Basics of Cryptography

Otakar A.

Introduction

- “Hidden writing”
- Increasingly used to protect information
- Can ensure confidentiality
  - Integrity and Authenticity too

History – The Manual Era

- Dates back to at least 2000 B.C.
- Pen and Paper Cryptography
- Examples
  - Scytale
  - Atbash
  - Caesar
  - Vigenère

History – The Modern Era

- Computers!
- Examples
  - Lucifer
  - Rijndael
  - RSA
  - ElGamal

Speak Like a Crypto Geek

Plaintext – A message in its natural format readable by an attacker

Ciphertext – Message altered to be unreadable by anyone except the intended recipients

Key – Sequence that controls the operation and behavior of the cryptographic algorithm

Keyspace – Total number of possible values of keys in a crypto algorithm

Speak Like a Crypto Geek (2)

Initialization Vector – Random values used with ciphers to ensure no patterns are created during encryption

Ensures the encryption of the same string twice does not return the same result.

Types of Cryptography

- Stream-based Ciphers
  - One at a time
  - Good for real-time services
- Block Ciphers
  - Substitution and transposition

Encryption Systems

- Substitution Cipher
  - Convert one letter to another
  - Cryptoquip
- Transposition Cipher
  - Change position of letter in text
  - Word Jumble (Anagram)
- Monoalphabetic Cipher
  - Caesar

Encryption Systems

- Polyalphabetic Cipher
  - Vigenère
- Modular Mathematics
  - Running Key Cipher
- One-time Pads
  - Randomly generated keys

Steganography

- Hiding a message within another medium, such as an image
- No key is required
- Example
  - Modify color map of JPEG image

Cryptographic Methods

- *Symmetric*
  - Same key for encryption and decryption
  - Key distribution problem
- *Asymmetric*
  - Mathematically related key pairs for encryption and decryption
  - Public and private keys

Cryptographic Methods

- *Hybrid*
  - Combines strengths of both methods
  - Asymmetric distributes symmetric key
    - » Also known as a *session key*
  - Symmetric provides bulk encryption
  - Example:
    - » SSL negotiates a hybrid method