SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY 

| Department of Information Technology | LP: IT22609<br>Rev. No: 00<br>Date: 20/01/2025 |
|---|---|
| ~~B.E~~/B.Tech/~~M.E/M.Tech~~ : Information Technology Regulation: R2022<br>PG Specialisation : NA<br>Sub. Code / Sub. Name : IT22609 / Information Security : Theory And Practices<br>Unit : I | |

**Unit Syllabus: INTRODUCTION TO SECURITY AND CRYPTOGRAPHY**

Overview of Security Parameters: Confidentiality, integrity and availability; Security violation and threats; Security policy and procedure; Assumptions and Trust; Security Assurance, Implementation and Operational Issues; Security Life Cycle. Foundations of Cryptography- Classical Encryption Techniques-Substitution Ciphers -Transposition ciphers - Crypt analysis.

**Suggested Activity:** Implement the following SUBSTITUTION & TRANSPOSITION TECHNIQUES concepts: a) Caesar Cipher b) Playfair Cipher c) Hill Cipher d) Vigenere Cipher e) Rail fence – row & Column Transformation

**Objective: To study and practice fundamental techniques in developing secure applications**

| Session No * | Topics to be covered | Ref | Teaching Aids |
|---|---|---|---|
| 1 | Overview of Security Parameters: Confidentiality, integrity and availability | 2–Ch.1; Pg.3-6 | BB/ PPT |
| 2 | Security violation and threats, Security policy and procedure | 2–Ch.1; Pg.6-11 | BB/ PPT |
| 3 | Assumptions and Trust, Security Assurance, Implementation and Operational Issues | 2–Ch.1; Pg.11-20 | BB/ PPT |
| 4 | Security Life Cycle | 3-Ch.1; Pg.25-37 | BB/ PPT |
| 5 | Foundations of Cryptography- Classical Encryption Techniques-Substitution Ciphers | 1-Ch.3; Pg.85-106<br>2-Ch.10; Pg.292-299 | BB/ PPT |
| 6 | Transposition ciphers - Cryptanalysis. | 1-Ch.3; Pg.107-117<br>2-Ch.10; Pg.290-292 | BB/ PPT |
| 7,8 | Implement SUBSTITUTION Techniques<br>a) Caesar Cipher, b) Playfair Cipher | 1-Ch.3; Pg.85-106<br>2-Ch.10; Pg.292-299 | Experiential Learning |
| 9,10 | Implement SUBSTITUTION Techniques<br>c) Hill Cipher d) Vigenere Cipher | 1-Ch.3; Pg.85-106<br>2-Ch.10; Pg.292-299 | Experiential Learning |
| 11,12 | Implement TRANSPOSITION Techniques<br>e) Rail fence – row & Column Transformation | 1-Ch.3; Pg.107-117<br>2-Ch.10; Pg.290-292 | Experiential Learning |
| Content beyond syllabus covered (if any): Practice on problems related to Vignere Cipher, Hill cipher, Single columnar and double columnar Transposition techniques | | | |

*** Session duration: 50 minutes**

**Sub. Code / Sub. Name: IT22609 / Information Security : Theory And Practices**

**Unit : II**

**Unit Syllabus : SYMMETRIC AND ASYMMETRIC TECHNIQUES**

Block Ciphers and the Data Encryption Standard, Advanced Encryption Standard, Introduction to Number Theory - The Euclidean Algorithm - Greatest Common Divisor, Modular Arithmetic - Euclidean Algorithm Revisited - The Extended Euclidean Algorithm, Public Key Cryptography and RSA, Other Public Key Cryptosystems - Diffie-Hellman Key Exchange – Elgamal Cryptographic Systems – Elliptic Curve Cryptography.

