| Branch: BCA | Semester-V |
|---|---|
| Subject Code: 5103 | Lecture: 04<br>Credit: 04 |
| Course Opted | Core Course – 17 |
| Subject Title | CYBER SECURITY |

**Course Objectives:**

- The learner will gain knowledge about protect personal data, and secure computer networks.
- The learner will be able to examine secure software and wed security. The learner will be able to find solution to the key distribution problem by using functional key pair; public key cryptography
- The learner will develop an understanding of security policies (such as confidentiality, integrity, and availability), as well as protocols to implement such policies.
- The learner will be able to examine certain attacks on networks and security related services.

**Course Outcomes:**

The student will

- Understand the basic security principals
- Understand the concepts of data confidentiality security concern and its solution through cryptography
- Be able to verify identity through various authentication mechanisms
- Learn about Safeguarding the network at the network layer
- Learn about attacks on the networks and security related services

| Modules | Sr. No. | Topic and Details | No. of Lectures Assigned | Marks Weightage % |
|---|---|---|---|---|
| UNIT-I | 1 | **Introduction to Cyber Security:**<br>Introduction to Cyber Security, History, Goals, Need of Security, Principles, Elements, Type of Cyber Attacks, Security Policies, Security Techniques, Steps for Better Security, Basics Security Terminology (Cryptography, Hacking, Encryption, Decryption) | 6 | 12 |
| | 2 | **Data Encryption techniques:**<br>Introduction: Encryption Methods (Symmetric Encryption & Asymmetric Encryption), Cypotography.<br><br>**Subsitution Ciphers:** Ceaser, Monoalphabetic, Playfair, Hill, Polyalphabetic, One-tine Pad or Vernam.<br><br>**Transposition Ciphers:** Single Columnar, Double Columnar. Cyptanalysis, Steganograhy.<br><br>**Data Encryption Standards:** Working of DES, Cracking of DES, Simplified Data Encryption Standards.<br><br>**Symmetric Ciphers:** Introduction, Blowfish Architecture, RC5, RC4, RC6, Comparison between | 6 | 12 |

| | | | | |
|---|---|---|---|---|
| | | RC6 and RC5, IDEA (International Data Encryption Algorithm) | | |
| **UNIT-II** | 3 | **Public Key Cryptosystems:** Introduction, Public Key Cryptography, RSA Algorithm (Working of RSA, Key length and Security)<br><br>**Authentication:** Introduction, Authentications Methods(Password-based, Two-factor, Biometric, Extensible).<br><br>**Kerberos:** Basics, Ticket Granting Approach, Public Key Cryptography, Advantges, Weakness and attacks, Applications and Limitations, Comparison of Kerberos with SSL, Authentication Servers | 6 | 12 |
| | 4 | **Digital Signatures:** Introduction, Implementation, Association of Digital Signatures and Encryption, Using Different Key pairs for Signing and Encryption.<br><br>**Algorithms for Digital Signature:** DSA(Digital Signature Algorithm, ECDSA(Elliptic Curve Digital Signature Algorithm), DSS, Attacks on Digital Signature.<br><br>**Electronic Mail Security:** Introduction, Pretty Good Privacy (PGP), MIME, S/MIME, Comparison of PGP and S/MIME.<br><br>**IP Security:** Introduction, IP Security Architecture, IPv6, IPsec, IPv4 and IPv6, IPsec Protocols and Operations<br><br>**Web Security:** Introduction, SSL, SSL Session and Connection, SSL Record Protocol, Secure Electronic Transaction. | 7 | 14 |
| **UNIT-III** | 5 | **Intrusions:** Introduction, Intrusion Detection, Intrusion Detection System, Password Management Practices, Limitations, Challenges<br><br>**Malicious Software:** Introduction, Malicious Code, Viruses, Worms, Trojans, Spyware, Ransom ware, Bots, Best Practices, Attacks | 6 | 12 |
| | 6 | **Firewall:** Introduction, Characteristics, Types, Benefits and Limitations, Architecture,<br><br>**Cyber Laws:** Introduction, Cyber Security Regulations, Role of International Law, Cyber Security Standards, Indian Cyber Space, National Cyber Security Policies. | 6 | 12 |
| **UNIT-IV** | 7 | **Digital Forensic:** Introduction to cyber crimes & Digital Forensic, Types of Digital Forensics, Digital Forensics Process, Areas of Application of computer forensics, Understanding the Suspects, Examples of Computer Forensics, Free space and Slack Space. | 6 | 12 |

| | | | | |
|---|---|---|---|---|
| | | | | |
| | 8 | **Case Studies on Cryptography and security:** Cryptographic Solutions, SSO, Secure inter-branch Payment Transactions, Denial of Service (DOS) attacks, IP Spoofing attacks, CSSV, secrete splitting, Contract signing. | 7 | 14 |
| **TOTAL** | | | **50** | **100** |

**Text Book:**

1. Atul Kahate, Cryptography and Network Security, McGraw Hill

**Reference Books:**


1. Cybersecurity Fundamentals: A Real-World Perspective
2. CRYPTOGRAPHY AND INFORMATION SECURITY, THIRD EDITION, PACHGHARE, V. K. Eastern Economy Edition, 2019.
3. Kaufman, C., Perlman, R. & Speciner, M., Network Security, Private Communication in a Public world, 2nd ed., Prentice Hall PTR, 2002
4. Stallings, W., Cryptography and Network Security: Principles and Practice, 3rd ed., Prentice Hall PTR., 2003.
5. Stallings, W., Network Security Essentials: Applications and Standards, Prentice Hall, 2000
6. A Course in Cryptography, By Heiko Knospe, The Sally Series, AMS.