Introduction to Cryptography and Information Security
UEE4611, Spring Semester 2020

Ching-Yi Lai
Institute of Communications Engineering
National Chiao Tung University

Chapter 7: Block Cipher Operation

- Multiple Encryption and Triple DES
- Electronic Codebook
- Cipher Block Chaining Mode
- Cipher Feedback Mode
- Output Feedback Mode
- Counter Mode
- XTS-AES Mode for Block-Oriented Storage Devices
- Format-Preserving Encryption

Multiple Encryption & Triple DES

(data encryption standard)

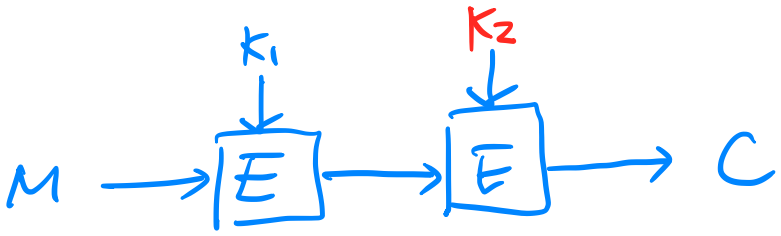
$DES: \{0,1\}^{64} \times \{0,1\}^{56} \rightarrow \{0,1\}^{64}$

key: 56 bits. $2^{56} = 7.2 \times 10^{16}$.

suffer to brute force attack today.

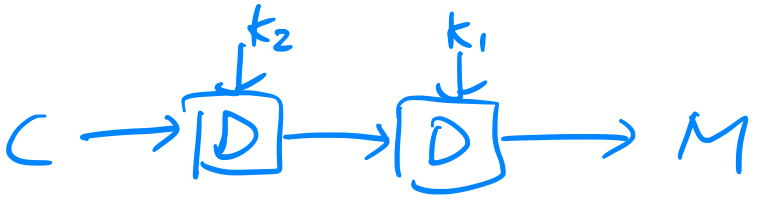
Double Encryption

k_i : 56 bits



$C = E(E(M, k_1), k_2) \stackrel{?}{=} E(M, k_3)$

$|k_3| = 56$.



$M = D(D(C, k_2), k_1)$.

key length = $56 \times 2 = 112$ bits.

Not equivalent to a single-stage DES.

[CAMP 92].

Meet-in-the-Middle Attack

Given a pair (M, C), $C = E(E(M, K_1), K_2)$
try to find the unknown keys K_1, K_2.

1. Construct a table with $E(M, K)$ $\forall K \in \{0,1\}^{56}$
2. Construct a table with $D(C, K)$ $\forall K \in \{0,1\}^{56}$
   $O(2^{56})$
3. If a match occurs, then test the two resulting keys against a new known plaintext-ciphertext pair.
   If the two keys produce the correct ciphertext, accept them as the correct keys.

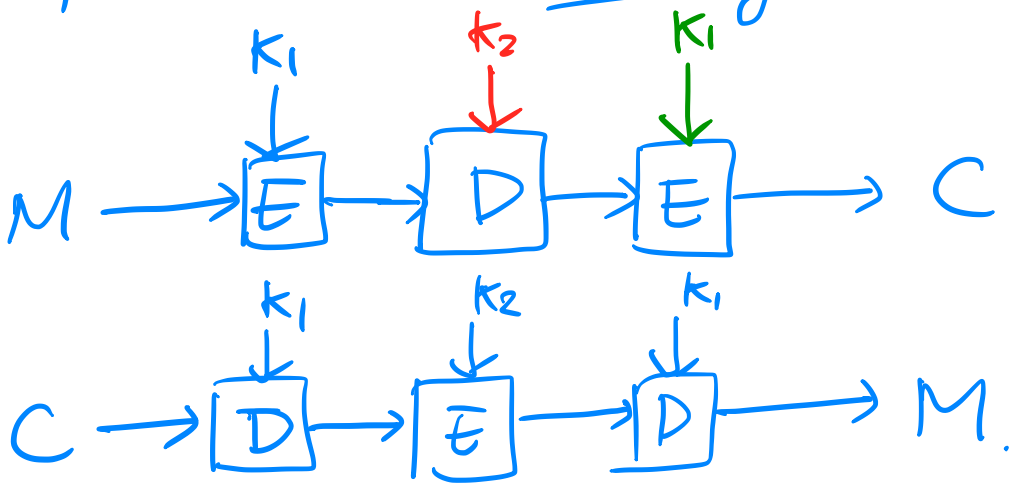
Given a plaintext M, there are 2^{64} possible ciphertexts.

