Other Block Ciphers

Huỳnh Trọng Thưa
htthua@ptithcm.edu.vn

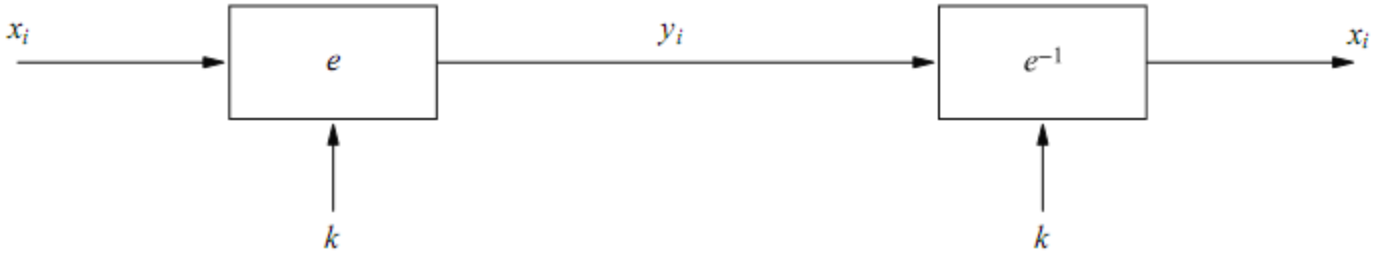
What will we learn?

- The most important modes of operation for block ciphers in practice
- Security pitfalls when using modes of operations
- The principles of key whitening
- Why double encryption is not a good idea, and the meet-in-the-middle attack
- Triple encryption

Encryption with Block Ciphers: Modes of Operation

- Electronic Code Book mode (ECB),
- Cipher Block Chaining mode (CBC),
- Cipher Feedback mode (CFB),
- Output Feedback mode (OFB),
- Counter mode (CTR).

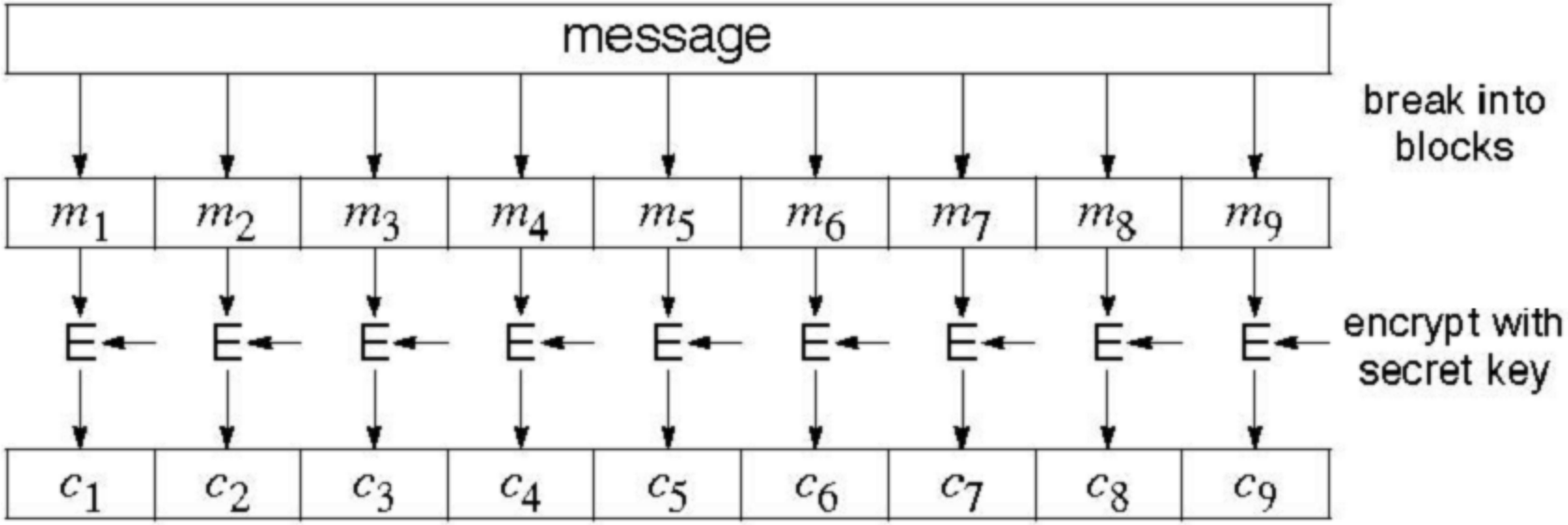
Electronic Codebook Mode (ECB)



Let $e()$ be a block cipher of block size b, and let x_i and y_i be bit strings of length b.

