

Bhoj Reddy Engineering College for Women: Hyderabad

Department of Information Technology

Lesson plan of faculty member for the academic year 2019–20

Class: III B Tech

Branch-Section: IT-B

Semester: II

Subject: Cryptography and Network Security

Lectures per week: 4

| Lecture Number | Topics to be covered | Date (s) |
|--|---|------------------|
| UNIT – I: Security Concepts, Cryptography Concepts and Techniques | | |
| 1 | Introduction-The need for Security | 17 December 2019 |
| 2 | Security Approaches, Principles of Security | 18 December 2019 |
| 3 | Types of Security Attacks | 19 December 2019 |
| 4 | Security Services, Security Mechanisms | 21 December 2019 |
| 5 | A Model for Network Security | 24 December 2019 |
| 6 | Plaintext and Cipher Text, Substitution Techniques | 28 December 2019 |
| 7 | Transposition Techniques | 31 December 2019 |
| 8 | Encryption and Decryption | 1 January 2020 |
| 9 | Symmetric and Asymmetric Key Cryptography | 4 January 2020 |
| 10 | Steganography, Key Range and Sizes, Possible Types of attacks | 7 January 2020 |
| UNIT-II: Symmetric and Asymmetric Key Ciphers | | |
| 11 | Block Cipher Principles, DES | 8 January 2020 |
| 12 | DES(Continued) | 9 January 2020 |
| 13 | AES | 11 January 2020 |
| 14 | Blowfish, RC5 | 16 January 2020 |
| 15 | IDEA, Block Cipher Operation | 18 January 2020 |
| 16 | Stream Cipher, RC4 | 21 January 2020 |
| 17 | Principles of Public Key Cryptosystems, RSA Algorithm | 22 January 2020 |
| 18 | Elgamal Cryptography | 23 January 2020 |
| 19 | Diffie-Hellman Key Exchange | 25 January 2020 |
| 20 | Knapsack Algorithm | 28 January 2020 |
| UNIT-III: Cryptographic Hash Functions, Key Management and Distribution | | |
| 21 | Message Authentication | 29 January 2020 |
| 22 | Secure Hash Algorithm(SHA-512) | 30 January 2020 |
| 23 | Message Authentication Codes-Authentication requirements | 1 February 2020 |
| 24 | HMAC, CMAC | 4 February 2020 |
| 25 | Digital Signatures | 5 February 2020 |
| 26 | Elgamal Digital Signature Scheme | 6 February 2020 |
| 27 | Revision | 8 February 2020 |
| 28 | Symmetric Key Distribution Using Symmetric Encryption | 13 February 2020 |
| 29 | Symmetric Key Distribution Using Asymmetric Encryption | 15 February 2020 |
| 30 | Distribution of public Keys | 18 February 2020 |
| 31 | Kerberos | 19 February 2020 |
| 32 | X.509 Authentication Service | 20 February 2020 |
| 33 | Public Key Infrastructure | 22 February 2020 |
| UNIT-IV: Transport Level Security and Wireless Network Security | | |
| 34 | Web Security Considerations, SSL | 25 February 2020 |
| 35 | Secure Socket Layer | 26 February 2020 |
| 36 | Transport Layer Security | 27 February 2020 |
| 37 | HTTPS | 29 February 2020 |
| 38 | Secure Shell | 03 March 2020 |
| 39 | Wireless Security | 4 March 2020 |
| 40 | Mobile Device Security | 5 March 2020 |
| 41 | IEEE 802.11Wireless LAN | 7 March 2020 |
| 42 | IEEE 908.11iWireless LAN Security | 10 March 2020 |
| 43 | Revision | 11 March 2020 |

| UNIT-V: E-Mail Security and Case Study | | |
|---|--|---------------|
| 44 | Pretty Good Privacy | 12 March 2020 |
| 45 | S/MIME | 14 March 2020 |
| 46 | IP Security Overview, IP Security Architecture | 17 March 2020 |
| 47 | Authentication Header | 18 March 2020 |
| 48 | Encapsulating Security Payload | 19 March 2020 |
| 49 | Combining Security Associations | 21 March 2020 |
| 50 | Internet Key Exchange | 24 March 2020 |
| 51 | Secure Multiparty Calculation | 26 March 2020 |
| 52 | Virtual Elections, Single Sign on | 28 March 2020 |
| 53 | Secure Inter Branch Payment Transactions | 31 March 2020 |
| 54 | Cross Site Scripting Vulnerability | 1 April 2020 |
| 55 | Revision | 4 April 2020 |
| 56 | Revision | 7 April 2020 |

Text books:

1. Cryptography and Network Security-Principles and Practice, 6/e, William Stallings, Pearson Education.
2. Cryptography and Network Security, Atul Kahate, 3/e, TMH.

Name and signature of the faculty: Minhaj Begum ----

Name and signature of Head of the Department: M Vinod ----