Information Security

Unit - I :-

① 1. Computer Security concepts.

2. The OSI Security Architecture

3. Security attacks

4. Security Services & Security mechanisms.

5. A model for N/w security.

② Classical encryption techniques - 1. Symmetric cipher model.
2. Substitution ciphers
3. Transposition ciphers
4. Steganography.

③ Modern Block Ciphers: 1. Block ciphers priciples.
2. Data encryption standard (DES)
3. Strength of DES
4. linear & differential cryptanalysis
5. Block cipher models of operations.
6. AES
7. RC4

Unit - II :-

① Introduction to Number theory: 1. Integer Arithmetic.
2. Modular Arithmetic
3. Matrices
4. linear congruence
5. Algebraic Structures

Scanned by CamScanner

6. GF(2^n) Fields
7. Primes
8. Primality Testing
9. Factorization
10. Chinese remainder Theorem
11. Quadratic Congruence
12. Exponentation & logarithm

② Public-key cryptography - 1. Principles of public-key cryptography.
2. RSA Algorithm
3. Diffie-Hellman key Exchange
4. ElGamal cryptopraphic system
5. Elliptic Curve Arithematic
6. Elliptic Curve cryptography.

Unit-III :-

① Cryptographic Hash Functions: 1. App's of cryptographic Hash func.
2. Requirements & Security
3. Hash Functions based on Cipher Block chaining.
4. Secure Hash Algorithm (SHA).

② Message Authentication Codes: 1. Message authentication requirements
2. Message authentication functions
3. Requirements for Message authentication codes
4. Security of MACs, HMACs based on Block cipher

Scanned by CamScanner

6. Authenticated Encryption Digital Signatures - RSA with SHA & DSS.

Unit - IV :-

① Key Management & distribution : 1. Symmetric key distribution using Symmetric Encryption.

2. Symmetric key distribution using Asymmetric.

3. Distribution of public keys.

4. X.509 certificates.

5. Public key infrastructure.

② User Authentication : 1. Remote user Authentication principles.

2. Remote user Authentication using Symettric Encryption

3. Kerberos.

4. Remote user Authentication using Asymmetric Encription.

5. Federated Identity Management.

6. Electronic mail security.

7. Pretty Good Privacy (PGP).

8. S/MIME

Unit - V :-

Security at the transport Layer (SSL & TLS) : 1. SSL Architecture

2. Four protocols.

3. SSL Message Formats.

4. Transport Layer Security

Scanned by CamScanner

5. HTTPS

6. SSH

② Security at the N/w layer (IPSec): 1. Two modes

2. Two Security Protocols.

3. Security Association

4. Security Policy

5. Internet key Exchange.

③ Slm Security: 1. Description of the slm

2. Users.

3. Trust & Trusted systems.

4. Buffer Overflow & Malicious s/w

5. Malicious Prgms

6. Worms

7. Viruses

8. Intrusion Detection System (IDS)

9. Firewalls. ✓

Scanned by CamScanner