Outline

- History
- Terms & Definitions
- Symmetric and Asymmetric Algorithms
- Hashing
- PKI Concepts
- Attacks on Cryptosystems

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 Mechanical Era

- Invention of cipher machines
- Examples
  - Confederate Army’s Cipher Disk
  - Japanese Red and Purple Machines
  - German Enigma

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

Cryptosystem – The combination of algorithm, key, and key management functions used to perform cryptographic operations

Cryptosystem Services

- Confidentiality
- Integrity
- Authenticity
- Nonrepudiation
- Access Control

Types of Cryptography

- Stream-based Ciphers
  - One at a time, please
  - Mixes plaintext with key stream
  - Good for real-time services
- Block Ciphers
  - Amusement Park Ride
  - Substitution and transposition

Encryption Systems

- Substitution Cipher
  - Convert one letter to another
  - Cryptoquip
- Transposition Cipher
  - Change position of letter in text
  - Word Jumble
- 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

Attributes of Strong Encryption

- ***Confusion***
  - Change key values each round
  - Performed through substitution
  - Complicates plaintext/key relationship
- ***Diffusion***
  - Change location of plaintext in ciphertext
  - Done through transposition

Symmetric Algorithms

- DES
  - Modes: ECB, CBC, CFB, OFB, CM
- 3DES
- AES
- IDEA
- Blowfish

Symmetric Algorithms

- RC4
- RC5
- CAST
- SAFER
- Twofish

Asymmetric Algorithms

- Diffie-Hellman
- RSA
- El Gamal
- Elliptic Curve Cryptography (ECC)

Hashing Algorithms

- MD5
  - Computes 128-bit hash value
  - Widely used for file integrity checking
- SHA-1
  - Computes 160-bit hash value
  - NIST approved message digest algorithm

Hashing Algorithms

- HAVAL
  - Computes between 128 and 256 bit hash
  - Between 3 and 5 rounds
- RIPEMD-160
  - Developed in Europe published in 1996
  - Patent-free

Birthday Attack

- Collisions
  - Two messages with the same hash value
- Based on the “birthday paradox”
- Hash algorithms should be resistant to this attack

Message Authentication Codes

- Small block of data generated with a secret key and appended to a message
- HMAC (RFC 2104)
  - Uses hash instead of cipher for speed
  - Used in SSL/TLS and IPSec

Digital Signatures

- Hash of message encrypted with private key
- Digital Signature Standard (DSS)
  - DSA/RSA/ECD-SA plus SHA
- DSS provides
  - Sender authentication
  - Verification of message integrity
  - Nonrepudiation

Encryption Management

- Key Distribution Center (KDC)
  - Uses master keys to issue session keys
  - Example: Kerberos
- ANSI X9.17
  - Used by financial institutions
  - Hierarchical set of keys
  - Higher levels used to distribute lower

Public Key Infrastructure

- All components needed to enable secure communication
  - Policies and Procedures
  - Keys and Algorithms
  - Software and Data Formats
- Assures identity to users
- Provides key management features