Secret Keys or Secret Algorithms?

- “Security by obscurity”
  - “hide” the details of the algorithms
  - drawback: hard to keep secret if cipher is used widely, or implementation can be reverse engineered
- Alternative: publish the algorithms
  - fewer vulnerabilities will result if many smart people try and fail to break the cipher
  - security of the cipher depends on the secrecy of the keys, instead

Secret Key Cryptography

- Same key is used for both encryption and decryption
  - this one key is shared by two parties who wish to communicate securely
- Also known as symmetric key cryptography, or shared key cryptography

Secrets? (Cont’d)

- Commercial world relies upon standardized, public algorithms, and secret keys
- Government tends to also rely on secret algorithms
Applications of Secret Key Crypto

- **Communicating securely** over an insecure channel
  - Alice encrypts using shared key
  - Bob decrypts result using same shared key
- **Secure storage** on insecure media
  - Bob encrypts data before storage
  - Bob decrypts data on retrieval using the same key

Applications... (Cont’d)

- **Message integrity**
  - Alice computes a message integrity code (MIC) from the message, then encrypts with shared key
  - Bob decrypts the MIC on receipt, and verifies that it agrees with message contents
- **Authentication**
  - Bob can verify Alice sent the message
  - how is that possible?

Generic Block Encryption

- Converts one input plaintext block of fixed size $k$ bits to an output ciphertext block also of $k$ bits
- Benefits of large $k$? of short $k$?

Key Sizes

- Keys should be selected from a large potential set, to prevent brute force attacks
- Secret key sizes
  - 40 bits were considered adequate in 70’s
  - 56 bits used by DES were adequate in the 80’s
  - 128 bits are adequate for now
- If computers increase in power by 40% per year, need roughly 5 more key bits per decade to stay “sufficiently” hard to break

Notation

<table>
<thead>
<tr>
<th>Notation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X \oplus Y$</td>
<td>Bit-wise exclusive-or of $X$ and $Y$</td>
</tr>
<tr>
<td>$X</td>
<td>Y$</td>
</tr>
<tr>
<td>$K(m)$</td>
<td>Message $m$ encrypted with secret key $K$</td>
</tr>
</tbody>
</table>

Two Principles for Cipher Design

- **Confusion:**
  - Make the relationship between the <plaintext, key> input and the <ciphertext> output as complex (non-linear) as possible
- **Diffusion:**
  - Spread the influence of each input bit across many output bits
Exploiting the Principles

• Idea: use multiple, alternating permutations and substitutions, e.g.,
  − S  P  S  P  ...
  − P  S  P  S  ...
• Do they have to alternate? e.g.,
  − S  S  S  P  P  P  ...
• Confusion is mainly accomplished by substitutions
• Diffusion is mainly accomplished by permutations
• Example ciphers: DES, AES

Secret Key… (Cont’d)

• Basic technique used in secret key ciphers: multiple applications of alternating substitutions and permutations

Well-known examples: DES, AES

Basic Form of Modern Block Ciphers

Overview

• Feistel Cipher has been a very influential “template” for designing a block cipher
• Major benefit: can do encryption and decryption with the same hardware
• Examples: DES, RC5

One “Round” of Feistel Encryption

1. Break input block i into left and right halves L_i and R_i
2. Copy R_i to create output half block L_{i+1}
3. Half block R_i and key K_i are “scrambled” by function f
4. XOR result with input half-block L_i to create output half-block R_{i+1}
One “Round” of Feistel Decryption

- Just reverse the arrows!

