

**UNIT I**

**Chapter 1 : Introduction to Computer & Information Security**

**1-1 to 1-33**

**Syllabus : Foundations of Computer Security :** Definition and Need of computer security, Security Basics: Confidentiality, Integrity, Availability, Accountability, Non - Repudiation and Reliability. **Risk and Threat Analysis :** Assets, Vulnerability, Threats, Risks, Counter measures. **Threat to Security :** Viruses, Phases of Viruses, Types of Virus, Dealing with Viruses, Worms, Trojan Horse, Intruders, Insiders. **Type of Attacks :** Active and Passive attacks, Denial of Service, DDOS, Backdoors and Trapdoors, Sniffing, Spoofing, Man in the Middle, Replay, TCP/IP Hacking, Encryption attacks. **Operating system security :** Operating system updates HotFix, Patch, Service Pack. Information, Need and Importance of Information, information classification, criteria for information classification, Security, need of security, Basics principles of information security.

1.1	Foundation of Computer Security .....	1-1
1.1.1	Definition of Security .....	1-1
1.1.2	Need of Security.....	1-2
1.1.3	Security Basics.....	1-2
1.2	Risk and Threat Analysis .....	1-4
1.2.1	Assets .....	1-4
1.2.2	Vulnerability .....	1-5
1.2.3	Threats.....	1-5
1.2.4	Risks .....	1-6
1.2.5	Countermeasures.....	1-7
1.3	Threat to Security .....	1-8
1.3.1	Viruses.....	1-8
1.3.2	Phases of Viruses (Life Cycle of Viruses).....	1-9
1.3.3	Types of Viruses .....	1-9
1.3.4	Dealing with Viruses.....	1-10
1.3.5	Worms .....	1-10
1.3.6	Trojan Horse .....	1-12
1.3.7	Intruders.....	1-12
1.3.8	Insiders .....	1-13



.4	Type of Attacks.....	1-13
1.4.1	Active and Passive Attacks .....	1-14
1.4.2	Denial of Service (DOS) .....	1-15
1.4.3	Distributed Denial of Service (DDOS).....	1-16
1.4.4	Backdoors and Trapdoors .....	1-17
1.4.5	Sniffing.....	1-18
1.4.6	Spoofing.....	1-19
1.4.7	Man-in-Middle Attack (Bucket-Bridge Attack) .....	1-21
1.4.8	Replay.....	1-22
1.4.9	TCP/IP Hijacking.....	1-23
1.4.10	Encryption Attacks .....	1-23
1.5	Operating System Security .....	1-24
1.5.1	Operating System Updates .....	1-24
1.6	Information Security.....	1-26
1.6.1	Information.....	1-26
1.6.2	Need and Importance of Information .....	1-26
1.6.3	Information Classification .....	1-27
1.6.4	Criteria for Information Classification.....	1-28
1.6.5	Need of Security.....	1-30
1.6.6	Basics Principles of Information Security.....	1-31

## UNIT II

### Chapter 2 : Authentication & Access Control

2-1 to 2-15

**Syllabus :** **Identification and Authentication** : User name and Password, Guessing password, Password attacks- Piggybacking, Shoulder surfing, Dumpster diving. **Biometrics** : Finger Prints, Hand prints, Retina, patterns, Voice patterns, Signature and Writing patterns, Keystrokes. **Access controls** : Definition, Authentication Mechanism, principle-Authentication, Authorization, Audit, Policies : DAC, MAC, RBAC.

2.1	Identification and Authentication .....	2-1
2.1.1	User Name and Password.....	2-1
2.1.2	Password Attacks.....	2-3



2.2	Biometrics .....	2-5
2.2.1	Types of Biometric .....	2-6
2.2.1(A)	Fingerprint.....	2-6
2.2.1(B)	Hand Print.....	2-6
2.2.1(C)	Retina .....	2-7
2.2.1(D)	Voice/Speech Patterns.....	2-7
2.2.1(E)	Signature and Writing Patterns.....	2-7
2.2.1(F)	Keystrokes .....	2-8
2.3	Access Control .....	2-8
2.3.1	Definition.....	2-9
2.3.2	Authentication Mechanism .....	2-9
2.3.3	Authentication and Authorization.....	2-10
2.3.4	Principle.....	2-10
2.3.5	Audit.....	2-13
2.3.6	Policies - DAC, MAC, RBAC .....	2-13

<b>UNIT III</b>
-----------------

**Chapter 3 : Cryptography****3-1 to 3-18**

<p><b>Syllabus</b> : Introduction: Plain Text, Cipher Text, Cryptography, Cryptanalysis, Cryptology, Encryption, Decryption. Substitution Techniques : Caesar's cipher, Modified Caesar's Cipher, Transposition Techniques : Simple Columnar Transposition. Steganography : Procedure. Symmetric and Asymmetric cryptography: Introduction to Symmetric encryption, DES (Data encryption Standard) algorithm, Asymmetric key cryptography: Digital Signature.</p>
---

