Cryptography and Security

Cunsheng DING

HKUST, Hong Kong

Version 3

Lecture 05: Modes of Operations for Block Ciphers

Outline of this Lecture

- One-key stream ciphers
- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter mode (CTR)
- Combining block ciphers

One-key Stream Ciphers

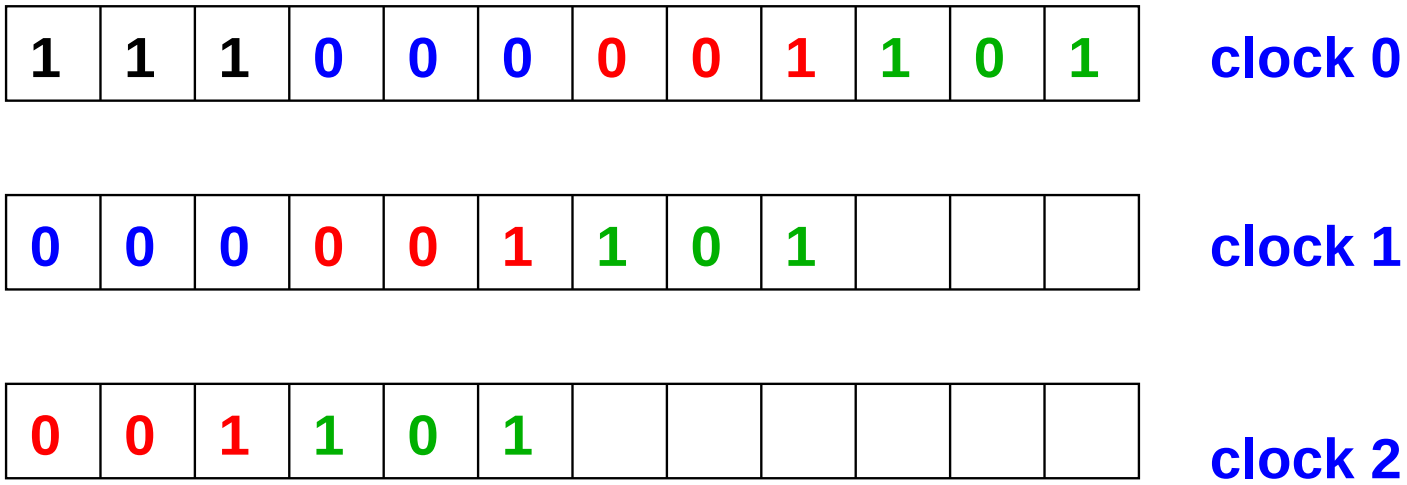
A 6-tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k, u)$, where

- $\mathcal{M}$, $\mathcal{C}$, $\mathcal{K}$ are respectively the plaintext space, ciphertext space, and key space;
- Any $k \in \mathcal{K}$ could be the encryption and decryption key; and
- u is a time-variable parameter stored in a memory device.
- E_k and D_k are encryption and decryption transformations with $D_k(E_k(m, u), u) = m$ for each $m \in \mathcal{M}$.

Remark: The ciphertext $c = E_k(m, u)$ depends on k, m and u, and is time-dependent, as u is time-dependent. We will see one-key stream ciphers today.

Shift Registers

Definition: An (n, t, b) left shift register is a memory device with n memory ceils such that at each time unit, the content of each ceil moves to the ceil left to it in t positions if this ceil exists, and will be shifted out if this ceil does not exist. Here b denotes the memory size in bits of each ceil. E.g., a $(12, 3, 1)$ left shift register:



Assumptions on a Given One-Key Block Cipher

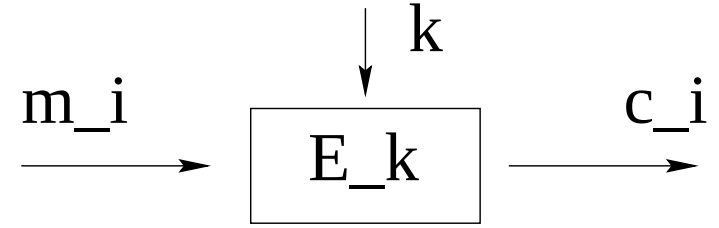
The underlying block cipher $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$ maps a plaintext block of n bits into a ciphertext of n bits. Padding the last block if necessary.