Encryption: $y_i = e_k(x_i), \quad i \geq 1$

Decryption: $x_i = e_k^{-1}(y_i) = e_k^{-1}(e_k(x_i)), \quad i \geq 1$



ECB critics

- Advantages
  - Block synchronization is not necessary.
- Problem
  - identical plaintext blocks result in identical ciphertext blocks, as long as the key does not change
  - Replay attack
- Usage:
  - not recommended to encrypt more than one block of data
  - encryption in database

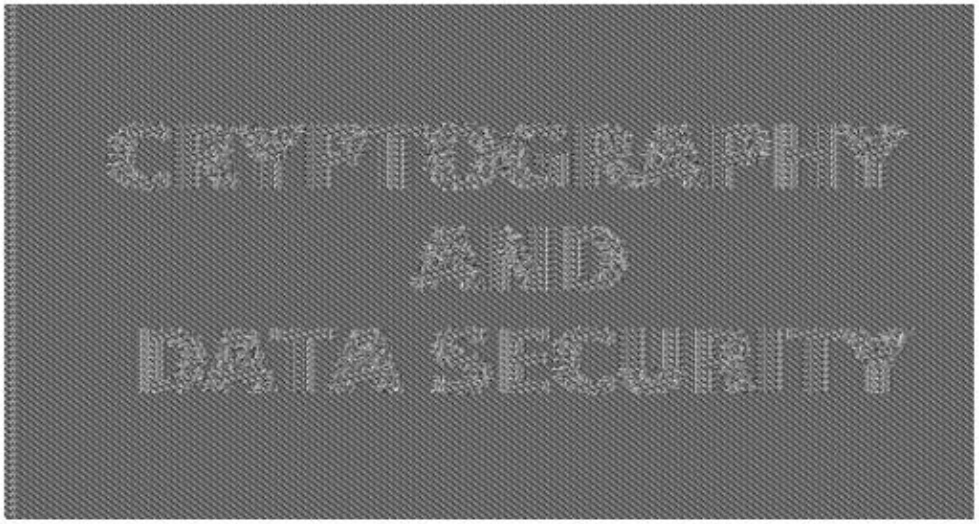
Ex of Substitution attack against electronic bank transfer

Block #	1	2	3	4	5
	Sending Bank A	Sending Account #	Receiving Bank B	Receiving Account #	Amount $