3.1	Introduction.....	3-1
3.1.1	Plaintext .....	3-1
3.1.2	Ciphertext.....	3-1
3.1.3	Cryptography .....	3-2
3.1.4	Cryptanalysis .....	3-2
3.1.5	Cryptology.....	3-3
3.1.6	Encryption.....	3-3
3.1.7	Decryption.....	3-3



3.2	Substitution and Transposition Technique .....	3-4
3.2.1	Substitution Technique .....	3-4
3.2.2	Transposition Technique .....	3-6
3.2.3	Comparison of Substitution Cipher and Transposition Cipher .....	3-8
3.3	Steganography – Procedure .....	3-8
3.4	Symmetric and Asymmetric Cryptography .....	3-9
3.4.1	Introduction to Symmetric Encryption .....	3-10
3.4.2	Asymmetric Key Cryptography .....	3-14
3.4.3	Comparison of Symmetric Key Cryptography and Asymmetric Key Cryptography .....	3-18

<b>UNIT IV</b>
----------------

**Chapter 4 : Firewall & Intrusion Detection System****4-1 to 4-16**

<p><b>Syllabus :</b> Firewall Need of Firewall, types of firewall- Packet Filters, Stateful Packet Filters, Application Gateways, Circuit gateways. Firewall Policies, Configuration, limitations, DMZ. Intrusion Detection System Vulnerability Assessment, Misuse detection, Anomaly Detection, Network- Based IDS, Host-Based IDS, Honeypots</p>
---

4.1	Firewall.....	4-1
4.1.1	Need of Firewall .....	4-1
4.1.2	Type of Firewall.....	4-2
4.2	Firewall Policies, Configuration, Limitation DMZ .....	4-5
4.2.1	Firewall Policies .....	4-5
4.2.2	Configuration.....	4-6
4.2.3	Limitations of Firewalls .....	4-8
4.2.4	DMZ (Demilitarized Zone) .....	4-8
4.3	Intrusion Detection System (IDS).....	4-9
4.3.1	What is IDS? .....	4-9
4.3.2	Vulnerability Assessment .....	4-11
4.3.3	Misuse Detection.....	4-11
4.3.4	Anomaly Detection .....	4-11
4.3.5	Host-Based IDS .....	4-12
4.3.6	Network Based IDS.....	4-13
4.3.7	Honeypots.....	4-14

**UNIT V**

**Chapter 5 : Network Security, Cyber Laws & Standards**

**5-1 to 5-42**

**Syllabus :** Kerberos: Working, AS, TGS, SS. IP Security- Overview, Protocols- AH, ESP, Modes- transport and Tunnel. Email security- SMTP, PEM, PGP. Public key infrastructure (PKI): Introduction, Certificates, Certificate authority, Registration Authority, X.509/PKIX certificate format. Cyber Crime : Introduction, Hacking , Digital Forgery, Cyber Stalking/Harassment, Cyber Pornography, Identify Theft and Fraud, Cyber terrorism, Cyber Defamation. Cyber Laws : Introduction need, Categories : Crime against Individual, Government, Property. Compliance standards : Implementing and Information Security Management System, ISO 27001, ISO 20000, BS 25999, PCI DSS, ITIL framework, COBIT framework.

5.1	Kerberos.....	5-1
5.1.1	AS, TGS, SS .....	5-2
5.1.2	Working.....	5-2
5.2	IP Security.....	5-5
5.2.1	Overview .....	5-5
5.2.2	Modes - Transport and Tunnel .....	5-6
5.2.3	Protocols - AH and ESP .....	5-7
5.3	Email Security .....	5-9
5.3.1	Simple Mail Transfer Protocol (SMTP) .....	5-10
5.3.2	Privacy Enhanced Mail (PEM).....	5-11
5.3.3	Pretty Good Privacy (PGP).....	5-14
5.4	Public Key Infrastructure (PKI).....	5-15
5.4.1	Introduction .....	5-15
5.4.2	Certificates .....	5-16
5.4.3	Certificate Authority (CA).....	5-18
5.4.4	Registration Authority (RA).....	5-19
5.4.5	X.509/PKIX Certificate Format.....	5-19
5.5	Cyber Crime .....	5-20
5.5.1	Introduction .....	5-20
5.5.2	Hacking.....	5-21
5.5.3	Digital Forgery.....	5-23
5.5.4	Cyberstalking or Harassment .....	5-23



---

5.5.5	Cyber Pornography .....	5-23
5.5.6	Identity Theft and Fraud .....	5-24
5.5.7	Cyber Terrorism .....	5-24
5.5.8	Cyber Defamation .....	5-24
5.6	Cyber Laws .....	5-25
5.6.1	Introduction and Need .....	5-25
5.6.2	Categories.....	5-26
5.7	Compliance Standards .....	5-26
5.7.1	Implementing and Information Security Management System (ISMS) .....	5-27
5.7.2	ISO 27001 .....	5-28
5.7.3	ISO 20000 .....	5-29
5.7.4	BS 25999 .....	5-31
5.7.5	PCI DSS .....	5-32
5.7.6	ITIL Framework .....	5-33
5.7.7	COBIT Framework .....	5-36
	• Time Management Sheet	
	• Model Question Papers .....	Q-1 to Q-6