Let $m = m_1 m_2 \cdots m_h$ be the message, where the m_i are plaintext blocks of t bits, and let $c = c_1 c_2 \cdots c_h$ be the corresponding ciphertext, where the c_i are ciphertext blocks of t bits.

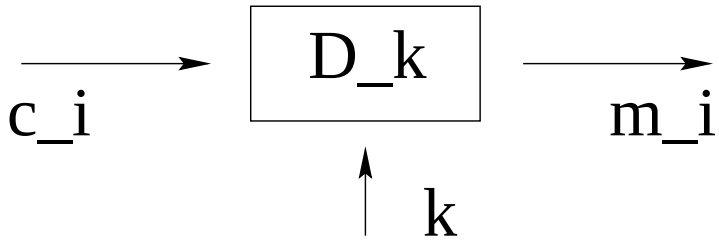
Electronic Codebook Mode (ECB)

Electronic Codebook Mode: Pictorial

Remark: It is the direct use of a one-key block cipher.



encryption



decription

Electronic Codebook Mode: Mathematical

Mathematical description of the encryption and decryption process:

Encryption: $c_i = E_k(m_i)$ for each i.

Decryption: $m_i = D_k(c_i)$ for each i.

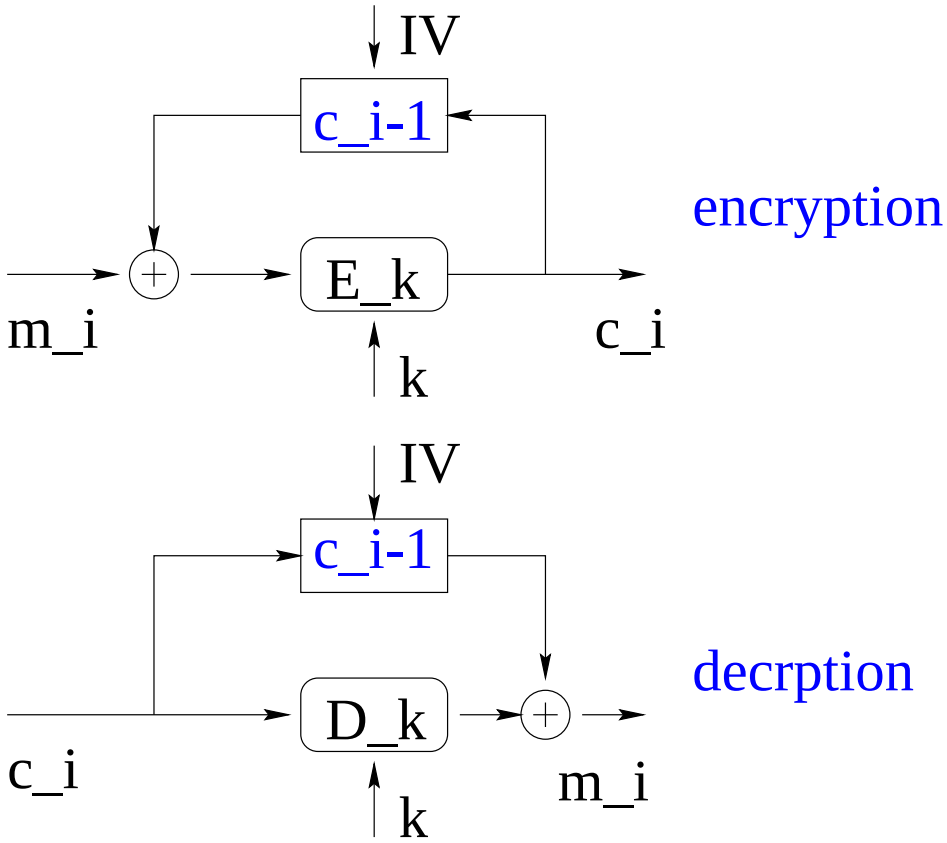
Application: secure transmission of short messages.

Remark: Same plaintext block is always encrypted to the same ciphertext block if the secret key is fixed.

Cipher Block Chaining Mode (CBC)

Cipher Block Chaining Mode: Pictorial

Add two building blocks into the new cipher. Choose any n-bit vector IV as the initial value of the $(n, n, 1)$ left-shift register, and define $c_0 = IV$.



Cipher Block Chaining Mode: Mathematical

Operation: Choose any n-bit vector IV as the initial value, and define $c_0 = IV$.

Encryption: $c_i = E_k(m_i \oplus c_{i-1})$ for each $i \geq 1$.

