Cryptography

Cunsheng DING

HKUST, Hong Kong

COMP3631

Lecture 09: Modes of Operation for Block Ciphers

Outline of This Lecture

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

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 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 variable. We will see one-key stream ciphers today.

A Different Definition of One-key Stream Ciphers

The different definition in the literature: 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 $(n, 1)$ Shift Registers

Definition: An $(n, 1)$ 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

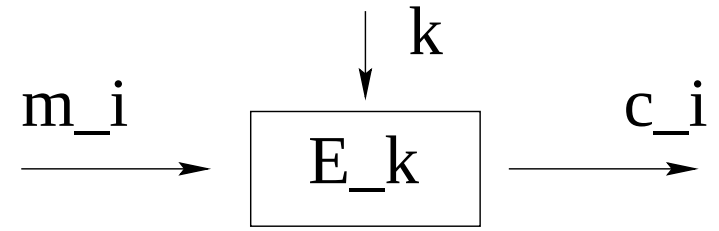
The given one-key block cipher $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$ maps a plaintext block of n bits into a ciphertext block of n bits.

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.

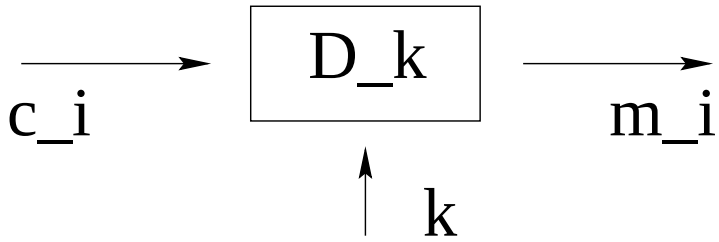
Electronic Codebook Mode (ECB)

Electronic Codebook Mode: Pictorial

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



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.

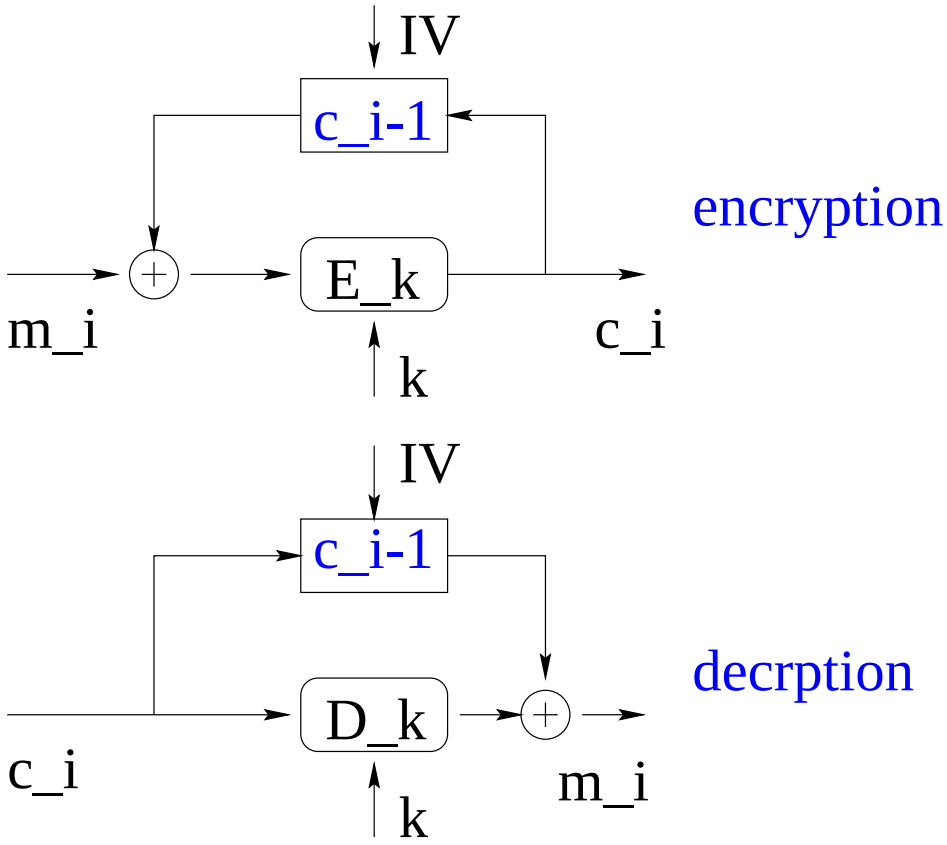
Application: secure transmission of short messages.

