DATA SECURITY

Credits: 4 **Semester:VI**
Subject Code: DS18601A **No. of Lecture Hours:60**

Objectives
• Understanding the significance of privacy, ethics in data environment.
• Analysing the steps to secure data.

Outcomes: Students will be able to
CO1: Identify some of the factors driving the need for data security
CO2: Examine and classify particular examples of attacks
CO3: Classify the terms vulnerability, threat and attack
CO4: Analyse physical points of vulnerability in simple networks
CO5: Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack, and explain the characteristics of hybrid systems.

UNIT – I
12hrs
Attacks on Computers and Computer Security:
1. Introduction, The Need for Security, Security Approaches, Principles of Security, Types of Security Attacks
2
2. Security Services, Plain Text and Cipher Text, Stream Ciphers, Block Ciphers 2
3. Security Mechanisms, A Model for Network Security
2
Cryptography:
4. Encryption and Decryption, Substitution Ciphers, Ceaser Cipher, Mono-Alphabetic Cipher, Play-Fair Cipher, Hill Cipher, Poly-Alphabetic Cipher, Transposition Techniques, One-Time Pads
5. Introduction to Symmetric and Asymmetric Key Cryptography and
2
Its Applications
2
6. Cryptanalysis, Types of Keys, Key Range and Key Size, Possible Types of Attacks
2

UNIT – II
12hrs
Symmetric Key Cryptography:
1. Block Cipher Principles, Symmetric Encryption Principles & Algorithms
2
2. DES Algorithm, Strength of DES, Triple DES
2

3. AES Algorithm, Overview of AES, Iterations in AES
2
4. Stream ciphers, RC4 Algorithm
2
5. Block cipher modes of operation, Electronic Code Book Mode (ECB), Cipher Block Chaining Mode (CBC), Cipher Feedback Mode (CFB), Counters Mode (CTR)
2 **Asymmetric key Cryptography**:
6. Principles of Public Key Cryptography, RSA Algorithm
2

UNIT – III

12hrs

Intruders, Virus and Firewalls:

1. Introduction to Intruders, Intrusion Detection Systems
2
2. Password Management, Password Protection, Password Selection Strategies
2
3. Viruses, Threats, Worms, Nature of Viruses, Types of Viruses, Malicious Program 2
4. Virus Counter Measures, Anti-Virus Approaches, Generic Decryption, Digital Immune System, Behavior-Blocking Software
2
5. Firewall Design Principles, Firewall Characteristics, Types of Firewalls, Firewall Configurations.
2
6. Trusted Systems, Data Access Control, Concept of Trusted Systems
2
Trojan Horse Defense

UNIT-IV

12hrs

Information Hiding:

1. Introduction to Information Hiding, Steganography, and Watermarking
2
2. Importance of Digital Watermarking, Importance of Steganography
3
3. Applications of Watermarking, Applications of Steganography
2
4. Properties of Watermarking Systems, Evaluating Watermarking Systems
3
5. Properties of Steganography and Steganalysis Systems. Evaluating and Testing Steganographic Systems
2
6. Robust Watermarking, Approaches, Robustness to Volumetric Distortions
2

UNIT – V

12hrs

Case Studies on Cryptography and Security:

1. Secure Inter-branch Payment Transactions
2
2. Cross site Scripting Vulnerability
2
3. Virtual Elections
2
4. Common Criteria for Information Technology Security Evaluation
2

Biometrics:

5. Components, Enrollment, Authentication, Techniques, Accuracy, Applications 2
6. Internet Standards, Internet Society, Internet Organizations, Internet Standard Categories, RFCs
2