Decryption: $m_i = D_k(c_i) \oplus c_{i-1}$ for each $i \geq 1$.

Remark: The original one-key block cipher is modified into a new cipher, which becomes a **stream cipher**.

Remark: This mode of operation is widely used in real-world security systems. It is used for encrypting lengthy messages.

Cipher Feedback Mode (CFB)

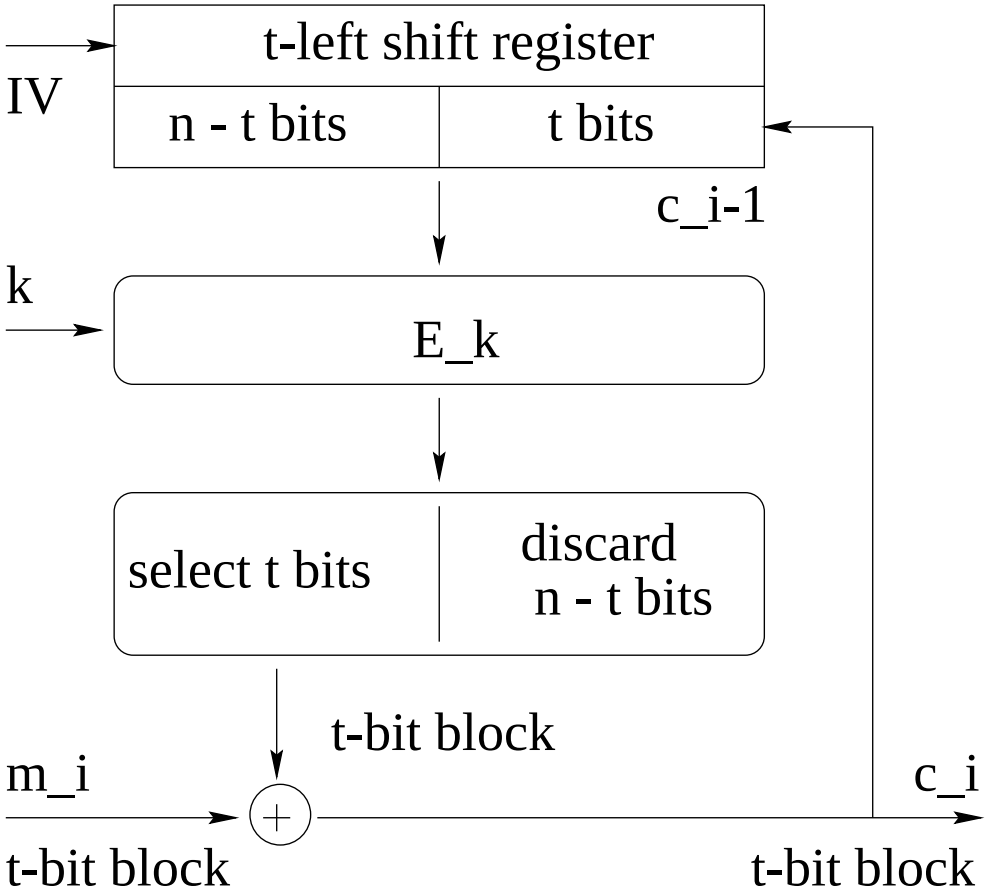
Cipher Feedback Mode: Main Facts

- It is another way to convert a block cipher into a stream cipher.
- Bit errors in transmission propagate for a number of positions.

Remark: With internal memory, a stream cipher based on the original block cipher.

Cipher Feedback Mode: Pictorial

Encryption: Set $1 \leq t \leq n$. Choose any n-bit vector IV as the initial value, and define c_0 to be the right-most t bits of IV.



Cipher Feedback Mode: Mathematical

Encryption: Set $1 \leq t \leq n$. Choose any n-bit vector IV as the initial value, and define c_0 to be the right-most t bits of IV.

