

CS 331 Computer Networks

Network Security

- Objectives
 - encryption
 - authentication
 - message integrity
 - non-repudiation
- Encryption, Attacks
- Encryption Categories
 - Secret method
 - Public method, secret key
 - Public method, public and private keys
- Man-in-the-middle attack
- Encryption Methods
 - Caesar cipher
 - Monoalphabetic cipher
 - Polyalphabetic cipher
 - Vigenere cipher
 - block cipher