

**CCIX - INFORMATION SYSTEM SECURITY**

**UNIT-I**

Introduction-attacks, services & mechanisms – security attacks- security services

Conventional encryption & message confidentiality- conventional encryption principles- conventional encryption algorithms- cipher block modes of operation- location of encryption devices- key distribution

**UNIT-II**

Public key cryptography & message authentication- approaches to message authentication secure hash functions – public key cryptography principles & algorithms – digital signature – key management – kerberos

**UNIT-III**

Ip security – ip security overview & architecture – authentication header – encapsulating security payload combining security associations – key management

**UNIT-IV**

Web security –web security requirements –secure sockets layer & transport layer security – secure electronics transaction

**UNIT-V**

Intruders & viruses – intruders – viruses & related threats

Firewalls- firewall design principles –trusted systems

**TEXT BOOK:**

Stallings W, NETWORK SECURITY ESSENTIALS,pearson education asia,2002.