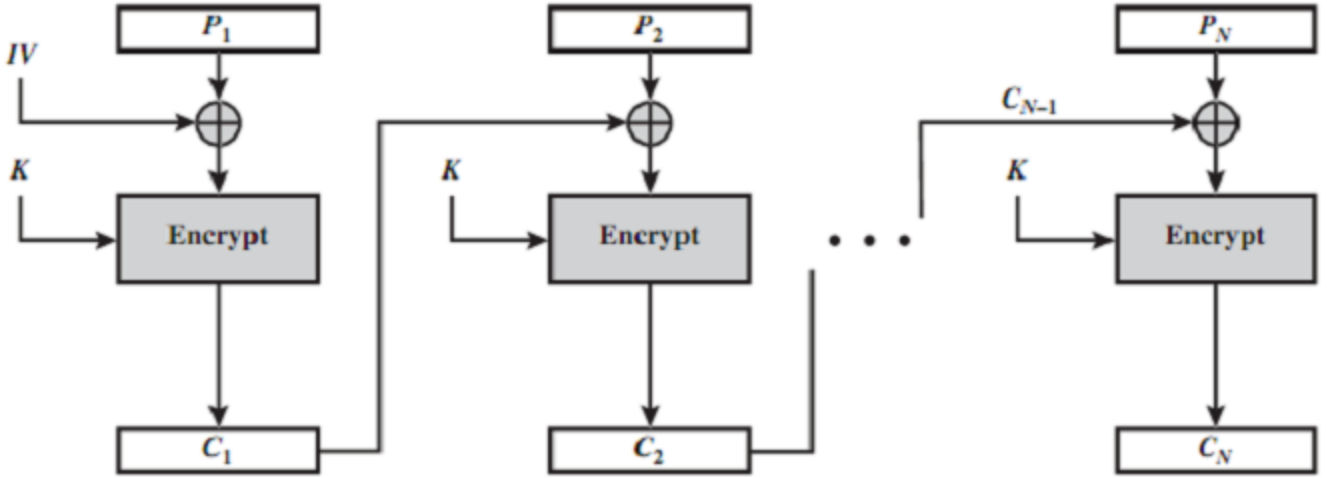
- Oscar observes the ciphertexts going through the communication network.
- After a while he can recognize the five blocks of his own transfer. He now stores blocks 1, 3 and 4 of these transfers.
- The same key is used for several other transfers between bank A and B.
- By comparing blocks 1 and 3 of all subsequent messages with the ones he has stored, Oscar recognizes all transfers that are made from some account at bank A to some account at bank B.
- He now simply replaces block 4 — which contains the receiving account number — with the block 4 that he stored before.

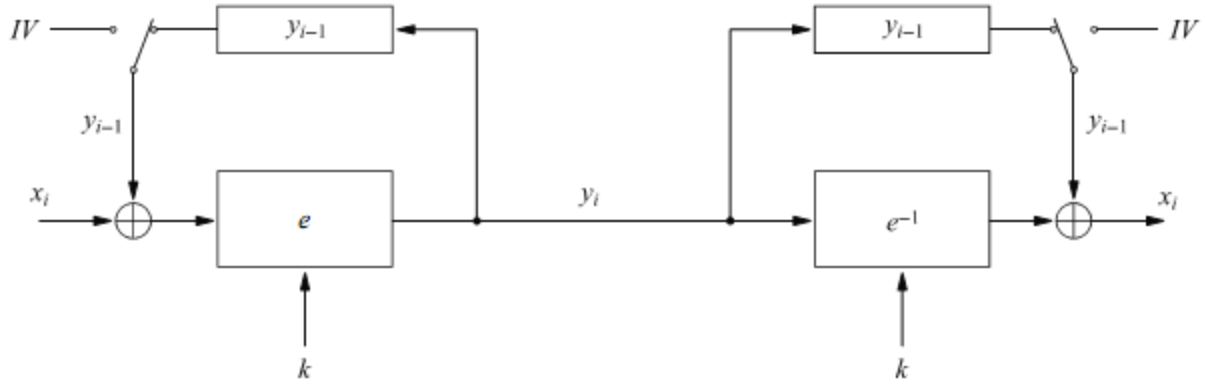
Encryption of bitmaps in ECB mode

CRYPTOGRAPHY
AND
DATA SECURITY



Cipher Block Chaining Mode (CBC)





CBC critics

Let $e()$ be a block cipher of block size b; let x_i and y_i be bit strings of length b; and IV be a nonce of length b.

Encryption (first block): $y_1 = e_k(x_1 \oplus IV)$

Encryption (general block): $y_i = e_k(x_i \oplus y_{i-1}), \quad i \geq 2$

Decryption (first block): $x_1 = e_k^{-1}(y_1) \oplus IV$

Decryption (general block): $x_i = e_k^{-1}(y_i) \oplus y_{i-1}, \quad i \geq 2$

$$d(y_1) = e_k^{-1}(y_1) \oplus IV = e_k^{-1}(e_k(x_1 \oplus IV)) \oplus IV = (x_1 \oplus IV) \oplus IV = x_1$$

