Lecture 2: Blockcipher

Viêt Tùng Hoang

The slides are loosely based on those of Prof. Mihir Bellare, UC San Diego.
Agenda

1. Blockcipher and Key Recovery

2. A Bird’s-Eye View of Real Blockciphers
Blockcipher

efficiently invertible given the key

$E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$

Key space  Domain

$K \xrightarrow{E} C \xrightarrow{E^{-1}} M$
Blockcipher Usage

Random key $K$ is known to both parties, but not given to adversary $A$.
Key-Recovery Attack: Scenario

\[ C_1 \leftarrow E_K(M_1) \quad \ldots \quad C_q \leftarrow E_K(M_q) \]

Guess \( K \)

\[ M_1 \quad \ldots \quad M_q \]
Modeling Key-Recovery Attack

**Game** $KR_E$

**procedure** Initialize()

$K \iff \mathcal{K}$

**procedure** Enc($M$)

return $E_K(M)$

**procedure** Finalize($K'$)

return $(K' = K)$

$Adv^\text{kr}_E(A) = \Pr[KR_E \Rightarrow 1]$

$Adv^\text{kr}_E(A) \approx 0$ means $A$ is doing poorly
Practicing Key-Recovery Attack

\[ E_K(M) = M \oplus K \]

\[ E_K(M) = \pi(M \oplus K) \]

\( \pi, \pi^{-1} \) are public

Public permutation
Agenda

1. Blockcipher and Key Recovery

2. A Bird’s-Eye View of Real Blockciphers
DES: Parameters and History

- Designed by IBM in 1974
- Used in ATM machines
- Replaced in 2001
Design of DES: Feistel Network

(One-round) Feistel($K, \cdot$)

Inverse of Feistel

**Question**: How to invert?
Construction of DES

56 bits

\( K \)

Key scheduler

48 bits

\( K_1 \) \ldots \( K_{16} \)

Unkeyed processing

\( M \)

\[ \text{Process}(\cdot) \]

\[ \text{Feistel}(K_1, \cdot) \]

\[ \ldots \]

\[ \text{Feistel}(K_{16}, \cdot) \]

\[ \text{Process}^{-1}(\cdot) \]

\( C \)
Exhaustive Key Search Attack

For \( K \in \mathcal{K} \) do

If \( E_K(M_i) = C_i \) for every \( i \in \{1, \ldots, d\} \) then return \( K \)

For \( E : \{0, 1\}^k \times \{0, 1\}^n \to \{0, 1\}^n \), if \( d > k/n \) then \( \text{Adv}^k_E(A) \approx 1 \)
### Exhaustive Key Search Attack on DES

<table>
<thead>
<tr>
<th>Timeline</th>
<th>Source</th>
<th>Attack time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1997</td>
<td>DESCHALL</td>
<td>96 days</td>
</tr>
<tr>
<td>1998</td>
<td>Distributed.NET</td>
<td>41 days</td>
</tr>
<tr>
<td>1998</td>
<td>EFF</td>
<td>56 hours</td>
</tr>
<tr>
<td>1998</td>
<td>Distributed.NET + EFF</td>
<td>22 hours</td>
</tr>
</tbody>
</table>
Incorrect Fix of DES: Double Encryption

112-bit key → prohibitive for exhaustive key search

But there’s a more clever attack!
Meet-in-the-Middle Attack

\[ M \xrightarrow{E_{K_1}} E_{K_1}(M) \xrightarrow{E_{K_2}} E_{K_2}(C) \xrightarrow{E_{K_2}^{-1}} C \]
Meet-in-the-Middle Attack

Let \( L_1, \ldots, L_N \) be all possible DES keys

\[ N = 2^{56} \]

\[
\begin{array}{|c|c|}
\hline
L_1 & E_{L_1}(M) \\
\hline
\vdots & \vdots \\
L_i & E_{L_i}(M) \\
\vdots & \vdots \\
L_N & E_{L_N}(M) \\
\hline
\end{array}
\]

\[
\begin{array}{|c|c|}
\hline
E_{L_1}^{-1}(C) & L_1 \\
\hline
\vdots & \vdots \\
E_{L_i}^{-1}(C) & L_j \\
\vdots & \vdots \\
E_{L_N}^{-1}(C) & L_N \\
\hline
\end{array}
\]

Find \( L_i, L_j \) such that \( E_{L_i}(M) = E_{L_j}^{-1}(C) \)

Can use further testing with Enc to eliminate false positives

By using hashing, can find the matching in \( O(N) \) time
The 3DES Constructions

**3DES2**

- $E_{K_1}$
- $E_{K_2}^{-1}$
- $E_{K_1}$

**3DES3**

- $E_{K_1}$
- $E_{K_2}^{-1}$
- $E_{K_3}$
Block Size Matters, Too

Birthday attack: $O(2^{n/2})$ time

Distinguish outputs from random

Practical for DES/2DES/3DES

$n = 64$
State of the Art: AES

- NIST standard since 2001
- Best known key-recovery attack takes about $2^{126}$ time

$k \in \{128, 192, 256\}$

$n = 128$
Security Against Key Recovery Is Not Enough

A Bad Example: Consider the following $E : \{0, 1\}^{128} \times \{0, 1\}^{256} \rightarrow \{0, 1\}^{256}$

$$E_K(M_1M_2) = \text{AES}_K(M_1) || M_2$$

As secure against key recovery as AES

Send half of the message in the clear!
So What Is a Good Blockcipher?

<table>
<thead>
<tr>
<th>Possible Properties</th>
<th>Necessary</th>
<th>Sufficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security against key recovery</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Hard to find $M$ given $C \leftarrow E_K(M)$</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Want:** a single “master” property that is sufficient to ensure security of common usage of blockcipher.