific Protection Mechanisms for Buffer Overflow.....	6-10
6.2.2(A)	Operating System Based Buffer Overflow Protection Mechanisms.....	6-11
6.2.2(B)	Compiler Based Buffer Overflow Protection Mechanisms.....	6-13
6.3	Types of Buffer Overflow.....	6-17
6.3.1	Based on Area of Memory	6-17
6.3.1(A)	Stack Overflow	6-17
6.3.1(B)	Heap Overflow	6-18
6.3.2	Based on Exploit.....	6-19
6.3.2(A)	Off-By-One.....	6-19
6.3.2(B)	Format String.....	6-19
6.3.2(C)	Integer	6-21
6.4	SQL Injection (SQLi)	6-21
6.4.1	How does SQLi Work?	6-22
6.4.2	Types of SQLi	6-24
6.4.2(A)	Based on the Order of Attack.....	6-24
6.4.2(B)	In-band.....	6-25
6.4.2(C)	Inferential (blind).....	6-26
6.4.2(D)	Out-of-band.....	6-27
6.4.3	Preventing SQLi.....	6-28
6.5	Malware (or Malicious Code).....	6-30
6.5.1	Concept Building-Activities related to Malware.....	6-30
6.5.2	Types of Malware.....	6-30
6.5.2(A)	Virus and Worms	6-32
6.5.3	General Guidelines for Preventing Malware	6-36