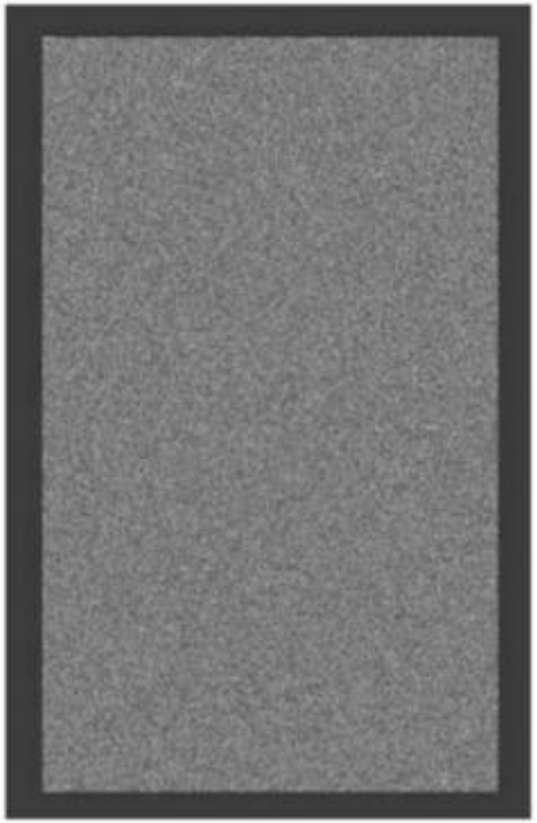
Decryption of all subsequent blocks y_i, $i \geq 2$

$$d(y_i) = e_k^{-1}(y_i) \oplus y_{i-1} = e_k^{-1}(e_k(x_i \oplus y_{i-1})) \oplus y_{i-1} = (x_i \oplus y_{i-1}) \oplus y_{i-1} = x_i$$

CBC critics (cont.)

- Good
  - Randomized encryption: repeated text gets mapped to different encrypted data.
  - A ciphertext block depends on all preceding plaintext blocks blocks
    - reorder affects decryption
- Bad
  - Errors in one block propagate to two blocks
  - Sequential encryption, cannot use parallel hardware

Encryption of bitmaps in CBC mode



Output Feedback Mode (OFB)

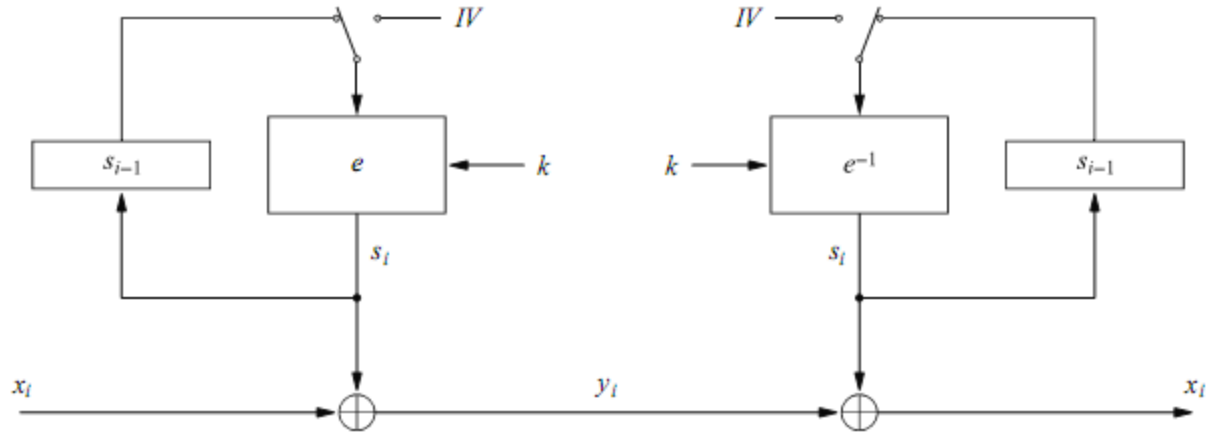
Let $e()$ be a block cipher of block size b; let x_i, y_i and s_i be bit strings of length b; and IV be a nonce of length b.

