# GUJARAT TECHNOGICAL UNIVERSITY
## DIPLOMA IN INFORMATION TECHNOLOGY

### SEMESTER- VI

Subject Name: **INFORMATION SECURITY**

| Sr. No. | Subject Content | Hrs. |
|---|---|---|
| 1 | **1.0 INTRODUCTION TO INFORMATION SECURITY**<br><br>1.1 What Is Information Security?<br>1.2 Overview of information Security<br>1.3 Security Services, Mechanisms and Attacks<br>1.4 The OSI Security Architecture<br>1.5 A Model for Network Security | 4 |
| 2 | **2.0 SYSTEM SECURITY**<br><br>2.1 Intruders<br><br>2.1.1 Intruders<br>2.1.2 Intruders detection<br>2.1.3 Password management.<br><br>2.2 Malicious Software<br><br>2.2.1 Viruses and Related Threats<br>2.2.2 Virus Countermeasures<br><br>2.3 Firewalls<br><br>2.3.1 Firewalls Design principle<br>2.3.2 Trusted Systems | 8 |
| 3 | **3.0 SYMMETRIC KEY CRYPTOGRAPHY**<br><br>3.1 Symmetric Cipher Model<br>3.2 Cryptography, Cryptanalysis | 4 |

| | | |
|---|---|---|
| 4 | **4.0 SUBSTITUTION TECHNIQUES**<br><br>4.1 Creaser Cipher, Monoalphabetic Ciphers, Playfair Cipher<br>4.2 One Time Pad, Transposition Techniques , Stegnography | 4 |
| 5 | **5.0 BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD**<br>5.1 Simplified DES , Block Cipher Principles<br>5.2 The Data Encryption Standard , The Strength of DES<br>5.3 Block Cipher Modes of Operation | 6 |
| 6 | **6.0 CONFIDENTIALITY USING SYMMETRIC ENCRYPTION**<br>6.1 Placement of Encryption Function<br>6.2 Traffic Confidentiality<br>6.3 Key Distribution<br>6.4 Random Number Generation | 6 |
| 7 | **7.0 PUBLIC-KEY CRYPTOGRAPHY AND RSA**<br><br>7.1 Principles of Public-key Cryptosystems<br>7.2 RSA<br>7.3 Key Management in public-key cryptosystem<br>7.4 Diffie-Hellman Key Exchange | 6 |
| 8 | **8.0 Digital Signature and Authentication Protocols**<br><br>8.1 Digital Signatures<br>8.2 Authentication Protocols<br>8.3 Digital Signature Standard | 4 |
| | Total | 42 |

## Laboratory Experiences:

1. Write a ‘c’program to Encrypt the plaintext and display the cipher text using Ceaser Cipher.
2. Write a ‘c’program to Decrypt the cipher text and display the plain text using Ceaser Cipher.
3. Write a ‘c’program to Encrypt the plaintext and display the cipher text using Monoalphabetic Substitution Cipher.
4. Write a ‘c’program to Decrypt the cipher text and display the plain text using Monoalphabetic Substitution Cipher.
5. Write a ‘c’program to Encrypt the plaintext and display the cipher text using playfair Cipher.
6. Write a ‘c’program to Decrypt the cipher text and display the plain text using playfair Cipher.
7. Write a ‘c’program to Encrypt the plaintext and display the cipher text using Vigenere Cipher.
8. Write a ‘c’program to Decrypt the cipher text and display the plain text using Vigenere Cipher.
9. Write a ‘c’program to Encrypt the plaintext and display the cipher text using Autokey Vigenere Cipher.
10. Write a ‘c’program to Decrypt the cipher text and display the plain text using Autokey Vigenere Cipher.
11. Write a ‘c’program to Encrypt the plaintext and display the cipher text using Columnar Transposition Cipher.
12. Write a ‘c’program to Decrypt the cipher text and display the plain text using Columnar Transposition Cipher.

## Text Book :

(1) Cryptography and Network Security By William Stallings(Pearson Education)

## Reference Books:

(1) Computer Security Basics By Debby Russell, G.T. Gangemi, Sr.(Oreilly)
(2) Network Security private communication in a PUBLIC world By Charlie Kaufman, Radia Perlman , Mike Speciner
(3) Security in Computing, Charless P. Pfleeger, Shari Lawrence Pfleeger.
(4) Enterprise Security, Robert C. Newman(Pearson Education)