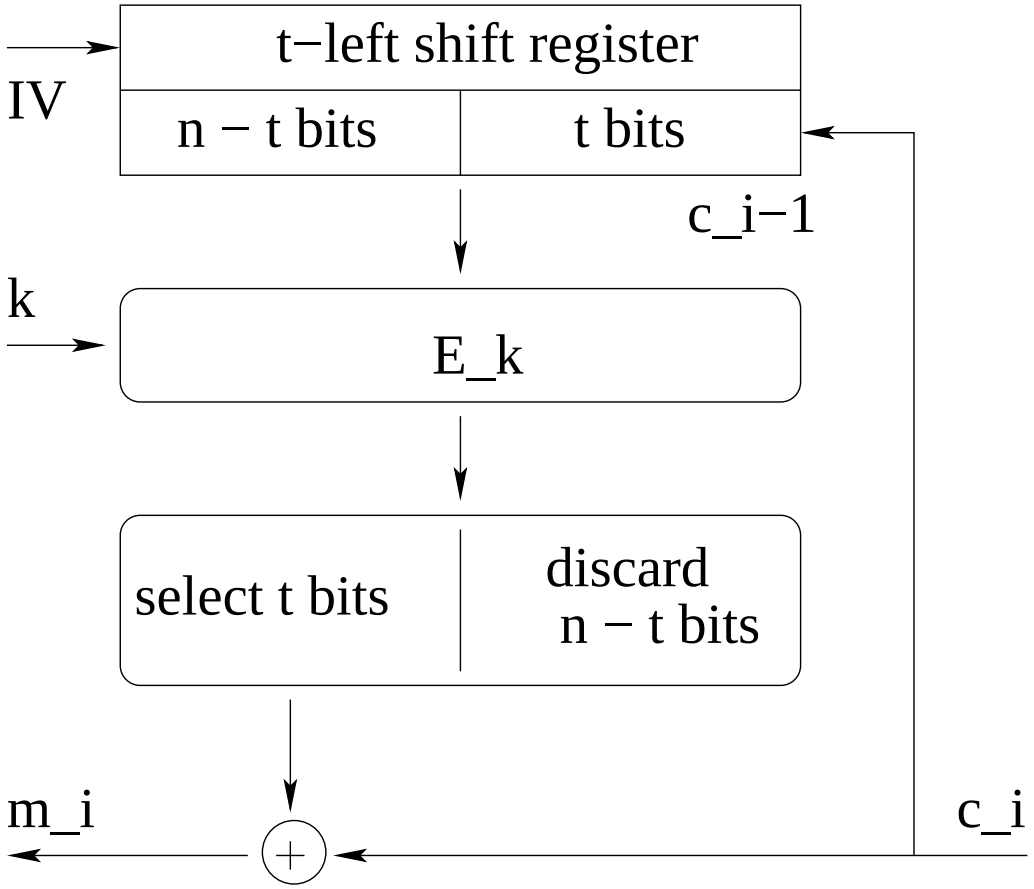
Let $||$ denote the concatenation, and S_t denote the selection of the left-most t bits. At time unit i assume that l_{i-1} is the left-most $n-t$ bits of the register before m_i is encrypted. Then encryption process is as follows:

$$c_i = m_i \oplus S_t[E_k(l_{i-1}||c_{i-1})]$$

for $i \geq 1$.

Cipher Feedback Mode: Pictorial

Decryption: Set $1 \leq t \leq n$. Choose any n-bit vector IV as the initial value, and define c_0 to be the right-most t bits of IV.



Cipher Feedback Mode: Mathematical

Decryption: Set $1 \leq t \leq n$. Choose any n-bit vector IV as the initial value, and define c_0 to be the right-most t bits of IV.

Let $||$ denote the concatenation, and S_t denote the selection of the left-most t bits. At time unit i assume that l_{i-1} is the left-most $n-t$ bits of the register before c_i is decrypted. Then decryption process is as follows:

$$m_i = c_i \oplus S_t[E_k(l_{i-1}||c_{i-1})]$$

for $i \geq 1$.

Output Feedback Mode (OFB)

