Cryptography and Security

Cunsheng DING

HKUST, Hong Kong

COMP5631

Lecture 05: Modes of Operation for Block Ciphers

Outline of This Lecture

- Several encodings of nonnegative integers
- A padding method for encryption
- One-key stream ciphers
- Electronic Codebook (ECB) mode
- Cipher Block Chaining (CBC) mode
- Counter (CTR) mode
- Combining block ciphers

Several Encodings of Nonnegative Integers

The Decimal Expression of Nonnegative Integers

- It is the expression we learnt in primary school.
- It is the base-10 expression of nonnegative integers.
- $i = i_t 10^t + i_{t-1} 10^{t-1} + \cdots + i_1 10^1 + i_0 10^0$, where each coefficient $i_j \in \{0, 1, 2, \ldots, 9\}$ and t is a nonnegative integer.
- We identify i with the sequence $i_t i_{t-1} \cdots i_1 i_0$.
- For example, $76503 = 7 \times 10^4 + 6 \times 10^3 + 5 \times 10^2 + 0 \times 10^1 + 3 \times 10^0$.

The Hexadecimal Expression of Nonnegative Integers

- It is the base-16 expression of nonnegative integers.
- Let $A = 10$, $B = 11$, $C = 12$, $D = 13$, $E = 14$, $F = 15$.
- $i = i_t 16^t + i_{t-1} 16^{t-1} + \cdots + i_1 16^1 + i_0 16^0$, where each coefficient $i_j \in \{0, 1, 2, \ldots, 9, A, B, C, D, E, F\}$ and t is a nonnegative integer.
- We identify i with the sequence $i_t i_{t-1} \cdots i_1 i_0$.
- For example,

$$980233 = E \times 16^4 + F \times 16^3 + 5 \times 16^2 + 0 \times 16^1 + 9 \times 16^0 = EF509.$$

The Binary Expression of Nonnegative Integers

- It is the base-2 expression of nonnegative integers.
- $i = i_t 2^t + i_{t-1} 2^{t-1} + \cdots + i_1 2^1 + i_0 2^0$, where each coefficient $i_j \in \{0, 1\}$ and t is a nonnegative integer.
- We identify i with the sequence $i_t i_{t-1} \cdots i_1 i_0$.
- For example, $17 = 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 1^0 = 10001$.
- For each fixed $h \geq 1$, each integer i in the set $\{0, 1, 2, \ldots, 2^{h-1}\}$ is uniquely expressed and identified as

$$i = i_{h-1} 2^{h-1} + i_{h-2} 2^{h-2} + \cdots + i_1 2^1 + i_0 2^0 = i_{h-1} i_{h-2} \cdots i_1 i_0.$$

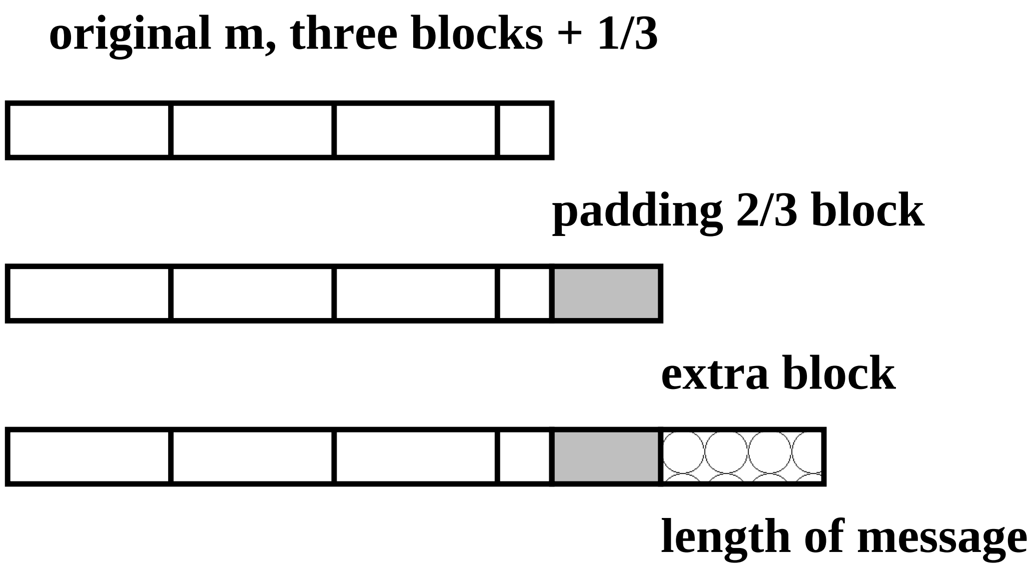
  This gives a bijection from the set $\{0, 1, 2, \ldots, 2^{h-1}\}$ to the set of all binary strings of length h.