**Suggested Activity:** Implement the following algorithms a) DES b) RSA Algorithm c) Diffiee-Hellman

**Objective: To Learn to implement the symmetric and asymmetric cryptographic algorithms**

| Session No * | Topics to be covered | Ref | Teaching Aids |
|---|---|---|---|
| 13 | Block Ciphers and the Data Encryption Standard | 1-Ch.4; Pg.118-140<br>2-Ch.10; Pg.299-302 | BB/ PPT |
| 14 | Advanced Encryption Standard | 1-Ch.6; Pg.171-206<br>2-Ch.10; Pg.303-306 | BB/ PPT |
| 15 | Introduction to Number Theory - The Euclidean Algorithm - Greatest Common Divisor, Modular Arithmetic - Euclidean Algorithm Revisited - The Extended Euclidean Algorithm | 1-Ch.2; Pg.46-61 | BB/ PPT |
| 16 | Public Key Cryptography and RSA | 1-Ch.9; Pg.283-312<br>2-Ch.10; Pg.306-312 | BB/ PPT |
| 17 | Other Public Key Cryptosystems - Diffie-Hellman Key Exchange | 1-Ch.10; Pg.313-318 | BB/ PPT |
| 18 | Elgamal Cryptographic Systems – Elliptic Curve Cryptography. | 1-Ch.10; Pg.318-333<br>2-Ch.10; Pg.307-314 | BB/ PPT |
| 19,20 | Implement DES | 1-Ch.4; Pg.118-140<br>2-Ch.10; Pg.299-302 | Experiential Learning |
| 21,22 | Implement RSA Algorithm | 1-Ch.9; Pg.283-312<br>2-Ch.10; Pg.306-312 | Experiential Learning |
| 23,24 | Implement Diffiee-Hellman | 1-Ch.10; Pg.313-318 | Experiential Learning |
| Content beyond syllabus covered (if any): Nil | | | |

*** Session duration: 50 mins**

SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY 

**Sub. Code / Sub. Name: IT22609 / Information Security : Theory And Practices**

**Unit : III**

**Unit Syllabus : DIGITAL SIGNATURE AND KEY MANAGEMENT**

Digital Signatures, Key Management - Session and Interchange Keys - Key Exchange - Symmetric Cryptographic Key Exchange – Kerberos - Public Key Cryptographic Key Exchange and Authentication - Key Generation - Storing and Revoking Key.

**Suggested Activity:** Implementation of Encryption and Decryption using Kelopatra tool. Implement of Authentication and Digital Signature using Kelopatra tool.

**Objective: To learn about secure coding practices.**

| Session No * | Topics to be covered | Ref | Teaching Aids |
|---|---|---|---|
| 25 | Digital Signatures | 2-Ch.10; Pg.318-323 | BB/ PPT |
| 26 | Key Management - Session and Interchange Keys - Key Exchange - Symmetric Cryptographic Key Exchange | 2-Ch.11; Pg.331-337 | BB/ PPT |
| 27 | Kerberos | 2-Ch.11; Pg.337-338 | BB/ PPT |
| 28 | Public Key Cryptographic Key Exchange and Authentication | 2-Ch.11; Pg.338-341 | BB/ PPT |
| 29 | Key Generation | 2-Ch.11; Pg.341-342 | BB/ PPT |
| 30 | Storing and Revoking Key | 2-Ch.11; Pg.353-359 | BB/ PPT |
| 31,32 | Implementation of Encryption and Decryption using Kelopatra tool | Internet | Experiential Learning |
| 33,34 | Implement of Authentication using Kelopatra tool. | Internet | Experiential Learning |
| 35,36 | Implement of Digital Signature using Kelopatra tool. | Internet | Experiential Learning |
| Content beyond syllabus covered (if any): Nil | | | |

*** Session duration: 50 mins**

SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY



**Sub. Code / Sub. Name: IT22609 / Information Security : Theory And Practices**
**Unit : IV**

**Unit Syllabus : SECURITY TECHNOLOGY**

Introduction- Access control- firewall, firewall using IP tables, protecting remote connections- Intrusion Detection and Prevention system –Honey pots, Honey Nets and Padded cell systems, scanning and analysis tools, Digital forensics.