Input block $i$

- Output block $i+1$

Complete Feistel Cipher: Encryption

- Round 1
- Round $i$
- Round $n$

Parameters of a Feistel Cipher

- Block size
- Key size
- Number of rounds
- Subkey generation algorithm
- “Scrambling” function $f$

Comments

- Decryption is same as encryption, only reversing the order in which round keys are applied
  - Reversability of Feistel cipher derives from reversibility of XOR
- Function $f$ can be anything
  - Hopefully something easy to compute
  - There is no need to invert $f$

DES (Data Encryption Standard)
DES (Data Encryption Standard)

- Standardized in 1976 by NBS
  - proposed by IBM,
  - Feistel cipher
- Criteria (official)
  - provide high level of security
  - security must reside in key, not algorithm
  - not patented
  - must be exportable
  - efficient to implement in hardware

DES Basics

- Blocks: 64 bit plaintext input, 64 bit ciphertext output
- Rounds: 16
- Key: 64 bits
  - every 8th bit is a parity bit, so really 56 bits long

DES Top Level View

- Initial permutation
- Round 1
- Round 2
- ... Round 16
- Swap Halves
- Final permutation

Initial and Final Permutations

- Initial permutation given below
  - input bit #58 → output bit #1, input bit #50 → output bit #2, ...

Initial... (Cont’d)

- Final permutation is just inverse of initial permutation, i.e.,
  - input bit #1 → output bit #58
  - input bit #2 → output bit #50
  - ...

• Criteria (unofficial)
  - must be slow to execute in software
  - must be breakable by NSA :-)

DES... (Cont’d)
Initial… (Cont’d)

• Note #1: Initial Permutation is fully specified (independent of key)
  – therefore, does not improve security!
  – why needed?
• Note #2: Final Permutation is needed to make this a Feistel cipher
  – i.e., can use same hardware for both encryption and decryption

Key Generation: First Permutation

- First step: throw out 8 parity bits, then permute resulting 56 bits
- Parity bits left out: 8, 16, 24, ...

Key Generation: Permutation with Discard

- 28 bits → 24 bits, each half of key
- Left half of $K_i = \text{permutation of } C_i$
- Right half of $K_i = \text{permutation of } D_i$
- Bits left out: 9, 18, 22, 25
- Bits left out: 35, 38, 43, 54

One DES (Feistel) Round

Key Round: $f$ (Mangler) Function

- Function $f$ = “Mangler”
- Input block $i$
- Output block $i+1$
**f: Expansion Function**

- 32 bits $\rightarrow$ 48 bits

<table>
<thead>
<tr>
<th>32</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
<tr>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
</tr>
<tr>
<td>28</td>
<td>29</td>
<td>30</td>
<td>31</td>
<td>32</td>
<td>1</td>
</tr>
</tbody>
</table>

**f: S-Box (Substitute, Shrink)**

- 48 bits $\rightarrow$ 32 bits
- 6 bits are used to select a 4-bit substitution
- i.e., for every output, there are four inputs that map to it

2 bits row

4 bits column

for $i = 1, \ldots, 8$

$S_i$ (Substitution)

Each row and column contain different numbers

<table>
<thead>
<tr>
<th>12/13/14/15</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>...</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>E</td>
<td>4</td>
<td>D</td>
<td>1</td>
<td>2</td>
<td>F</td>
<td>B</td>
<td></td>
<td>---</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>F</td>
<td>7</td>
<td>4</td>
<td>E</td>
<td>2</td>
<td>D</td>
<td></td>
<td>---</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>E</td>
<td>B</td>
<td>D</td>
<td>6</td>
<td>2</td>
<td></td>
<td>---</td>
</tr>
<tr>
<td>3</td>
<td>F</td>
<td>C</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td></td>
<td>---</td>
</tr>
</tbody>
</table>

Example: input = 100110, output = 1000

For $S_2, S_3$ (and rest of $S_i$), see the textbook

**f: Permutation**

- 48 bits $\rightarrow$ 48 bits

<table>
<thead>
<tr>
<th>16</th>
<th>7</th>
<th>20</th>
<th>21</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>12</td>
<td>28</td>
<td>17</td>
</tr>
<tr>
<td>1</td>
<td>15</td>
<td>23</td>
<td>26</td>
</tr>
<tr>
<td>5</td>
<td>18</td>
<td>31</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>24</td>
<td>14</td>
</tr>
<tr>
<td>32</td>
<td>27</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>19</td>
<td>13</td>
<td>30</td>
<td>6</td>
</tr>
<tr>
<td>22</td>
<td>11</td>
<td>4</td>
<td>25</td>
</tr>
</tbody>
</table>