A Padding Method for Encryption

Why Padding Messages

Question: If you use AES to encrypt your message, you need to break it into blocks of 128 bits. However, it is possible that the last block is not a complete block of 128 bits. How would you encrypt the last block?

A Method for Padding Messages



- Padding is done even if the last block is a complete block.
- The padded part is $10\ldots0$, where the number of 0's depends on the message block size and the size of the last message block.

In summary, padding is always done.

One-Key Stream 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, key space;
- Any $k \in \mathcal{K}$ could be the encryption and decryption key;
- u is a time-variable parameter stored in a memory device.
- The encryption and decryption process are $c = E_k(m, u)$ and $m = D_k(c, u)$. Hence, E_k and D_k are encryption and decryption functions with $D_k(E_k(m, u), u) = m$ for each $m \in \mathcal{M}$ and each u.

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

A Different Definition of One-key Stream Ciphers

The different definition: If a cipher does the encryption bit by bit, the cipher is called a stream cipher. Otherwise, it is a block cipher.

Remark: This definition is used in some textbooks on cryptography and has led to a confusion.

Warning: In this course, you must use our definition in the previous slide.

A Type of Shift Registers

The $(n, n, 1)$ Shift Registers

Definition: An $(n, n, 1)$ shift register is a memory device with n memory cells such that

- each memory cell can store 1 bit, and
- the content of the register will be shifted out whenever the register is clocked.

A Block Cipher to Be Used in a Mode of Operation

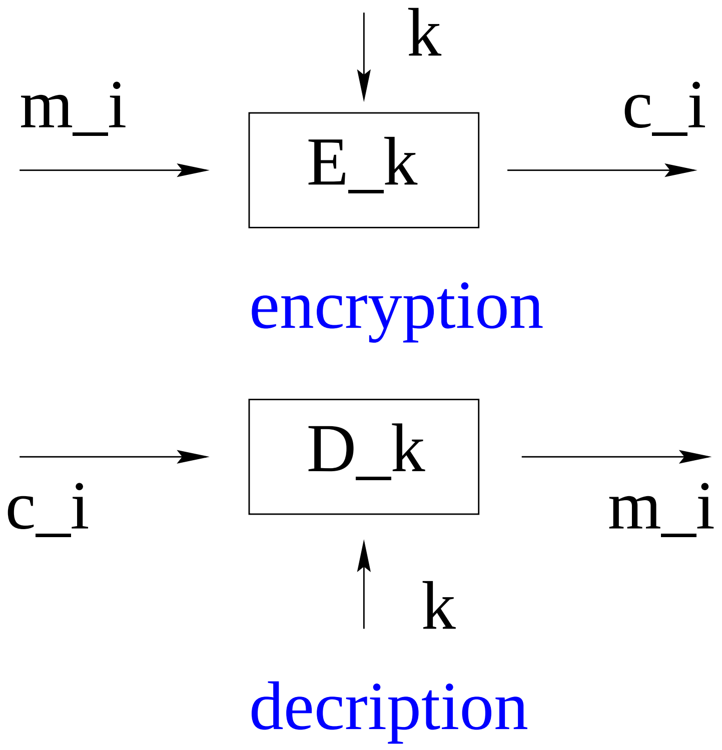
The underlying one-key block cipher $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$ maps a plaintext block of n bits into a ciphertext of n bits.

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

Electronic Codebook Mode (ECB)

Electronic Codebook Mode: Pictorial

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



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.