Encryption (first block): $s_1 = e_k(IV)$ *and* $y_1 = s_1 \oplus x_1$

Encryption (general block): $s_i = e_k(s_{i-1})$ *and* $y_i = s_i \oplus x_i, \quad i \geq 2$

Decryption (first block): $s_1 = e_k(IV)$ *and* $x_1 = s_1 \oplus y_1$

Decryption (general block): $s_i = e_k(s_{i-1})$ *and* $x_i = s_i \oplus y_i, \quad i \geq 2$



Key stream is not generated bitwise but instead in a blockwise fashion.

Cipher Feedback Mode (CFB)

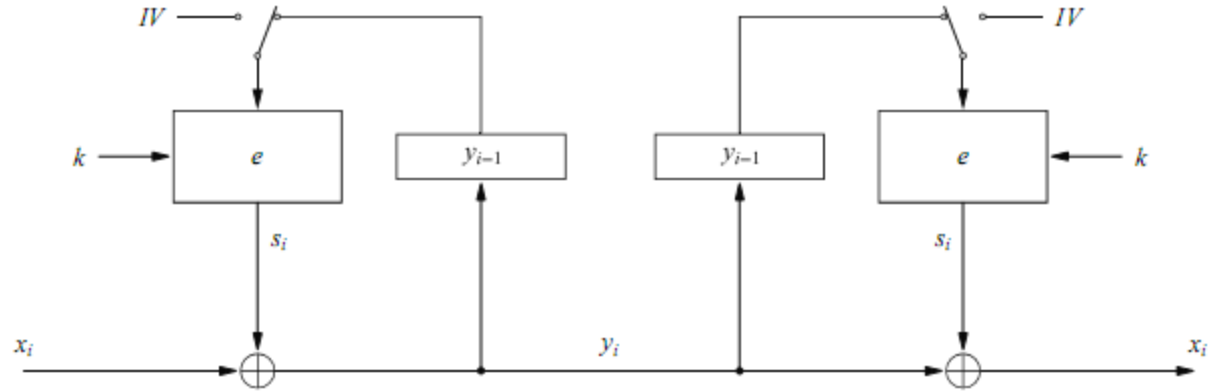
Let $e()$ be a block cipher of block size b; let x_i and y_i be bit strings of length b; and IV be a nonce of length b.

