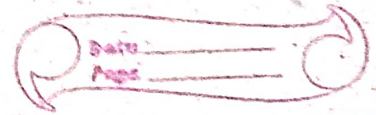


Cryptography



Unit-1

- 1) Caesar, Hill, Playfair and Rail fence cipher for encryption numerical.
- 2) Vernam Cipher & One Time Pad for short note.
- 3) Symmetric vs. Asymmetric Ciphers.
- 4) Definition only for Substitution technique, transportation technique, monoalphabetic cipher, polyalphabetic cipher.

Unit-2

- 1) Extended Euclidean Algorithm.
- 2) Finding Multiplicative inverses.
- 3) Calculating results of polynomial over $GF(2)$
- 4) Round operations in IDEA.
- 5) Advanced Encryption Standard (AES).

Unit-3

- 1) Miller-Rabin Primality Testing.
- 2) Fermat's theorem, Euler's totient function, Euler's theorem, Primitive root.
- 3) D-H Key Exchange, Man-In-the-Middle Attack, RSA algorithm.

Unit-4

- 1) One way property of hash function.
- 2) Message Digests Version 4 (MD4).
- 3) ~~SHA~~ Digital Signature, DSS and RSA approach for digital signature.

Unit-5

- 1) Authentication system, Challenge Response System, Kerberos Protocol.

Unit-6

- 1) Concept of PKI trust model, SSL Protocol, Firewalls.

Unit-7

- 1) Virus vs. Worm vs. Trojan Horse, IDS.