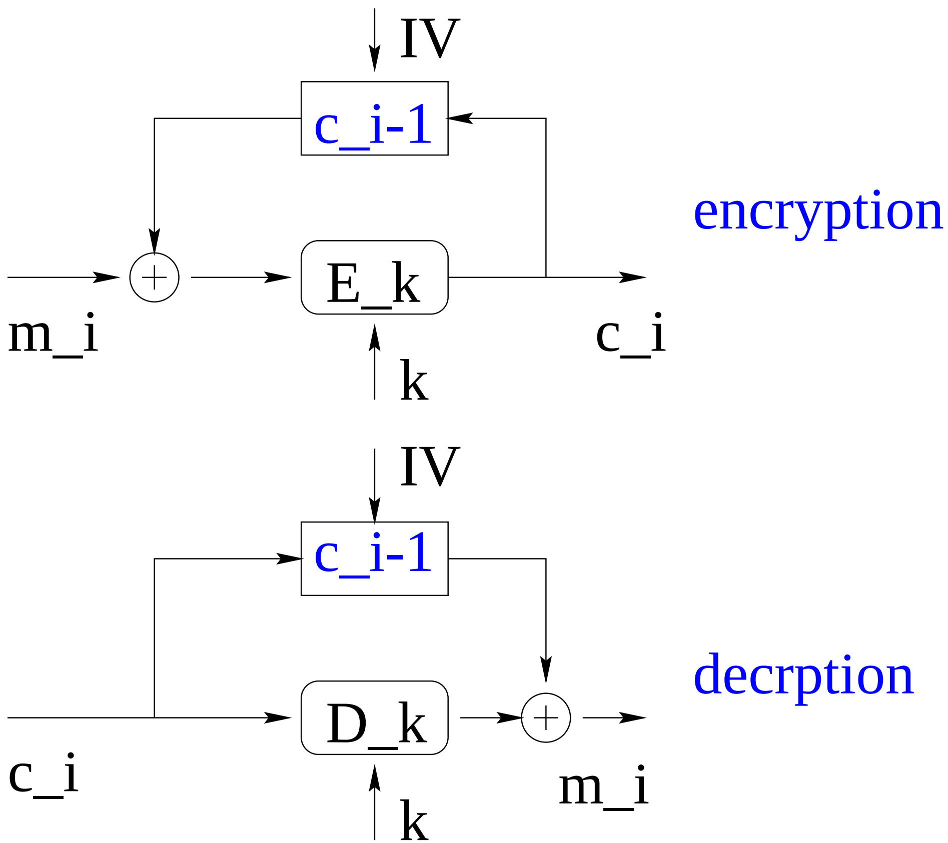
Application: secure transmission of short messages.

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 $(n, n, 1)$ 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 $i \geq 1$.

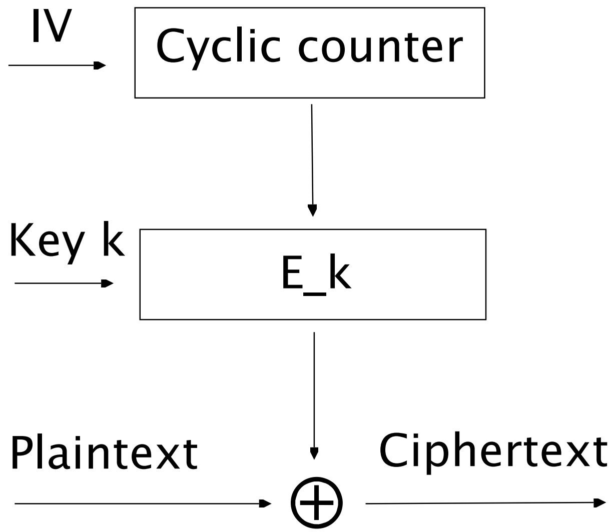
Decryption: $m_i = D_k(c_i) \oplus c_{i-1}$ for each $i \geq 1$.

Exercise: Prove the correctness of the decryption process.

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.

Counter Mode: Encryption

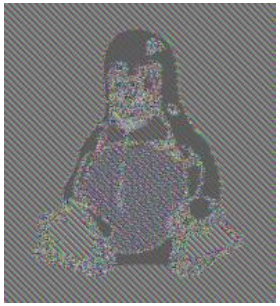


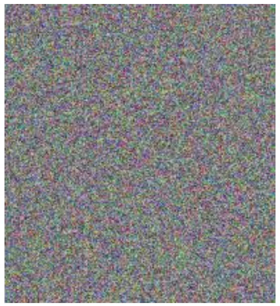
Counter: It cycliclly counts the integers in $\{0, 1, 2, \ldots, 2^n - 1\}$.

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

Exercise: Draw a picture of the decryption process.

Stream Ciphers Versus Block Ciphers





Experimental result: The AES-CBC is more secure than the AES-ECB.

Stream Ciphers Versus Block Ciphers

Exercise: Explain why the AES-CBC is better than the AES-ECB in terms of security level.

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.

Exercise: Write down the decryption process for each cipher above.