**DES Implementation**

- That’s it!
- Operations
  - Permutation
  - Swapping halves
  - Substitution (S-box, table lookup)
  - Bit discard
  - Bit replication
  - Circular shift
  - XOR
- Hard to implement? HW: No, SW: Yes

**Test Program**

- DES Block Cipher Calculator
- DES Key (in Hex): 8e098bcb764a0bc6
- Encrypted value for 123456789abcdefg
- Value Letters: $\text{A}$: A, $\text{B}$: B, $\text{C}$: C, $\text{D}$: D, $\text{E}$: E, $\text{F}$: F, $\text{G}$: G, $\text{H}$: H
- Keys of DES Calculations or Secret
DESA

Good Design?

- “We don’t know if
  - the particular details were well-chosen for strength,
  - whether someone flipped coins to construct the S-boxes,
  - or whether the details were chosen to have a weakness that could be exploited by the designers.”

Issues for Block Ciphers

- Number of rounds should be large enough to make advanced attacks as expensive as exhaustive search for the key

Principles for S-Box Design

- S-box is the only non-linear part of DES
- Each row in the S-Box table should be a permutation of the possible output values
- Output of one S-box should affect other S-boxes in the following round

Desirable Property: Avalanche Effect

- Roughly: a small change in either the plaintext or the key should produce a big change in the ciphertext
- Better: any output bit should be inverted (flipped) with probability .5 if any input bit is changed
- $f$ function
  - must be difficult to un-scramble
  - should achieve avalanche effect
  - output bits should be uncorrelated

DES Avalanche Effect: Example

- 2 plaintexts with 1 bit difference:
  0x0000000000000000 and
  0x8000000000000000
encrypted using the same key:
  0x016B24621C181C32

- Resulting ciphertexts differ in 34 bits (out of 64)
- Similar results when keys differ by 1 bit
Example (cont’d)

- An experiment: number of rounds vs. number of bits difference

<table>
<thead>
<tr>
<th>Round #</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits changed</td>
<td>1</td>
<td>6</td>
<td>21</td>
<td>35</td>
<td>39</td>
<td>32</td>
<td>31</td>
<td>29</td>
<td>...</td>
</tr>
</tbody>
</table>

| 9 | 11 | 12 | 13 | 14 | 15 | 16 |

| 42 | 44 | 32 | 30 | 30 | 26 | 29 | 34 | ... |

DES: Keys to Avoid Using

- “Weak keys”: 4 keys with property $K_1(K_2(m)) = m$
- What’s bad about that?
- These are keys which, after the first key permutation, are:
  - 28 0’s followed by 28 0’s
  - 28 0’s followed by 28 1’s
  - 28 1’s followed by 28 0’s
  - 28 1’s followed by 28 1’s

More Keys to Avoid!

- “Semi-weak keys”: pairs of keys with the property $K_1(K_2(m)) = m$
- What’s bad about that?
- These are keys which, after the first key permutation, are:
  1. 28 0’s followed by alternating 0’s and 1’s
  2. 28 0’s followed by alternating 1’s and 0’s
  ... 12. alternating 1’s and 0’s followed by alternating 1’s and 0’s

DES Key Size

- 56 bits is currently too small to resist brute force attacks using readily-available hardware
- Ten years ago it took $250,000 to build a machine that could crack DES in a few hours
- Now?

