CRNS Syllabus

Test-1

CHAPTER 1:

Cryptography basics – Encryption/Decryption

Symmetric types – Substitution and Transposition cipher

Substitution ciphers:

Caesar, Playfair, Hill, One-time pad, Monoalphabetic, Polyalphabetic, Vigenere

Transposition ciphers:

Rail Fence and Row Column transposition

Examples of Security Requirements

Key Security Concepts -CIA Triad,

Security Architecture

Types of security attacks – Active (Interruption, Fabrication, Replay, Modification) Vs. Passive attacks (Interception, Traffic Analysis)

Security Services – (Authentication, Access Control, Data Integrity, confidentiality, Non-repudiation)

Steganography

Cryptanalysis, Brute-force attack

Model for Network Security

CHAPTER 2:

Working principle of the Feistel structure in DES.

How Block Cipher works.

Difference between Symmetric and Asymmetric key encryption.

DES & its steps (all appropriate diagrams).

CHAPTER 3:

Hash Functions and Data Integrity, Properties of Hash Function, Patterns of hashing data, Security of Hash Functions, Collision-free property

---