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 new building blocks into the given cipher. Choose any n-bit vector IV as the initial value of the $(n, 1)$ 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**.

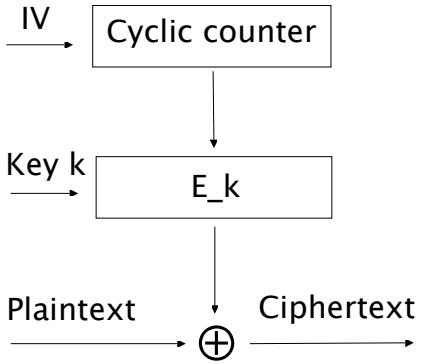
Remark: This mode of operation is widely used in real-world security systems. It is used for encrypting lengthy messages.

Cipher Block Chaining Mode: The Initial Value

- The initial value IV denoted by c_0 is not part of the key of the new cipher, but it is better to keep it confidential.
- The generation and distribution of the IV c_0 will be treated later (see Lectures 14 and 21).
- In any hardware implementation of the new cipher (i.e., the given block cipher in CBC mode), c_0 must be pre-stored in a memory device.
- For each $i \geq 1$, c_i may be used for encrypting the first plaintext block of the next plaintext later. Hence, it must be stored in a memory device.

  For example, suppose the first plaintext to be encrypted today is $m = m_2 m_1$ and the second plaintext to be encrypted tomorrow is $m' = m'_3 m'_2 m'_1$. Then the ciphertext block c_2 corresponding to m_2 computed today will be used for encrypting m'_1 tomorrow and must be stored in a memory device.

Counter Mode: The Encryption Process



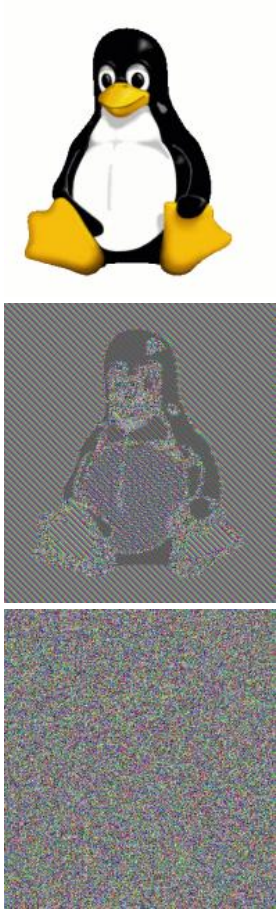
Counter: It cyclicly counts the integers in $\{0, 1, 2, \ldots, 2^n - 1\}$. Z_0 is an IV stored in the counter and $Z_i = (Z_{i-1} + 1) \bmod 2^n$ for $i \geq 1$.

Building blocks of the new cipher: E_k the encryption function of the given block cipher. The counter & the adder are the new building blocks.

The mathematical expression: $C_i = M_i \oplus E_k(Z_{i-1})$ for $i \geq 1$.

In-class 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.

Online Demo of Block Ciphers in the CBC Mode

In the following URL, you find the demo of some block ciphers in the CBC mode with/withou padding.

`https://8gwifi.org/CipherFunctions.jsp`

Appendix: Security Services Provided by Encryption

Security Services Provided by Encryption

Question: Let E_k and D_k denote the encryption and decryption function of the AES-CBC. Assume that the AES-CBC is secure. What are the possible security services that could be provided by the following protocol?

$$\text{Alice} \longrightarrow E_k(m) \longrightarrow \text{Bob}.$$

Recall the security services covered in Lecture 3: Data confidentiality, data integrity, data origin authentication, sender authentication, anti-replay, and signer nonrepudiation.

Attention: We will answer this question gradually, as it takes time to do it. See, e.g., Lecture 13.