

**77UNIT I****Chapter 1 : Security Basics 1-1 to 1-30**

**Syllabus :** Introduction, Elements of Information Security, Security Policy, Techniques, Steps, Categories, Operational Model of Network Security, Basic Terminologies in Network Security. Threats and Vulnerability, Difference between Security and Privacy.

1.1	Concept Building – Security – What is it really?.....	1-1
1.2	Elements of Information Security.....	1-3
1.3	Basic Terminologies in Network Security (OSI Model).	1-7
1.3.1	The OSI Security Architecture .....	1-8
1.3.2	Categories of Security Services.....	1-9
1.4	Security Techniques / Steps / Mechanisms .....	1-9
1.4.1	Placement of Security Services and Mechanisms .....	1-10
1.5	Operational Model of Network Security (Network Security Model) .....	1-11
1.6	Security Threats and Vulnerabilities .....	1-13
1.6.1	Security Threats .....	1-13
1.6.1(A)	Comparison between Security Threats .....	1-15
1.6.2	Security Vulnerabilities .....	1-15
1.6.3	STRIDE Model .....	1-16
1.7	Security Attacks .....	1-17
1.7.1	Active Attacks.....	1-18
1.7.2	Passive Attacks.....	1-20
1.7.3	Comparison between Active and Passive Attacks .....	1-21
1.8	Security Policy.....	1-21
1.8.1	Characteristics of Policies .....	1-22
1.8.2	Types of Policies .....	1-22
1.8.3	Policy Implementation .....	1-27

**UNIT II****Chapter 2 : Data Encryption Techniques and Standards 2-1 to 2-46**

**Syllabus :** Introduction, Encryption Methods: Symmetric, Asymmetric, Cryptography, Substitution Ciphers. Transposition Ciphers, Stenography applications and limitations, Block Ciphers and methods of operations, Feistel Cipher, Data Encryption Standard (DES), Triple DES, DES Design Criteria, Weak Keys in DES Algorithms, Advance Encryption Standard (AES).

2.1	Concept Building – Information Secrecy .....	2-1
2.2	Introduction to Cryptography .....	2-2
2.3	Classical Encryption Techniques.....	2-4
2.3.1	Substitution .....	2-4
2.3.1(A)	Difference between Monoalphabetic and Polyalphabetic Ciphers.....	2-22
2.3.2	Transposition.....	2-22
2.4	Rotor Machines .....	2-25
2.5	Steganography .....	2-26
2.6	Methods of Encryption.....	2-27
2.6.1	Symmetric Key Encryption .....	2-27
2.6.2	Asymmetric Key Encryption.....	2-28
2.6.3	Comparison between Symmetric and Asymmetric Keys... ..	2-31
2.7	Types of Symmetric Algorithms (Ciphers) .....	2-31
2.7.1	Block Ciphers .....	2-31
2.7.2	Stream Ciphers .....	2-32
2.7.3	Comparison between Block and Stream Cipher .....	2-33
2.8	Data Encryption Standard (DES).....	2-33
2.8.1	Block Cipher Design Principles (DES Design Criteria).....	2-33
2.8.2	Block Diagram and Internals of DES .....	2-34
2.8.3	Block Cipher – Modes of Operation (for DES and other Block Ciphers in General).....	2-36
2.8.4	Comparison between Modes of Operation.....	2-38
2.8.5	Weakness in DES .....	2-39
2.8.6	Double DES .....	2-39



2.8.7	3DES or Triple DES .....	2-40
2.9	Advanced Encryption Standard (AES).....	2-41
2.9.1	Block Diagram and Internals of AES .....	2-41
2.9.2	Comparison between DES and AES .....	2-43
2.10	Attacks on Cryptosystems.....	2-43
2.10.1	Comparison between Differential and Linear Cryptanalysis.....	2-44

**UNIT III****Chapter 3 : Public Key and Management 3-1 to 3-55**

**Syllabus** : Public Key Cryptography, RSA Algorithm: Working, Key length, Security, Key Distribution, Diffie-Hellman Key Exchange, Elliptic Curve: Arithmetic, Cryptography, Security, Authentication methods, Message Digest, Kerberos, X.509 Authentication service. Digital Signatures: Implementation, Algorithms, Standards (DSS), Authentication Protocol.

