CS 356 – Lecture 2
Cryptographic Tools

Spring 2013
Chapter 2

Cryptographic Tools
Cryptographic Tools

• Cryptographic algorithms important element in security services

• Review various types of elements
  – symmetric encryption
  – secure hash functions
  – public-key (asymmetric) encryption
  – digital signatures and key management

• Example use to encrypt stored data
Symmetric Encryption

- the universal technique for providing confidentiality for transmitted or stored data

- also referred to as conventional encryption or single-key encryption

- two requirements for secure use:
  - need a strong encryption algorithm
  - sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure
SYMMETRIC ENCRYPTION

Figure 2.1 Simplified Model of Symmetric Encryption
Data Encryption Standard (DES)

- the most widely used encryption scheme
  - FIPS PUB 46
  - referred to as the Data Encryption Algorithm (DEA)
  - uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block

- strength concerns:
  - concerns about algorithm
    - DES is the most studied encryption algorithm in existence
  - use of 56-bit key
    - Electronic Frontier Foundation (EFF) announced in July 1998 that it had broken a DES encryption
Attacking Symmetric Encryption

Cryptanalytic Attacks

- rely on:
  - nature of the algorithm
  - some knowledge of the general characteristics of the plaintext
  - some sample plaintext-ciphertext pairs
  - exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
  - if successful all future and past messages encrypted with that key are compromised

Brute-Force Attack

- try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
  - on average half of all possible keys must be tried to achieve success
Exhaustive Key Search

<table>
<thead>
<tr>
<th>Key Size (bits)</th>
<th>Number of Alternative Keys</th>
<th>Time Required at 1 Decryption/µs</th>
<th>Time Required at $10^6$ Decryptions/µs</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>$2^{32} = 4.3 \times 10^9$</td>
<td>$2^{31} \mu s = 35.8$ minutes</td>
<td>2.15 milliseconds</td>
</tr>
<tr>
<td>56</td>
<td>$2^{56} = 7.2 \times 10^{16}$</td>
<td>$2^{55} \mu s = 1142$ years</td>
<td>10.01 hours</td>
</tr>
<tr>
<td>128</td>
<td>$2^{128} = 3.4 \times 10^{38}$</td>
<td>$2^{127} \mu s = 5.4 \times 10^{24}$ years</td>
<td>5.4 $\times 10^{18}$ years</td>
</tr>
<tr>
<td>168</td>
<td>$2^{168} = 3.7 \times 10^{50}$</td>
<td>$2^{167} \mu s = 5.9 \times 10^{36}$ years</td>
<td>5.9 $\times 10^{30}$ years</td>
</tr>
<tr>
<td>26 characters (permutation)</td>
<td>$26! = 4 \times 10^{26}$</td>
<td>$2 \times 10^{26} \mu s = 6.4 \times 10^{12}$ years</td>
<td>6.4 $\times 10^6$ years</td>
</tr>
</tbody>
</table>

**Average Time Required for Exhaustive Key Search**
Figure 2.2 Time to Break a Code (assuming 10^6 decryptions/ms) The graph assumes that a symmetric encryption algorithm is attacked using:

• a brute-force approach of trying all possible keys.
Triple DES (3DES)

- repeats basic DES algorithm three times using either two or three unique keys
- first standardized for use in financial applications in ANSI standard X9.17 in 1985

**attractions:**
- 168-bit key length overcomes the vulnerability to brute-force attack of DES
- underlying encryption algorithm is the same as in DES

**drawbacks:**
- algorithm is sluggish in software
- uses a 64-bit block size
Advanced Encryption Standard (AES)

needed a replacement for 3DES

3DES was not reasonable for long term use

NIST called for proposals for a new AES in 1997

should have a security strength equal to or better than 3DES

significantly improved efficiency

symmetric block cipher

128 bit data and 128/192/256 bit keys

selected Rijndael in November 2001

published as FIPS 197
DES, 3DES, and AES

<table>
<thead>
<tr>
<th></th>
<th>DES</th>
<th>Triple DES</th>
<th>AES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaintext block size (bits)</td>
<td>64</td>
<td>64</td>
<td>128</td>
</tr>
<tr>
<td>Ciphertext block size (bits)</td>
<td>64</td>
<td>64</td>
<td>128</td>
</tr>
<tr>
<td>Key size (bits)</td>
<td>56</td>
<td>112 or 168</td>
<td>128, 192, or 256</td>
</tr>
</tbody>
</table>

DES = Data Encryption Standard
AES = Advanced Encryption Standard

•Comparison of Three Popular Symmetric Encryption Algorithms
Practical Security Issues

• typically symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block

• electronic codebook (ECB) mode is the simplest approach to multiple-block encryption
  • each block of plaintext is encrypted using the same key
  • cryptanalysts may be able to exploit regularities in the plaintext

• modes of operation
  • alternative techniques developed to increase the security of symmetric block encryption for large sequences
  • overcomes the weaknesses of ECB
Block Cipher Concepts

1. Divide (plaintext) Data Into Fixed Blocks
   • DES divides message into 64 bit blocks

2. Apply The Algorithm to Each Block
   • Input is block and symmetric key
   • Output is a block of encrypted data

3. Transmit the Encrypted Block

4. Decrypt the Block
   • Input is block and symmetric key
   • Output is a block of decrypted data
Block Cipher Encryption

Stream Encryption

Figure 2.3 Types of Symmetric Encryption
Block & Stream Ciphers

**Block Cipher**
- processes the input one block of elements at a time
- produces an output block for each input block
- can reuse keys
- more common

**Stream Cipher**
- processes the input elements continuously
- produces output one element at a time
- primary advantage is that they are almost always faster and use far less code
- encrypts plaintext one byte at a time
- pseudorandom stream is one that is unpredictable without knowledge of the input key
Message Authentication

- protects against active attacks
- verifies received message is authentic
  - contents have not been altered
  - from authentic source
  - timely and in correct sequence
- can use conventional encryption
  - only sender & receiver share a key
Figure 2.4 Message Authentication Using a Message Authentication Code (MAC). The MAC is a function of an input message and a secret key.
Secure Hash Functions

Figure 2.5 Block Diagram of Secure Hash Function; $h = H(M)$
Hash Function Requirements

- can be applied to a block of data of any size
- produces a fixed-length output
- $H(x)$ is relatively easy to compute for any given $x$
- one-way or pre-image resistant
  - computationally infeasible to find $x$ such that $H(x) = h$
- second pre-image resistant or weak collision resistant
  - computationally infeasible to find $y \neq x$ such that $H(y) = H(x)$
- collision resistant or strong collision resistance
  - computationally infeasible to find any pair $(x, y)$ such that $H(x) = H(y)$
Security of Hash Functions

- there are two approaches to attacking a secure hash function:
  - cryptanalysis
    - exploit logical weaknesses in the algorithm
  - brute-force attack
    - strength of hash function depends solely on the length of the hash code produced by the algorithm

- SHA most widely used hash algorithm

- additional secure hash function applications:
  - passwords
    - hash of a password is stored by an operating system
  - intrusion detection
    - store H(F) for each file on a system and secure the hash values
Message Authentication Using a One-Way Hash Function

Figure 2.6 Message Authentication Using a One-Way Hash Function. The hash function maps a message into a relatively small, fixed-size block.
What’s Next

- Read Chapter 1 and 2
  - Chap 1: Focus on big picture and recurring concepts
  - Chap 2: Identify cryptographic tools and properties
- Project 1 is Posted on Course Website
  - Due 9/6
- Homework 2 is Posted on Course Website
  - Due Thursday
- Next Lecture Topics from Chapter 2
  - More Cryptographic Tools