→ Railfence Method (Rail = 3 ; Rail = 2 ;)

→ RSA (sums, theory)

→ AES (theory)

→ DES (theory)

→ TCP hijacking (theory)

→ Play-~~Cph~~ fair cipher method (sum)

↓ (rules)

→ Blow-Fish Encry Algo

(blocks (no-of) _ block diag (all))

(include Feestal Cipher)

→ Diffie Hellman (problem)

→ SQL injection (practical ex → (From lab) ; Theory)

→ Ciesar Cipher (ex, theory)

(Use the ciesar cipher with shift of 14 to encrypt & decrypt message for "GOOD MORNING")

(both decryption & encryption)

→ Types of attacks.

→ Block & stream cipher diff with ex

→ MIM

→ All techniques

→ triple DES

→ How is authentication done in public-key cryptosystem ?

→ Symmetric cipher → Hill cipher model

→ security mechanisms

→ avalanche effect

→ Explain feistel cipher (coif given block diag)