3.1	Modular Arithmetic .....	3-1
3.1.1	Congruence Property .....	3-2
3.2	Arithmetic in Cryptography .....	3-3
3.2.1	Euclid's or Euclidean Algorithm .....	3-4
3.2.2	Extended Euclidean Algorithm.....	3-5
3.2.3	Multiplicative Inverse using extended Euclidean Algorithm .....	3-10
3.2.4	Chinese Remainder Theorem.....	3-13
3.2.5	Fermat's Theorem .....	3-18
3.2.6	Euler's theorem .....	3-19
3.3	Public Key Cryptography .....	3-20
3.3.1	Principles of Public Key Cryptosystems.....	3-20
3.4	RSA.....	3-21
3.4.1	Attacks on RSA.....	3-24
3.5	Diffie-Hellman Key Exchange Algorithm .....	3-24
3.6	Elliptic Curve Arithmetic and Cryptography.....	3-27
3.6.1	How does it work? .....	3-28
3.7	ElGamal Curve Arithmetic and Cryptography .....	3-29
3.8	Concept Building – Information Accuracy .....	3-31
3.9	Message Authentication Methods (Functions) .....	3-32
3.9.1	Cryptographic Hash Functions .....	3-32

3.10	MAC (Message Authentication Code).....	3-39
3.11	Digital Signature .....	3-43
3.11.1	How does this work? .....	3-43
3.11.2	Properties of Digital Signature .....	3-44
3.11.3	X.509 Certificate.....	3-45
3.11.4	Digital Signature Schemes .....	3-46
3.11.5	Digital Signature Standard (DSS) .....	3-48
3.11.6	Digital Signature Algorithm (DSA) .....	3-48
3.12	Kerberos.....	3-49
3.13	Needham Schroeder Authentication Protocol.....	3-51
3.13.1	The Needham–Schroeder Symmetric Key Based Authentication Protocol .....	3-51
3.13.2	The Needham–Schroeder Asymmetric Key Based Authentication Protocol .....	3-52

**UNIT IV****Chapter 4 : Security Requirements 4-1 to 4-29**

**Syllabus** : IP Security: Introduction, Architecture, IPV6, IPV4, IPSec protocols, and Operations, AH Protocol, ESP Protocol, ISAKMP Protocol, Oakkey determination Protocol, VPN. WEB Security: Introduction, Secure Socket Layer (SSL), SSL Session and Connection, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, Handshake Protocol. Electronic Mail Security: Introduction, Pretty Good Privacy, MIME, S/MIME, Comparison. Secure Electronic Transaction (SET).

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) .....	4-3
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	VPN.....	4-10



4.2.1	Types of VPN.....	4-10
4.2.2	Challenges of using VPN.....	4-11
4.3	Web Security.....	4-12
4.4	Secure Socket Layer (SSL).....	4-12
4.4.1	Overview of SSL Protocol.....	4-13
4.4.1(A)	Session and Connection States.....	4-13
4.4.1(B)	SSL Record Layer Protocol.....	4-14
4.4.1(C)	SSL Change Cipher Spec Protocol.....	4-16
4.4.1(D)	SSL Alert Protocol.....	4-16
4.4.1(E)	SSL Handshake Protocols.....	4-17
4.4.2	Transport Layer Security (TLS).....	4-18
4.5	HTTPS.....	4-18
4.5.1	Comparison between HTTP and HTTPS.....	4-19
4.5.2	Motivation / Benefits of using HTTPS.....	4-19
4.5.3	Format, Port Number and Representation.....	4-20
4.6	Secure Electronic Transactions (SET).....	4-21
4.7	Email Security.....	4-22
4.7.1	Pretty Good Privacy (PGP).....	4-22
4.7.1(A)	Web of Trust.....	4-22
4.7.1(B)	PGP Services.....	4-23
4.7.1(C)	PGP Algorithms.....	4-25
4.7.2	MIME.....	4-26
4.7.3	S/MIME.....	4-26
4.7.3(A)	S/MIME Services.....	4-26
4.7.3(B)	S/MIME Algorithms.....	4-26
4.7.3(C)	S/MIME Cryptographic Message Syntax (CMS).....	4-27
4.7.3(D)	Comparison between PGP and S/MIME.....	4-27