Cryptanalysis of DES

- Differential cryptanalysis exploits differences between encryptions of two different plaintext blocks
  - provides insight into possible key values
  - DES well designed to defeat differential analysis
- Linear cryptanalysis requires known plaintext / ciphertext pairs, analyzes relationships to discover key value
  - for DES, requires analyzing $O(2^{47})$ pairs
- No attacks on DES so far are significantly better than brute force attacks, for comparable cost

AES
Overview

- Selected from an open competition, organized by NSA
  - winner: Rijndael algorithm, standardized as AES
- Some similarities to DES (rounds, round keys, alternate permutation+substitution)
  - but not a Feistel cipher
- Block size = 128 bits
- Key sizes = 128, 192, or 256
- Main criteria: secure, well justified, fast

AES-128 Overview

- 128-bit input
- 128-bit keys
- Q1: What happens in each round?
- Q2: How are round keys generated?

AES-128 State

- Each plaintext block of 16 bytes is arranged as 4 columns of 4 bytes each

Round 1. AES S-Box

- Each byte of state is replaced by a value from following table
  - eg. byte with value 0x95 is replaced by byte in row 9 column 5, which has value 0x2A

One AES-128 Round

1. Apply S-box function to each byte of the state (i.e., 16 substitutions)
2. Rotate…
   - (row 0 of state is unchanged)
   - row 1 of the state left 1 column
   - row 2 of the state left 2 columns
   - row 3 of the state left 3 columns
3. Apply MixColumn function to each column of state
   - last round omits this step

S-Box (Cont’d)

The S-Box is what makes AES a non-linear cipher

For every value of b there is a unique value for b'
- It is faster to use a substitution table (and easier).

\[
x = b^{-1} \text{ in } GF(2^8), \text{i.e., } x \text{ is the inverse of byte } b
\]
S-Box Example

- The S-Box is what makes AES a non-linear cipher

State

\[ \begin{align*}
\text{Before Shift Rows} & \quad \text{After Shift Rows} \\
\text{Before SubBytes} & \quad \text{After SubBytes} \\
\end{align*} \]

Round Step 2. Rotate (Example)

Before Shift Rows

| S3 | CA | 70 | 0C |
| D0 | B7 | D6 | DC |
| 51 | 04 | F8 | 32 |
| 63 | BA | 68 | 79 |

After Shift Rows

| 53 | CA | 70 | 0C |
| B7 | D6 | DC | D0 |
| F8 | 32 | 51 | 04 |
| 79 | 63 | BA | 68 |

Round Step 3. MixColumn Function

- Applied to each column of the state
- For each column, each byte \( a_0 \ldots a_{i+3} \) of the column is used to lookup up four 4-byte intermediate columns \( t_0 \ldots t_{i+3} \) from a table (next slide)
- The intermediate columns \( t_0 \ldots t_{i+3} \) are then combined (next slide + 1):
  - rotate vertically so top octet of \( t_0 \) is in same row as input octet \( a_0 \)
  - XOR the four rotated columns together

MixColumn… (Cont’d)

- Part of the MixColumn table:
  - right (low-order) nibble (4 bits)
  - left (high-order) nibble (4 bits)

Generating Round Keys in AES-128

The key (16 bytes) is arranged in 4 columns of 4 rows, as for the input (plaintext) block.

Deriving the round keys makes use of a table of constants:

- Removes symmetry and linearity from key expansion

<table>
<thead>
<tr>
<th>Round</th>
<th>Constant ( c_i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0x6C</td>
</tr>
<tr>
<td>2</td>
<td>0xA8</td>
</tr>
<tr>
<td>3</td>
<td>0xA8</td>
</tr>
<tr>
<td>4</td>
<td>0x4D</td>
</tr>
<tr>
<td>5</td>
<td>0x9A</td>
</tr>
<tr>
<td>6</td>
<td>0x2F</td>
</tr>
<tr>
<td>7</td>
<td>0x5B</td>
</tr>
<tr>
<td>8</td>
<td>0x9C</td>
</tr>
<tr>
<td>9</td>
<td>0xE3</td>
</tr>
<tr>
<td>10</td>
<td>0xC6</td>
</tr>
</tbody>
</table>
Inverse S-Box