Encryption (first block): $y_1 = e_k(IV) \oplus x_1$

Encryption (general block): $y_i = e_k(y_{i-1}) \oplus x_i, \quad i \geq 2$

Decryption (first block): $x_1 = e_k(IV) \oplus y_1$

Decryption (general block): $x_i = e_k(y_{i-1}) \oplus y_i, \quad i \geq 2$

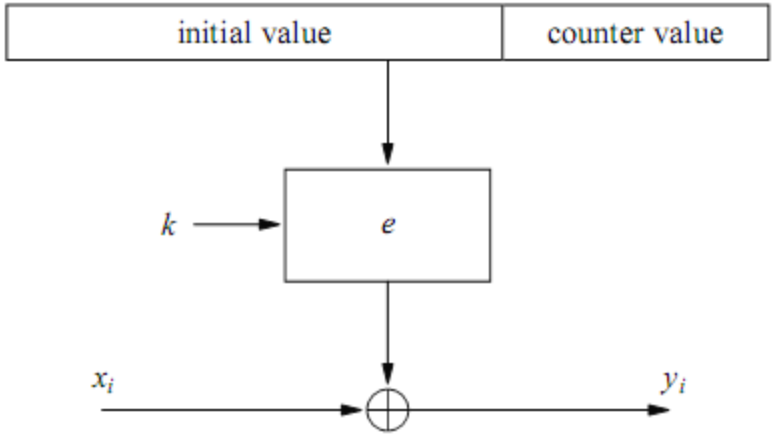


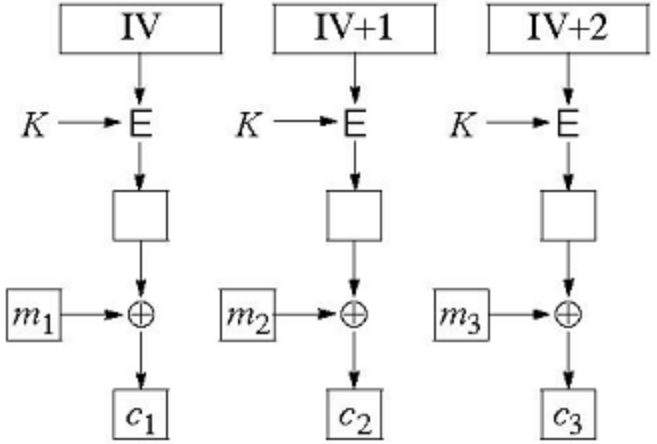
Counter Mode (CTR)

Let $e()$ be a block cipher of block size b, and let x_i and y_i be bit strings of length b. The concatenation of the initialization value IV and the counter CTR_i is denoted by $(IV||CTR_i)$ and is a bit string of length b.

Encryption: $y_i = e_k(IV||CTR_i) \oplus x_i, \quad i \geq 1$

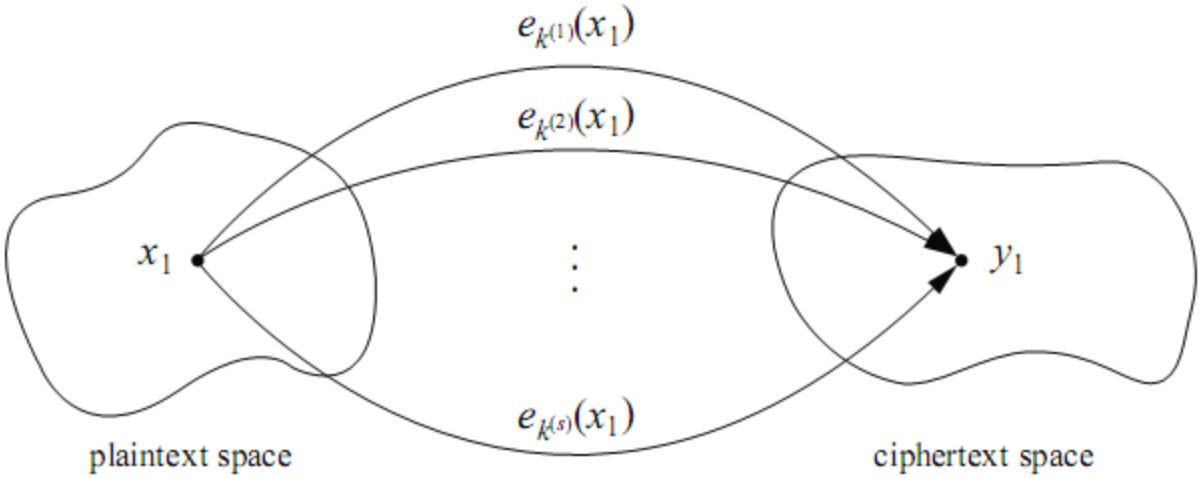
Decryption: $x_i = e_k(IV||CTR_i) \oplus y_i, \quad i \geq 1$





Exhaustive Key Search Revisited

- A brute-force attack can produce false positive results. $DES_{k_i}(x_1) \stackrel{?}{=} y_1, \quad i = 0, 1, \ldots, 2^{56} - 1$
- Ex: A cipher with a block width of 64 bit and a key size of 80 bit. we find on average $2^{80}/2^{64} = 2^{16}$ keys that perform the mapping $e_k(x1) = y1$.