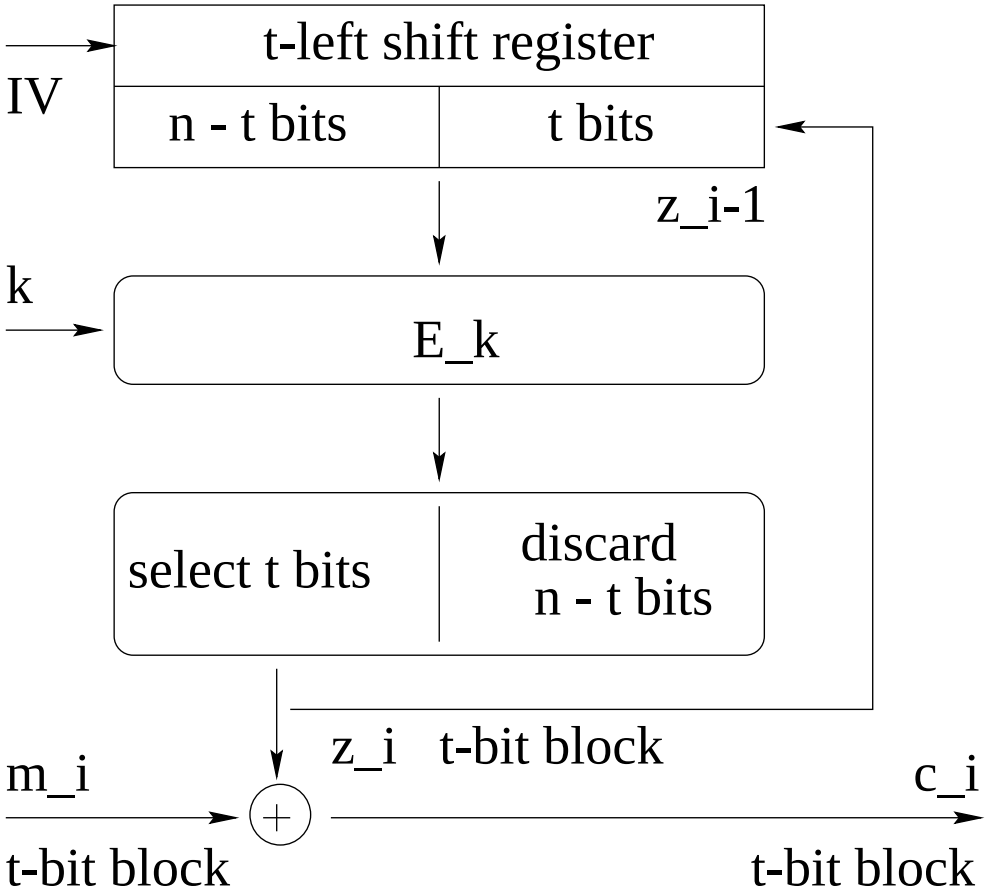
Output Feedback Mode: Main Facts

- It is another way to convert a block cipher into a stream cipher.
- Bit errors in transmission do not propagate.

Remark: With internal memory, a stream cipher based on the original block cipher.

Output Feedback Mode: Pictorial

Encryption: Set $1 \leq t \leq n$. Choose any n-bit vector IV as the initial value, and define z_0 to be the right-most t bits of IV.



Output Feedback Mode: Mathematical

Encryption: Set $1 \leq t \leq n$. Choose any n-bit vector IV as the initial value, and define z_0 to be the right-most t bits of IV.

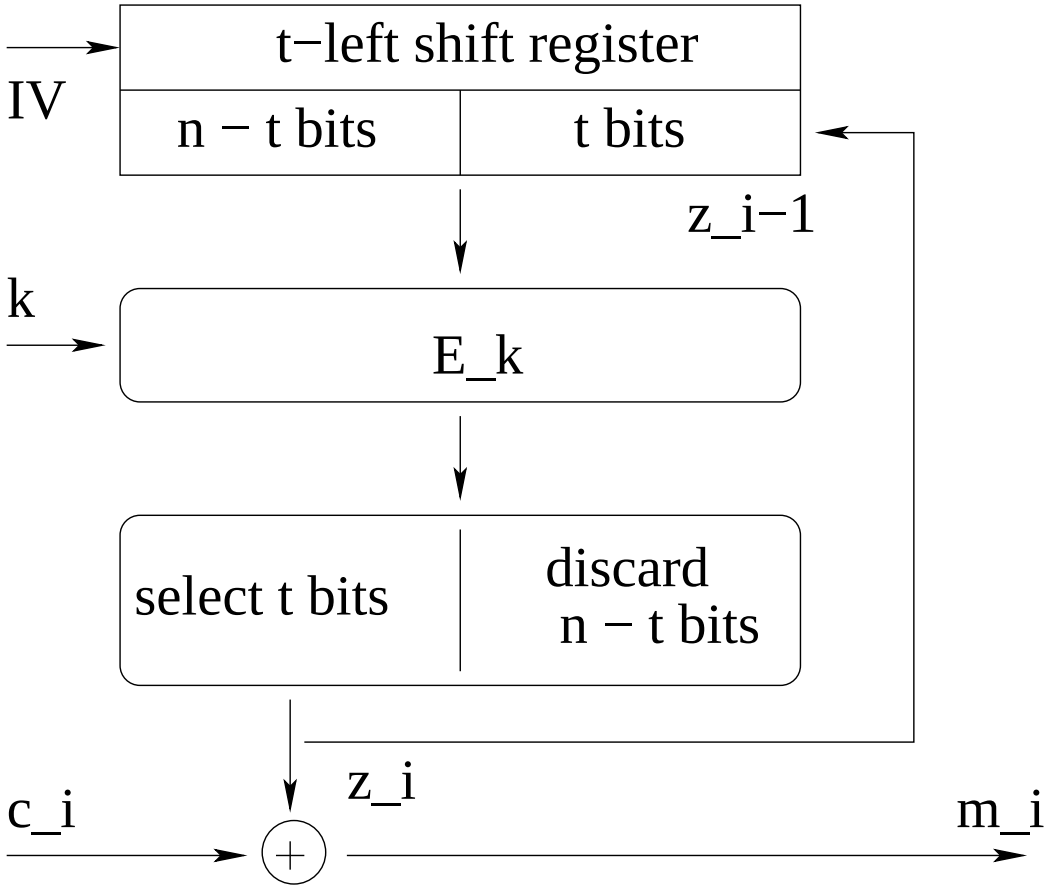
Let $||$ denote the concatenation, and S_t denote the selection of the left-most t bits. At time unit i assume that l_{i-1} is the left-most $n-t$ bits of the register before m_i is encrypted. Then encryption process is as follows:

$$c_i = m_i \oplus S_t[E_k(l_{i-1}||z_{i-1})]$$

for $i \geq 1$.

Output Feedback Mode: Pictorial

Decryption: Set $1 \leq t \leq n$. Choose any n-bit vector IV as the initial value, and define z_0 to be the right-most t bits of IV.



Output Feedback Mode: Mathematical

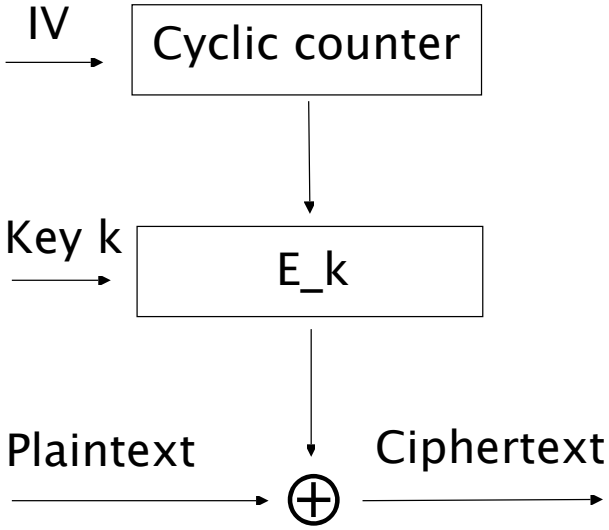
Decryption: Set $1 \leq t \leq n$. Choose any n-bit vector IV as the initial value, and define c_0 to be the right-most t bits of IV.

Let $||$ denote the concatenation, and S_t denote the selection of the left-most t bits. At time unit i assume that l_{i-1} is the left-most $n-t$ bits of the register before c_i is decrypted. Then decryption process is as follows:

$$m_i = c_i \oplus S_t[E_k(l_{i-1}||z_{i-1})]$$

for $i \geq 1$.

Counter Mode: Encryption



Counter: It cyclicly counts the integers in $\{0, 1, 2, \ldots, 2^n - 1\}$.

The message block size: n bits, the same as that of the original cipher.

Decryption: The same as the encryption function

Combining Block Ciphers

Combining Block Ciphers

Double Encryption: $c = E_{k_2}(E_{k_1}(m))$, each k_i is a secret key of the original cipher.

Triple Encryption: $c = E_{k_3}(E_{k_2}(E_{k_1}(m)))$, each k_i is a secret key of the original cipher.

Triple-DES (3DES): $c = E_{k_3}(D_{k_2}(E_{k_1}(m)))$, where each k_i has 56-bits. Widely used in real-world security systems!

Cascading: $c = E'_{k_2}(E''_{k_1}(m))$, where E'_k and E''_k are two different block ciphers.

Other Block Ciphers

Example: FEAL, RC2, IDEA, Skipjack, GOST, Blowfish, SAFER, RC5.

- B. Schneier, Applied Cryptography, 2nd Edition, John Wiley & Sons, 1996, Chapter 15.