For i\(^{th}\) round of keys, i = 1..10

\[
\text{temp} = \text{column j-1 of (i-1)\(^{th}\) (previous) round}
\]
\[
\text{rotate temp upward one byte}
\]
\[
\text{S-Box transform each byte of temp}
\]
\[
\text{XOR first byte of temp with c,}
\]

for column index j = 1..3

\[
\text{temp} = \text{column j-1 of i\(^{th}\) (this) round}
\]
\[
\text{result} = \text{temp XOR} \text{column j-1 of i\(^{th}\) (previous) round}
\]

Key Expansion Rationale

- Designed to resist known attacks
- Design criteria include
  - knowing part of the key doesn’t make it easy to
    find entire key
  - key expansion must be invertible, but enough non-
    linearity to hinder analysis
  - should be fast to compute, simple to describe and
    analyze
  - key bits should be diffused into the round keys

Mathematics

AES Operates on the binary field \(GF(2^8)\)

- this can be represented as a polynomial \(b(x)\) with
  binary coefficients \(b \in \{0,1\}\):
  \[
b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0
\]

Multiplication in \(GF(2^8)\) consists of multiplying
  two polynomials modulo an irreducible
  polynomial of degree 8

- AES uses the following irreducible polynomial
  \[
m(x) = x^4 + x^3 + x^2 + x + 1
\]

†

In this context, \(b(x)\) is a polynomial over the finite field \(GF(2^8)\), representing an element of the field. The multiplication of two polynomials in this field is done by polynomial long division, taking into account the irreducible polynomial \(m(x)\) as the modulus. This is a key aspect in the definition of AES operations, particularly in the MixColumns operation.

AES-128 Decryption (Conceptual)

- Run cipher in reverse, with inverse of each operation replacing the encryption operations
- Inverse operations:
  - XOR is its own inverse
  - inverse of S-box is just the inverse table (next slide)
  - inverse of rotation in one direction is rotation in other direction
  - inverse of MixColumn is just the inverse table (next slide + 1)
AES Decryption (Actual)

- Run cipher in forward direction, except...
  - use inverse operations
  - apply round keys in reverse order
  - apply InvMixColumn to round keys K1..K9
- Decryption takes more memory and cycles encryption
  - can only partially reuse hardware for encryption

AES Assessment

- Speed: about 16 clock cycles/byte on modern 32-bit CPUs
  - 200 MByte/s on a PC, no special hardware!
- No known successful attacks on full AES
  - best attacks work on 7-9 rounds (out of 10-14 rounds)
- Clean design
  - For brute force attacks, AES-128 will take $4 \times 10^{21} X \approx 2^{72}$ more effort than DES

Attacks on AES

Differential Cryptanalysis: based on how differences in inputs correlate with differences in outputs
  - greatly reduced due to high number of rounds

Linear Cryptanalysis: based on correlations between input and output
  - S-Box & MixColumns are designed to frustrate Linear Analysis

Side Channel Attacks: based on peculiarities of the implementation of the cipher

Side Channel Attacks

Timing Attacks: measure the time it takes to do operations
  - some operations, with some operands, are much faster than other operations, with other operand values
  - provides clues about what internal operations are being performed, and what internal data values are being produced

Power Attacks: measures power to do operations
  - changing one bit requires considerably less power than changing many bits in a byte

Summary

- Secret key crypto is (a) good quality, (b) faster to compute than public key crypto, and (c) the most widely used crypto
- DES strong enough for non-critical applications, but triple-DES is better
- AES even better (stronger and much faster), has versions with 128-, 192-, and 256-bit keys
- Secret key crypto requires “out-of-band”, bilateral key negotiation/agreement