**UNIT V****Chapter 5 : Firewall and Intrusion 5-1 to 5-59**

**Syllabus :** Introduction, Computer Intrusions. Firewall Introduction, Characteristics and types, Benefits and limitations. Firewall architecture, Trusted Systems, Access Control. Intrusion detection, IDS: Need, Methods, Types of IDS, Password Management, Limitations and Challenges.

5.1	Firewalls.....	5-1
5.1.1	Classification of Firewalls.....	5-2
5.1.2	Challenges in Managing and Deploying Firewalls.....	5-5
5.2	Computer Intrusions and Intrusion Detection Systems (IDS).....	5-6
5.2.1	Introduction.....	5-6
5.2.2	Need for IDS.....	5-6
5.2.3	Types of IDS.....	5-7
5.2.4	Limitations and Challenges of IDS.....	5-8
5.3	Access Control.....	5-8
5.4	Trusted Systems.....	5-17
5.4.1	Bell-LaPadula (BLP) Model.....	5-17
5.4.2	Biba Model.....	5-21
5.5	Authentication Methods.....	5-25
5.5.1	Introductory Concepts.....	5-26
5.5.2	Types of Authentication Methods.....	5-27
5.5.3	Comparison between the Authentication Types.....	5-32
5.5.4	Factors of Authentication.....	5-32
5.5.5	Password Based Authentication.....	5-33
5.5.6	Password Selection Criteria (Quality Guidelines).....	5-37
5.5.7	Storing Passwords on System.....	5-37
5.5.8	Attacks, Limitations and Challenges on Password Based Authentication.....	5-39
5.5.9	Token Based Authentication.....	5-46



5.5.10	Biometric Based Authentication.....	5-52
5.5.10(A)	Components of Biometric Systems .....	5-52
5.5.10(B)	Operating Biometric Systems .....	5-52
5.5.10(C)	Accuracy of Biometric Systems .....	5-54
5.5.10(D)	Types of Biometric Systems .....	5-55

### UNIT VI

#### Chapter 6 : Confidentiality and Cyber Forensic

**6-1 to 6-46**

**Syllabus :** Introduction to Personally Identifiable Information (PII), Cyber Stalking, PII impact levels with examples Cyber Stalking, Cybercrime, PII Confidentiality Safeguards, Information Protection Law: Indian Perspective.

6.1	Privacy on Web .....	6-1
6.2	Introduction to Personally Identifiable Information (PII).....	6-1
6.2.1	Privacy Principles .....	6-2
6.3	Concept Building - Privacy Risks on the Web.....	6-4
6.4	PII Impact Levels.....	6-12
6.5	PII Confidentiality Safeguards .....	6-14

6.5.1	Difference between Security and Privacy .....	6-23
6.6	Concept Building - Privacy Laws Around the World.....	6-23
6.7	Cybercrime.....	6-25
6.7.1	Introduction, Definition and Origin .....	6-25
6.7.2	Cybercrime and Information Security.....	6-26
6.7.3	Categories of Cybercrimes .....	6-28
6.7.4	Classification of Cybercrimes .....	6-29
6.7.5	The Legal Perspectives of Cybercrimes .....	6-30
6.7.5(A)	The Indian Perspective.....	6-31
6.7.5(B)	The Global Perspective .....	6-37
6.8	Cyberstalking .....	6-41
6.8.1	Cyberstalking Harassments.....	6-41
6.8.2	Types of Stalkers .....	6-42
6.8.3	How cyberstalking works ? .....	6-42
6.8.4	How to safeguard yourself from stalking ? .....	6-43
6.8.5	Provisions in the Indian Jurisdiction for Stalking .....	6-44
6.9	Phases of Cyber Forensics .....	6-44



Technical Publications