

UNIT - I

➤ Chapter 1 : Introduction		1-1 to 1-20
1.1	Computer Security.....	1-1
	1.1.1 Introduction to Computer Security.....	1-1
	1.1.2 Need of Security.....	1-1
✓	Syllabus Topic : Security Trends	1-2
1.2	Security Trends	1-2
	1.2.1 Information Security Trends	1-2
	1.2.2 Network Security Trends	1-5
	1.2.3 Network Security Trends that could happen in the Coming Year	1-6
✓	Syllabus Topic : The OSI Security Architecture	1-10
1.3	The OSI Security Architecture.....	1-10
	1.3.1 Security Architecture for OSI	1-10
✓	Syllabus Topic : Security Attacks	1-11
1.4	Types of Security Attacks	1-11
	1.4.1 Passive Attacks.....	1-11
	1.4.2 Active Attacks	1-12
✓	Syllabus Topic : Security Services	1-15
1.5	Security Services	1-15
	1.5.1 Authentication	1-15
	1.5.2 Access Control	1-16
	1.5.3 Confidentiality.....	1-16
	1.5.4 Data Integrity	1-17
	1.5.5 Non-repudiation	1-18
	1.5.6 Availability.....	1-18
✓	Syllabus Topic : Security Mechanisms	1-19
1.6	Security Mechanisms	1-19
➤ Chapter 2 : Classical Encryption Techniques		2-1 to 2-21
2.1	Cryptography.....	2-1
	2.1.1 Advantages of Cryptography	2-2
✓	Syllabus Topic : Symmetric Cipher Model	2-2
2.2	Symmetric Cipher Model	2-2
2.3	Cryptanalysis	2-3
	2.3.1 Symmetric Cryptography / Private Key Encryption (PrKE)	2-5
✓	Syllabus Topic : Substitution Techniques	2-7
2.4	Substitution Techniques	2-7
	2.4.1 Caesar Cipher Substitution.....	2-7

2.4.2	Mono-alphabetic Substitution	2-8
2.4.3	Playfair Cipher	2-9
2.4.4	Hill Cipher (Polygram)	2-13
2.4.5	Vigenere Cipher (Poly-alphabetic)	2-15
2.4.6	One-Time Pad	2-18
✓	Syllabus Topic : Transposition Techniques	2-19
2.5	Transposition Techniques	2-19
✓	Syllabus Topic : Steganography	2-20
2.6	Steganography	2-20
2.6.1	Difference between Cryptography and Stenography	2-20

➤ Chapter 3 : Block Cipher and DES	3-1 to 3-27
---	--------------------

✓	Syllabus Topic : Block Cipher Principles	3-1
3.1	Block Cipher Principles	3-1
3.1.1	Need for Feistel cipher	3-3
3.1.2	Feistel Block Cipher	3-3
3.1.3	Encryption Process	3-3
3.1.4	Decryption Process	3-5
3.1.5	Number of Rounds	3-5
3.1.6	Diffusion and Confusion	3-5
✓	Syllabus Topics : Data Encryption Standard	3-6
3.2	Data Encryption Standard	3-6
✓	Syllabus Topic : The Strength of DES	3-6
3.2.1	Description of DES	3-6
3.2.2	Example of DES Encryption	3-7
✓	Syllabus Topic : The Strength of AES	3-16
3.3	AES	3-16
3.3.1	AES Encryption Process	3-17
✓	Syllabus Topic : Multiple Encryption and Triple DES	3-18
3.4	Multiple Encryption and Triple DES	3-18
3.4.1	Multiple DES	3-18
✓	Syllabus Topic : Block Cipher Modes of Operation	3-21
3.5	Block cipher modes of operation	3-21
✓	Syllabus Topic : Stream Ciphers	3-26
3.6	Stream Ciphers	3-26

➤ Chapter 4 : Public Key Cryptography and RSA	4-1 to 4-9
--	-------------------

4.1	Asymmetric Cryptography / Public Key Encryption (PuKE)	4-1
4.1.1	Advantages of Public-key (Asymmetric) Cryptography over Private-key (Symmetric) Cryptography	4-3