|  |  |
| --- | --- |
| **Course – 69 Title: Cryptography and Network Security** |  |
| **Course No.: CCE 421 Credit : 3.00 Contact Hours: 3** | **Total Marks: 100** |

**11.1 Rationale:**

As a computer scientist needs to know the network architecture, security, protection mechanism, attacker, and intruder.

**11.2 Objectives:**

1. To learn the network architecture
2. To know the network security attack, security mechanism and security protection
3. To gain the knowledge about encryption and decryption (cryptography) algorithms
4. To learn the internet/web/email security attack, security mechanism and security protection

|  |  |  |  |
| --- | --- | --- | --- |
| **11.3**  **Learning Outcomes** | **11.4**  **Course Content** | **11.5**  **Teaching Strategy/ Learning Experience** | **11.6 Assessment Strategy** |
| 1. Description of OSI layer architecture 2. Explain the security attacks, services and mechanism 3. Analyze a network model for security | Introduction: The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Internetwork Security, Internet Standards the Internet Society | Lecture  Assignment | Short answer  Analytical answer  quiz |
| 1. Define encryption 2. Description of different encryption technique. 3. OSI layer architecture 4. Explain the security attacks, services and mechanism 5. Analyze a network model for security | Symmetric Encryption and Message Confidentiality: Symmetric Encryption Principles, Symmetric Encryption Algorithms, Cipher Block Modes of Operation, Location of Encryption Devices, Key Distribution | Lecture  Brainstorming Assignment | Short answer  Analytical answer  quiz |
| 1. Define public key cryptography 2. Description of different message authentication technique. 3. Outline of hash function in cryptography, Digital signature and key management | Public Key Infrastructure, Public-Key Cryptography and Message Authentication: Approaches to Message Authentication, Secure Hash Functions and HMAC, Public Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures, Key Management | Lecture  Brainstorming Assignment | Short answer  Analytical answer  quiz  Group exercise |
| 1. Outline of different authentication Application | Authentication Applications: Kerberos, X.509 Directory Authentication Service | Lecture  Case studies | Analytical answer  quiz |
| 1. Outline of e-mail provider and security | Electronic Mail Security: Pretty Good Privacy (PGP), S/MIME | Lecture  Case studies | Short answer  Analytical answer |
| 1. Outline of IP security and architecture 2. Description | IP Security: IP Security Overview, IP Security Architecture, Authentication, Header, Encapsulating Security Payload, Combining Security Associations, Key Management. | Lecture  Assignment  Case studies | Short answer  Analytical answer  quiz  Group exercise |
| 1. Outline of web security and requirements 2. Analyze SSL, TLS and SET 3. Description of SNMP, SNMPv1 Community Facility, SNMPv3 | Web Security: Web Security Requirements, Secure Sockets Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET) | Lecture  Assignment  Case studies | Short answer  Analytical answer  quiz |
| 1. Outline of intruders | Network Management Security: Basic Concepts of SNMP, SNMPv1 Community Facility, SNMPv3 | Lecture  Assignment  Case studies | Short answer  quiz |
| 1. Outline of intruders | INTRUDERS: Intruders, Intrusion Detection, Password Management | Lecture | Short answer  quiz  Group exercise |

**RECOMMENDED BOOKS AND PERIODICALS**

**Text Books**: