

CSE 207B: Applied Cryptography

Nadia Heninger

UCSD

Fall 2025 Lecture 3

Last time: Stream ciphers

This time: Block ciphers

Block ciphers

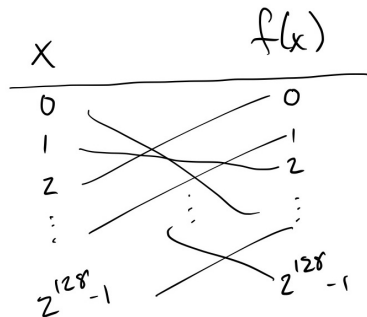
Definition (Block cipher)

- 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

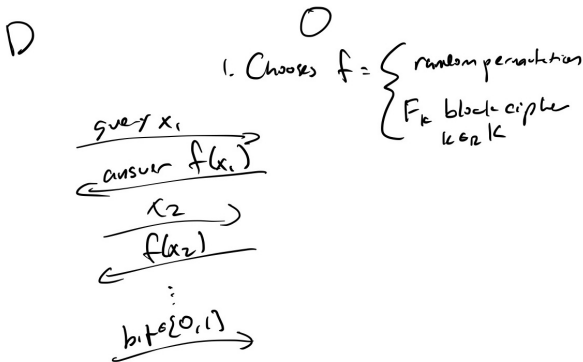
A secure block cipher should be computationally indistinguishable from a truly random permutation.

A random permutation can be represented as a lookup table:



Problem: not efficient to store.

Distinguishing experiment for block ciphers



Definition

F_k is a secure block cipher if \forall efficient D

$$|\Pr[D(F_k) = 1] - \Pr[D(f) = 1]| \text{ negligible}$$

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:

- $\text{Enc}_k(m_1 || m_2 || \dots || m_\ell) = F_k(m_1) || F_k(m_2) || \dots || F_k(m_\ell)$
- $\text{Dec}_k(c_1 || c_2 || \dots || c_\ell) = F_k^{-1}(c_1) || F_k^{-1}(c_2) || \dots || F_k^{-1}(c_\ell)$

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?

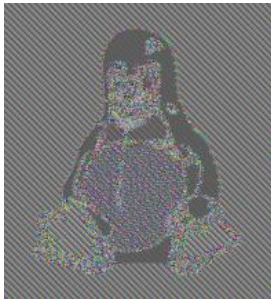
- For one block?

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

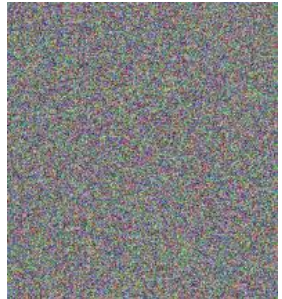
- For many blocks?



m



ECB mode



Secure encryption

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:

USER	PASSWORD	HINT
4e18acc1ab27a2d6		WEATHER VANE SWORD
4e18acc1ab27a2d6		
4e18acc1ab27a2d6	a0e2876eb1ea1fca	NAME 1
8babb6279e06e66d		DUH
8babb6279e06e66d	a0e2876eb1ea1fca	
8babb6279e06e66d	85e9da81a3a78adc	57
4e18acc1ab27a2d6		FAVORITE OF 12 APOSTLES
1ab29ae86dab6e5ca	7a2d6a0a2876eb1e	WITH YOUR OWN HAND YOU HAVE DONE ALL THIS
a1f9b2b6299e7a2b	e0dec1e6ab797397	SEXY EARLOBES
a1f9b2b6299e7a2b	617ab027727ad85	BEST TOS EPISODE
39738b7adb0baaf7	617ab027727ad85	SUGARLAND
1ab29ae86dab6e5ca		NAME + JERSEY #
877ab7889d3862b1		ALPHA
877ab7889d3862b1		
877ab7889d3862b1		
877ab7889d3862b1		OBVIOUS
877ab7889d3862b1		MICHAEL JACKSON
38a7c9279codeb44	9dca1d79d4dec6d5	
38a7c9279codeb44	9dca1d79d4dec6d5	HE DID THE MASH, HE DID THE
38a7c9279codeb44		PURLAINED
a8ae5785c767a7e7a	9dca1d79d4dec6d5	SAV LATER 3 POKEMON

THE GREATEST CROSSWORD PUZZLE
IN THE HISTORY OF THE WORLD

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.

<https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/>

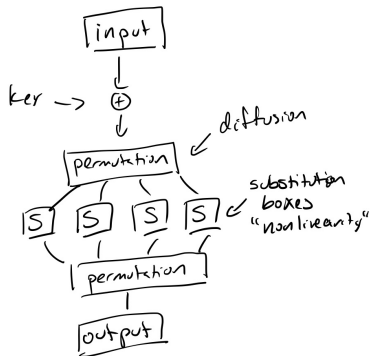
Theorem

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



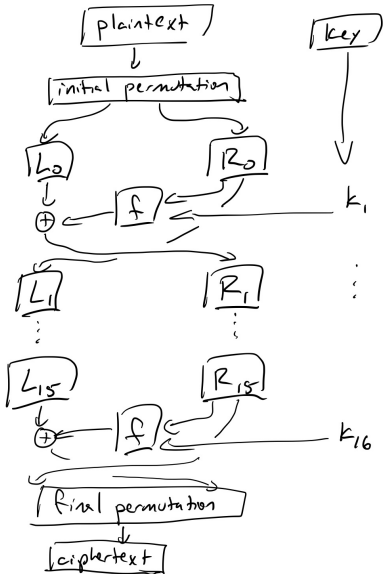
Ideal properties:

- “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

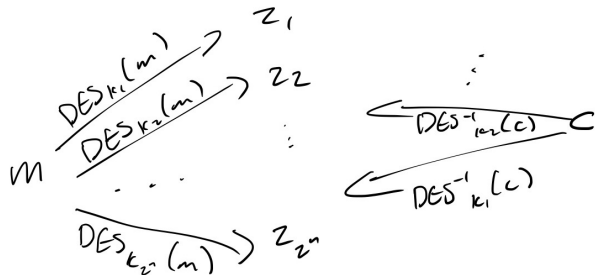
Obvious idea: Why not just encrypt twice?

$$2DES_{k_1, k_2}(m) = DES_{k_2}(DES_{k_1}(m))$$

Naively expect (k_1, k_2) to have 112 bit strength, thus resist exhaustive search

Meet-in-the-middle attacks

Input: $(m, c = 2DES_{k_1, k_2}(m))$



1. For all $k_i \in \{0, 1\}^n$, compute $z_i = DES_{k_i}(m)$, store (z_i, k_i) .
2. For all $k_j \in \{0, 1\}^n$, compute $z_j = DES_{k_j}^{-1}(c)$, 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

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

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

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.

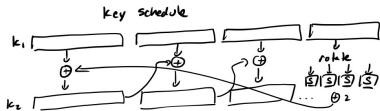
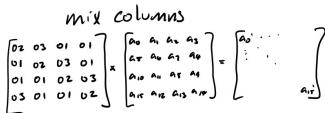
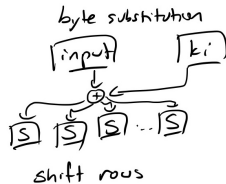
3DES

$$3DES_{k_1, k_2, k_3}(m) = DES_{k_3}(DES_{k_2}^{-1}(DES_{k_1}(m)))$$

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.