CSE 207B:
Applied Cryptography

Nadia Heninger
UCSD

Fall 2023 Lecture 3
Last time: Stream ciphers

This time: Block ciphers
Definition (Block cipher)

- Deterministic cipher (Enc, Dec)
- Message space = ciphertext space = $X$, key space = $K$
- Fix $k \in K$, $F_k : X \rightarrow X$
- $F_k^{-1}$ exists
- $\text{Enc}_k(m) = F_k(m)$
- $\text{Dec}_k(c) = F_k^{-1}(c)$
Security for block ciphers

A secure block cipher should be computationally indistinguishable from a truly random permutation.

A random permutation can be represented as a lookup table:

<table>
<thead>
<tr>
<th>$x$</th>
<th>$f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>$2^{128}$ - 1</td>
<td>$2^{128}$</td>
</tr>
</tbody>
</table>

Problem: not efficient to store.
Distinguishing experiment for block ciphers

Definition

$F_k$ is a secure block cipher if $\forall$ efficient $D$

$$\left| \Pr[D(F_k) = 1] - \Pr[D(f) = 1] \right| \text{ negligible}$$
Security against brute force attacks

**Candidate attack:** Enumerate all keys $k$ until you find one such that $F_k(x_i) = \text{Enc}(x_i)$ for all queried $x_i$.

- Implication 1: $|K|$ must be super-polynomial to resist attack.
- Implication 2: Only need 2 queries in order for unique $k$ whp.
Using a block cipher for encryption

Obvious idea for one block:
- $\text{Enc}_k(m) = F_k(m)$
- $\text{Dec}_k(c) = F_k^{-1}(c)$

Obvious but insecure idea for multiple block:
- $\text{Enc}_k(m_1||m_2||\ldots||m_\ell) = F_k(m_1)||F_k(m_2)||\ldots||F_k(m_\ell)$
- $\text{Dec}_k(c_1||c_2||\ldots||c_\ell) = F_k^{-1}(c_1)||F_k^{-1}(c_2)||\ldots||F_k^{-1}(c_\ell)$

This is called “Electronic Code Book” (ECB) mode.
Is ECB mode secure?

• For one block?
Is ECB mode secure?

• For one block?

ECB mode is semantically secure if a message is one block.
Is ECB mode secure?

- For one block?
  
  ECB mode is semantically secure if a message is one block.

- For many blocks?
Is ECB mode secure?

• For one block?

ECB mode is semantically secure if a message is one block.

• For many blocks?

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
Hackers recently leaked 153 million Adobe user emails, encrypted passwords, and password hints.

Adobe encrypted the passwords improperly, misusing block-mode 3DES. The result is something wonderful:

<table>
<thead>
<tr>
<th>USER PASSWORD</th>
<th>HINT</th>
</tr>
</thead>
<tbody>
<tr>
<td>4e18acc1ab76a2d6</td>
<td>WEATHER VANE SWORD</td>
</tr>
<tr>
<td>4e18acc1ab76a2d6</td>
<td>NAME1</td>
</tr>
<tr>
<td>8abb6279e06e6d</td>
<td>DUH</td>
</tr>
<tr>
<td>8abb6279e06e6d</td>
<td>57</td>
</tr>
<tr>
<td>8abb6279e06e6d</td>
<td>FAVORITE OF 12 APOSTLES</td>
</tr>
<tr>
<td>85c9da8a8a7ac</td>
<td>WITH YOUR OWN HAND YOU HAVE DONE ALL THIS</td>
</tr>
<tr>
<td>4e18acc1ab76a2d6</td>
<td>SEXY EARLOBES</td>
</tr>
<tr>
<td>4e18acc1ab76a2d6</td>
<td>BEST TOS EPISODE</td>
</tr>
<tr>
<td>1ab29e86d6e5ca</td>
<td>SUGARLAND</td>
</tr>
<tr>
<td>1ab29e86d6e5ca</td>
<td>NAME + JERSEY #</td>
</tr>
<tr>
<td>877eb789d3862b1</td>
<td>ALPHA</td>
</tr>
<tr>
<td>877eb789d3862b1</td>
<td>OBVIOUS</td>
</tr>
<tr>
<td>877eb789d3862b1</td>
<td>MICHAEL JACKSON</td>
</tr>
<tr>
<td>38a7c9279codeb44</td>
<td>HE DID THE MASH, HE DID THE PURLOINED</td>
</tr>
<tr>
<td>38a7c9279codeb44</td>
<td>FAVI LATTER-3 POKEMON</td>
</tr>
</tbody>
</table>