There are 2^{112} keys. Thus $2^{112}/2^{64} = 2^{48}$ keys may produce the same plaintext-ciphertext pair, but only one of them is the correct pair.

The additional known plaintext-ciphertext can reduce the false alarm rate to $2^{48}/2^{64} = 2^{-16}$.

The probability that the correct keys are determined is $1 - 2^{-16}$.

Triple DES with two keys K_1, K_2.



This allows the users of 3DES to decrypt data encrypted by users of the older single DES.

No practical cryptanalytic attack on 3DES

brute force: $2^{112} \sim 5 \times 10^{33}$.

Block cipher $\{0,1\}^b \times \{0,1\}^k \rightarrow \{0,1\}^b$.

If we have a plaintext longer than b,

$\Rightarrow$ break it into b-bit blocks and then encrypt each block using the same key.

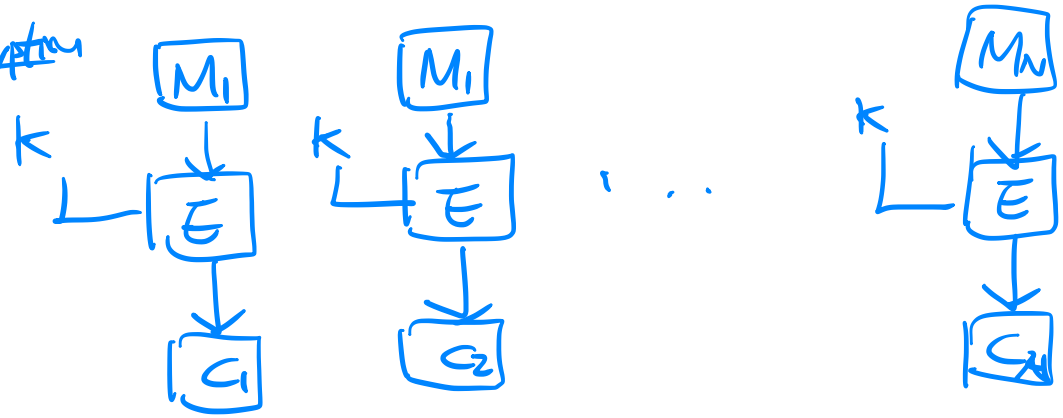
But a number of security issues arise when multiple blocks of plaintext are encrypted using the same key.

NIST: five modes of operations.

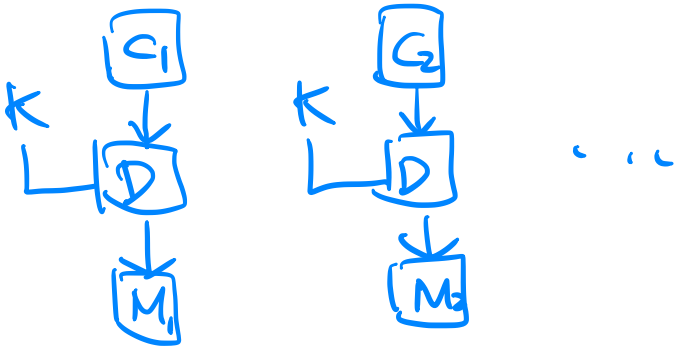
Electronic Codebook (ECB)

$M = M_1 M_2 \cdots M_N$. $|M_i| = b$.

Encryption



Decryption



The same key is used.

Table 3.5 Average Time Required for Exhaustive Key Search

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$26! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

Table 7.1 Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

NIST