**UNIT 1**

1. Networks Security.
2. Introduction Cryptography.
3. Security Threats.
   1. Types:
      * Malware
      * Phishing
      * Ransomware
4. Vulnerability.:
   1. Type:
      * Software Vulnerability.
      * Network Vulnerabilities.
      * Configuration Vulnerability.
5. Active Attack.
   1. Type of Active Attack:
      * Denial -of-service (Dos) Attack.
      * Man-in-the-Middle (MitM) Attack.
6. Passive attacks.
   1. Types of Passive Attack:
      * Password Attacks.
      * Packet Sniffing.
7. Security services and mechanisms.
   1. Types:
      * Access Control.
      * Authentication.
      * Encryption
      * Firewalls.
8. Conventional Encryption Model.
   1. Types:
      * Data encryption Standard (DES).
      * Advanced Encryption Standard. (AES).
9. CIA model (Confidentiality Integrity Availability)

**UNIT 2**

1. Modular Arithmetic.
   1. Types:
      * Modular Addition
      * Modular Multiplication
      * Modular exponentiation.
   2. Application:
      * Public-key cryptography.
      * Digital signatures.
      * Messages authentication codes.
2. Euclidean Algorithm.
3. Extended Euclidean Algorithm.
4. Fermat Theorem.
5. Euler’s Theorem.

**UNIT 3**

1. Dimension of Cryptography.
   1. Types of Dimensions.
      * Asymmetric Cryptography.
      * Cryptography Protocols.
      * Digital Signatures
      * Has Function.
      * Key Exchange Protocol.
      * Symmetric Cryptography.
2. Classical cryptographic techniques block. (DES, AES).
   1. Types:
      1. Data Encryption Standard (DES).
      2. Advanced Encryption Standard (AES).
3. Feistel Cipher Structure
   1. Steps:
      1. Key Expansion
      2. Round Function.
      3. Rounds of processing.
      4. Fila Round.
4. Simplifies DES
   1. Steps:
      1. Key Generation
      2. Initial Permutation (IP).
      3. Feistel Structure.
      4. Inverse Initial Permutation (IP-1)
5. Double DES.
6. Triple DES.
7. Block Cipher Design Principles.
   1. Design Principles of Block Ciphers:
      1. Confusion.
      2. Diffusion.
      3. Key Expansion.
      4. Security against know attacks.
   2. Types:
      1. DES
      2. AES
      3. 3DES
8. AES
   1. Types:
      1. Electronic Codebook (ECB).
      2. Cipher Block Chaining (CBC)
      3. Counter (CTR).
9. Modes of Operation in Public-key Cryptography.
   1. Type:
      1. Symmetric-key Encryption.
      2. Asymmetric-key encryption.
      3. Hybrid Encryption.
      4. Key exchanges.
      5. Digital Signatures.
10. Principles of Public-key Cryptography
    1. How work:
       1. Key Generation.
       2. Encryption.
       3. Decryption.
       4. Digital Signatures.
11. RSA Algorithm.
    1. How work:
       1. Key Generation.
       2. Encryption.
       3. Decryption.
12. Key Management
    1. Several important aspects.
       1. Key generation.
       2. Key Distribution.
       3. Key Storage.
       4. Key Revocation.
       5. Key Rotation
       6. Key Escrow.
13. Diffie-Hellman Key Exchange.
14. Elgamal Algorithm.
15. Elliptic Curve Cryptography.

**UNIT 4**

1. Has Algorithms.
2. MAC Algorithm.
3. Authentication Requirements.
   1. Types of Authentication Requirements:
      1. Somethings You Know (SYK).
      2. Something You Have (SYH).
      3. Somethings You Are (SYA).
      4. Location-Based Authentication.
      5. Time-Based Authentication.
4. Functions
   1. Types:
      1. Symmetric Function.
      2. Asymmetric Function.
      3. Hash Function.
      4. Digital Signature Function.
      5. Key Exchanges Functions.
5. Message Authentication Code.
   1. Types:
      1. HMAC (Hash-based MAC)
      2. CMAC (Cipher-based MAC)
6. Hash Functions
   1. Types:
      1. Cryptography Has Functions.
      2. Non-Cryptographic Has Functions.
      3. Message Digest Functions.
7. Secure Has Algorithm.
   1. Types:
      1. SHA-256 (Secure Hash Algorithm 256).
      2. SHA-512 (Secure Hash Algorithm 512)
      3. MD5 (Message-Digest-Algorithm 5)
8. Digital Signatures.
   1. Types:
      1. Symmetric Digital Signatures Algorithm
      2. Rivest-Shamir-Adleman (RSA).
9. Key Distribution Techniques.
   1. Types:
      1. Symmetric Key Distribution.
         1. Pre-Shared Key (PSK).
      2. Asymmetric Key Distribution.
         1. Public Key Infrastructure (PKI).

**UNIT 5**

1. Threats in Networks:
   1. Types:
      1. Malware.
      2. DoS
2. Networks Security Control Architecture.
   1. Components:
      1. Perimeter Security Controls.
      2. Networks Segmentation.
      3. Access Control Mechanism.
      4. Intrusion Detection and prevention System.
      5. Data Encryption.
      6. Vulnerability Management.
      7. Networks Monitoring and Logging.
      8. Security Awareness Training.
      9. Incident Repones Plan.
3. Encryption.
4. Content Integrity.
5. Strong Authentication.
6. Access Controls.
   1. Types:
      1. Physical Access Controls.
      2. Technical Access Controls.
      3. Administrative Access Controls.
7. Wireless Security.
   1. Wireless Security Components:
      1. Encryption.
      2. Authentication.
      3. Access Control.
      4. Instruction Detection and Prevention Systems.
      5. Regular Update and Patch Management.
      6. Networks Monitoring and Logging.
8. Honeypots.
   1. Types of Honeypots.
      1. Low-Interaction Honeypot.
      2. High-Interaction Honeypot.
9. Traffic flow security.
10. Personal Firewalls
    1. Types:
       1. Software Based Firewall.
       2. Hardware Based Firewall.
11. Instruction Detection System (IDS).
    1. Types:
       1. Network based IDS
       2. Host-based IDS
       3. Wireless IDS
       4. Application Based IDS.
12. Email Security
13. PGP (Pretty Good Privacy.)
14. S/SMIME (Secure / Multipurpose Internet Mail Extensions.)