**Suggested Activity:** Implement IDS using Snort tool

**Objective: To learn techniques specific to mitigating the occurrence of common software vulnerabilities.**

| Session No * | Topics to be covered | Ref | Teaching Aids |
|---|---|---|---|
| 37 | Introduction- Access control- firewall, firewall using IP tables | 3-Ch.6; Pg.325-371 | BB/ PPT |
| 38 | protecting remote connections | 3-Ch.6; Pg.371-379 | BB/ PPT |
| 39 | Intrusion Detection and Prevention system | 3-Ch.7; Pg.385-424 | BB/ PPT |
| 40 | Honey pots, Honey Nets and Padded cell systems | 3-Ch.7; Pg.424-428 | BB/ PPT |
| 41 | scanning and analysis tools | 3-Ch.7; Pg.428-443 | BB/ PPT |
| 42 | Digital forensics | 3-Ch.12; Pg.677-686 | BB/ PPT |
| 43,44 | Implement IDS using Snort tool | Internet | Experiential Learning |
| 45,46 | Study of Network Firewall Visualization Tool | Internet | Experiential Learning |
| 47,48 | Automated Attack and Penetration Tools Exploring N-Stalker, a Vulnerability Assessment Tool | Internet | Experiential Learning |
| Content beyond syllabus covered (if any): Study of Network Firewall Visualization Tool, Automated Attack and Penetration Tools Exploring N-Stalker, a Vulnerability Assessment Tool | | | |

*** Session duration: 50 mins**

SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY



**Sub. Code / Sub. Name: IT22609 / Information Security : Theory And Practices**
**Unit : V**

**Unit Syllabus : BLOCK CHAIN AND BEYOND**

Hashing – SHA – MD5 – Block chain: Basics – Contents of a Block – Hashchain to Blockchain - Digital Money to Distributed Ledgers , Design Primitives: Protocols, Security, Consensus, Permissions, Privacy - Basic consensus mechanisms Requirements for the consensus protocols, Proof of Work (PoW) – Crypto Currency.

**Suggested Activity:** Implement SHA, MD5, Secure File Management

**Objective: To implement security controls.**

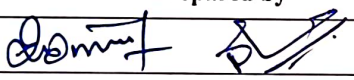
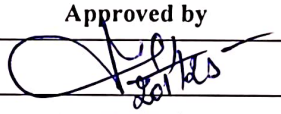
| Session No * | Topics to be covered | Ref | Teaching Aids |
|---|---|---|---|
| 49 | Hashing – SHA – MD5 | Internet | BB/ PPT |
| 50 | Block chain: Basics – Contents of a Block – Hashchain to Blockchain | Internet | BB/ PPT |
| 51 | Digital Money to Distributed Ledgers | Internet | BB/ PPT |
| 52 | Design Primitives: Protocols, Security, Consensus, Permissions, | Internet | BB/ PPT |
| 53 | Privacy - Basic consensus mechanisms | Internet | BB/ PPT |
| 54 | Requirements for the consensus protocols, Proof of Work (PoW) – Crypto Currency. | Internet | BB/ PPT |
| 55,56 | Implement SHA | Internet | Experiential Learning |
| 57,58 | Implement MD5 | Internet | Experiential Learning |
| 59,60 | Demo on login creation and Access Control | Internet | Experiential Learning |
| Content beyond syllabus covered (if any): Nil | | | |

*** Session duration: 50 mins**

Sub. Code / Sub. Name: IT22609 / Information Security : Theory And Practices

## REFERENCES:

1. Stallings William. Cryptography and Network Security: Principles and Practice, Seventh Edition, Pearson/PrenticeHal; 2018.
2. Matt Bishop ,"Computer Security art and science ", Second Edition, Pearson Education.
3. Michael E Whitman and Herbert J Mattord, "Principles of Information Security", Vikas Publishing House, New Delhi, fifth edition, Cengage learning , 2015.
4. Melanie Swa, "Block chain: Blueprint for a new economy", First edition, O'Reilly, 2015
5. Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", Fourth Edition, Prentice Hall, 2007.
6. Mark Rhodes- Ousley ,"Information Security: The complete Reference", Second Edition Mcgraw Hill, 2013.

| | Prepared by | Approved by |
|---|---|---|
| Signature |  |  |
| Name | Dr. A. Indumathi, Ms. N. Uma | Dr. V. Vidhya |
| Designation | Associate Professor, Assistant Professor | HoD/INT |
| Date | 20/01/2025 | 20/01/2025 |
| Remarks *: | | |
| Remarks *: | | |

*** If the same lesson plan is followed in the subsequent semester/year it should be mentioned and signed by the Faculty and the HOD**