The greatest crossword puzzle in the history of the world

https://xkcd.com/1286/
Move Fast & Roll Your Own Crypto
A Quick Look at the Confidentiality of Zoom Meetings

By Bill Marczak and John Scott-Railton April 3, 2020

This report examines the encryption that protects meetings in the popular Zoom teleconference app. We find that Zoom has “rolled their own” encryption scheme, which has significant weaknesses. In addition, we identify potential areas of concern in Zoom’s infrastructure, including observing the transmission of meeting encryption keys through China.

Key Findings

- Zoom documentation claims that the app uses “AES-256” encryption for meetings where possible. However, we find that in each Zoom meeting, a single AES-128 key is used in ECB mode by all participants to encrypt and decrypt audio and video. The use of ECB mode is not recommended because patterns present in the plaintext are preserved during encryption.

Theorem

ECB mode applied to distinct message blocks is semantically secure.

Proof idea.

The encryption of a sequence of distinct data blocks looks like a sequence of random data blocks.
Block cipher design: substitution-permutation network

Ideal properties:
- “diffusion”: mix inputs with permutations, xor
- “confusion”: nonlinearity, S-boxes

One round is insecure: Key recovery from a single known plaintext pair.
Feistel network
IBM, early 1970s

- Key schedule: Key expanded deterministically into many round keys
- Round function: DES round function $f$ composed of permutations, xor, and S-boxes
Data Encryption Standard (DES)

- Cipher design standardized by NIST in 1977
- Designed by IBM with input from NSA
- “We sent the S-boxes off to Washington. They came back and were all different.” –Alan Konheim, one of the designers
- NSA also pushed to decrease key size from 64 to 56 bits
- Late 1980s: Biham and Shamir rediscover differential cryptanalysis and discover that changes to S-boxes made DES resistant to attack
- 1997: DES challenges solved by distributed computation
- 1998: Deep Crack project breaks DES in 56 hours for $250,000 of special-purpose hardware
- 2007: COPACOBANA can brute force DES in 13 days with FPGAs
Attempting to adapt DES to make it more secure

**Obvious idea:** Why not just encrypt twice?

\[ 2\text{DES}_{k_1,k_2}(m) = \text{DES}_{k_2}(\text{DES}_{k_1}(m)) \]

Naively expect \((k_1, k_2)\) to have 112 bit strength, thus resist exhaustive search.
Meet-in-the-middle attacks

Input: \((m, c = 2\text{DES}_{k_1,k_2}(m))\)

1. For all \(k_i \in \{0,1\}^n\), compute \(z_i = \text{DES}_{k_i}(m)\), store \((z_i, k_i)\).
2. For all \(k_j \in \{0,1\}^n\), compute \(z_j = \text{DES}_{k_j}^{-1}(c)\), store \((z_j, k_j)\).
3. For every match \(z_i = z_j\), have a candidate key \((k_i, k_j)\).
Analysis of meet-in-the-middle attack on 2DES

- DES has key size 56 bits
- Block length 64 bits

\[ \Pr[(k_i, k_j) \text{ is a match}] = 2^{-64} \]

\[ \mathbb{E}[\# \text{ of matches}] = 2^{2 \times 56} \cdot 2^{-64} = 2^{48} \]

After a small number of input/output pairs, narrow down to 1 key pair.

**Cost analysis** for \( m \) input pairs:

1. \( 2m2^n \) encryptions.
2. \( 2mn2^n \) storage.
3DES

\[ 3DES_{k_1,k_2,k_3}(m) = DES_{k_3}(DES_{k_2}^{-1}(DES_{k_1}(m))) \]

Why alternate? If \( k_1 = k_2 = k_3 \) this is equivalent to DES.
AES (Advanced Encryption System)

- Chosen in 2000 after a NIST-run competition.
- Rijndael (Joan Daemen, Vincent Rijmen)
- 128, 192, 256-bit versions
- 10 rounds
- Sub-steps of each round designed for lookup tables
- Best attack: $2^{126.1}$ time
Homework 2 is online! Due in 1.5 weeks.