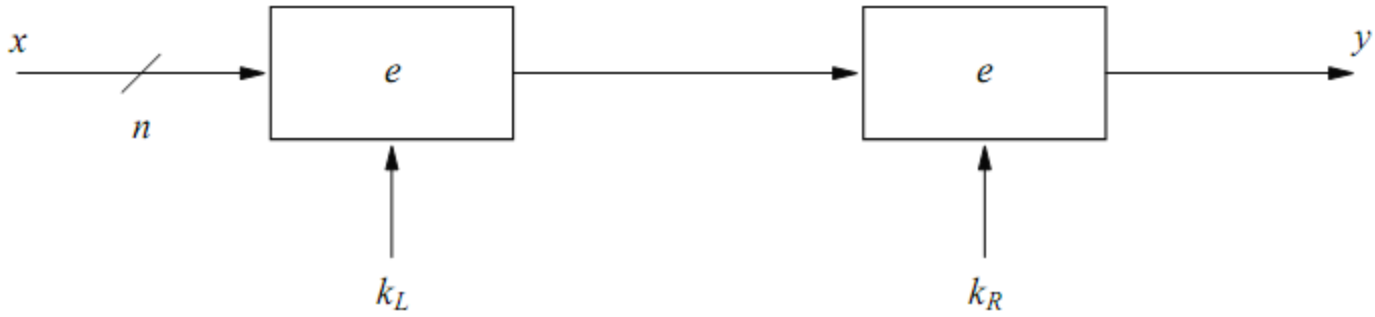
Multiple keys map between one plaintext and one ciphertext

Increasing the Security of Block Ciphers

- Multiple encryption
  - Double Encryption
  - Triple Encryption
  - Problem: Meet-in-the-Middle Attack
- Key whitening

Double Encryption and Meet-in-the-Middle Attack

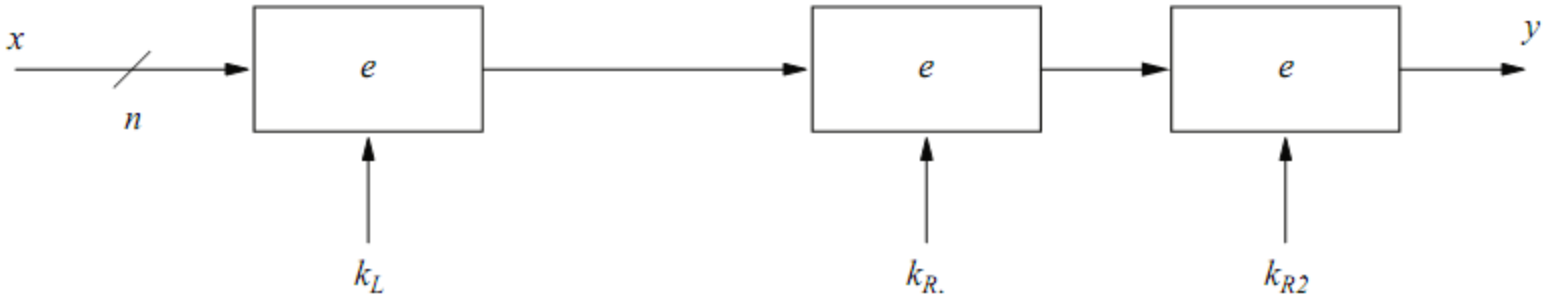
- Key length: κ bits
- Brute-force attack: require $2^{\kappa} \cdot 2^{\kappa} = 2^{2\kappa}$ encryptions (or decryptions)
- Meet-in-the-middle attack:
  - The total complexity is $2^{\kappa} + 2^{\kappa} = 2 \cdot 2^{\kappa} = 2^{\kappa+1}$.



Triple Encryption and Meet-in-the-Middle Attack

$$y = e_{k_3}(e_{k_2}(e_{k_1}(x))) \qquad y = e_{k_1}(e_{k_2}^{-1}(e_{k_3}(x)))$$

- Key length: κ bits
- Brute-force attack: require $2^{\kappa} \cdot 2^{\kappa} \cdot 2^{\kappa} = 2^{3\kappa}$ encryptions (or decryptions)
- Meet-in-the-middle attack:
  - The total complexity is $2^{2\kappa}$.
  - 3DES;:56 bits key => attacker performs 2^{112} key tests (not 2^{168})



Key Whitening

$$\textbf{\textit{Encryption:}}\ y = e_{k,k_1,k_2}(x) = e_k(x \oplus k_1) \oplus k_2.$$
$$\textbf{\textit{Decryption:}}\ x = e^{-1}_{k,k_1,k_2}(x) = e^{-1}_k(y \oplus k_2) \oplus k_1$$