**PARVATHANENI BRAHMAYYA SIDDHARTHA COLLEGE OF ARTS & SCIENCE**
***Autonomous***
**Siddhartha Nagar, Vijayawada-520010**
***Re-accredited at 'A+'by the NAAC***

**Offered to: M.Sc. (Computer Science)**

# 22CS4E6: INFORMATION SECURITY

| **CourseName** | Information Security | **L** | **T** | **P** | **C** | **CIA** | **SEE** | **TM** |
|---|---|---|---|---|---|---|---|---|
| **CourseCode** | 22CS4E6 | 4 | 0 | 0 | 4 | 30 | 70 | 100 |
| **Year of Introduction:** 2023 | **Year of Offering:** 2023 | **Year of Revision**: Nil | | **Percentage of Revision:** Nil | | | | |
| **L**-Lecture, T-Tutorial, **P**-Practical, **C**-Credits, **CIA**-InternalMarks, **SEE**-ExternalMarks, **TM**-TotalMarks | | | | | | | | |

**Course Description and Purpose:** The course is intended to understand and gain knowledge on Computer& Network Security, Conventional cryptography Techniques, Digital Signatures, Key Management and Distribution and User Authentication and IP Security and Intruders and Firewalls.

**Course Objective:** The course aims to provide a comprehensive understanding of computer and network security, covering cryptography related symmetric and asymmetric techniques, digital signatures, key management, user authentication to secure digital communication and defend against cyber threats.

**Course Outcomes:**
**CO1:** Recall Information Security, Conventional, Symmetric and Asymmetric Cryptography.
**CO2:** Infer Authentication and Digital Signatures and Program Security
**CO3:**Illustrate Kerberos, Vulnerability, Errors and Viruses.
**CO4:** Evaluate program security, Honeypots, Personal Firewalls and IDS.
**CO5:** Identify Security in Networks, Design and Types of Firewalls and Secure Hash function.

| **CO-PO MATRIX** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **COURSE CODE** | **CO-PO** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** |
| | **CO1** | H | | | | H | |
| | **CO2** | H | | H | | | |
| | **CO3** | M | L | | | | |
| | **CO4** | H | | H | | | |
| | **CO5** | H | | | | H | |

## UNIT-I (12 Hours)

**Introduction to Information Security:** Attacks, Vulnerability, Security Goals, Security Services and mechanisms
**Conventional Cryptographic Techniques:** Conventional substitution and transposition ciphers, One-time Pad

## UNIT-II (12 Hours)

**Conventional Cryptographic Techniques:** Blockcipher and Stream Cipher, Steganography

**Symmetric and Asymmetric Cryptographic Techniques:**DES, AES, RSA algorithm

**UNIT-III (12 Hours)**

**Authentication and Digital Signatures:** Use of Cryptographyfor authentication, Secure Hash function, Key management – Kerberos

**UNIT-IV (12 Hours)**

**Program Security:**Nonmalicious Program errors – Bufferoverflow, Incomplete mediation, Time-of-check to Time-of- use Errors, Viruses, Trapdoors, Salami attack, Man-in-the- middle attacks, Covert channels.

**UNIT-V (12 Hours)**

**Security in Networks:** Threats in networks, Network SecurityControls – Architecture, Encryption, Content Integrity, StrongAuthentication, Access Controls, Wireless Security,Honeypots, Traffic flow security, Firewalls – Design andTypes of Firewalls, Personal Firewalls, IDS, Email Security – PGP,S/MIME

| **ReferenceTextBooks** | | | |
|---|---|---|---|
| | Author | Title | Publisher |
| 1 | Charles P. Pfleeger | Security in Computing | Fourth Edition, Pearson Education |
| 2 | WilliamStallings | Cryptography And Network Security Principles And Practice | Pearson Education, Fourth Edition. |
| 3 | WilliamStallings | Cryptography And Network Security Principles And Practice | Pearson Education, FifthEdition. |
| 4 | Wenbo Mao | Modern Cryptography: Theory and Practice | Prentice Hall |
| 5 | William Stallings | Network Security Essentials: Applications and Standards | Prentice Hall |

**PARVATHANENI BRAHMAYYA SIDDHARTHA COLLEGE OF ARTS & SCIENCE**
***Autonomous***
**Siddhartha Nagar, Vijayawada-520010**
***Re-accredited at 'A+'by the NAAC***

**M.Sc. (Computer Science)** **Semester :IV**

**Course Code: 22CS4E6 Course Name: Information Security**

**Time: 3 Hours** **Max Marks: 70**

**SECTION-A**

**Answer the following questions. (5×4=20Marks)**

1. (a) Explain security Goals.(CO1,L2)

(or)

(b) Explain One Time Pad with an example. (CO1,L2)

2. (a) What is Steganography? Explain. (CO1,L1)

(or)

(b) Explain RSA Algorithm. (CO1,L1)

3. (a) What is Digital Signatures? (CO2,L1)

(or)

(b) Listsecure hash function. (CO5,L1)

4. (a) Explain Trapdoors. (CO4,L2)

(or)

(b) Explain Time-of-check to Time-of- use Errors,. (CO3,L2)

5. (a) Explain Access Controls. (CO2,L2)

(or)

(b) Explain Firewall Characteristics? (CO4,L2)

**SECTION-B**

**Answer the following questions. (5×10=50Marks)**

6. (a) Explain various Security Attacks and Security Services. (CO1,L2)

(or)

(b) Explain Substitution Techniques. (CO1,L2)

7. (a) Illustrate Block Ciphers. (CO1,L2)

(or)

(b) Explain AES Algorithm. (CO1,L2)

8. (a) Explain Key Management. (CO2,L5)

(or)

(b) Explain Kerberos in detail. (CO3,L5)

9. (a) ExplainBuffer Overflow (CO2,L5)

(or)

(b) Illustrate Man-in-the- middle attacks. (CO5,L5)

10. (a) Discuss Honeypots. (CO4,L6)

(or)

(b) Discuss Various Types of Firewalls. (CO5,L6)