Computer Security

Cunsheng DING, HKUST

COMP4631

Lecture 07: Several One-Key Block Ciphers

Outline of this Lecture

- One-key stream ciphers
- The Data Encryption Standard (DES)
- The Triple DES
- The Advanced Encryption Standard (AES)
- A method for padding messages
- The Cipher Block Chaining (CBC) mode

One-key Stream Ciphers

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

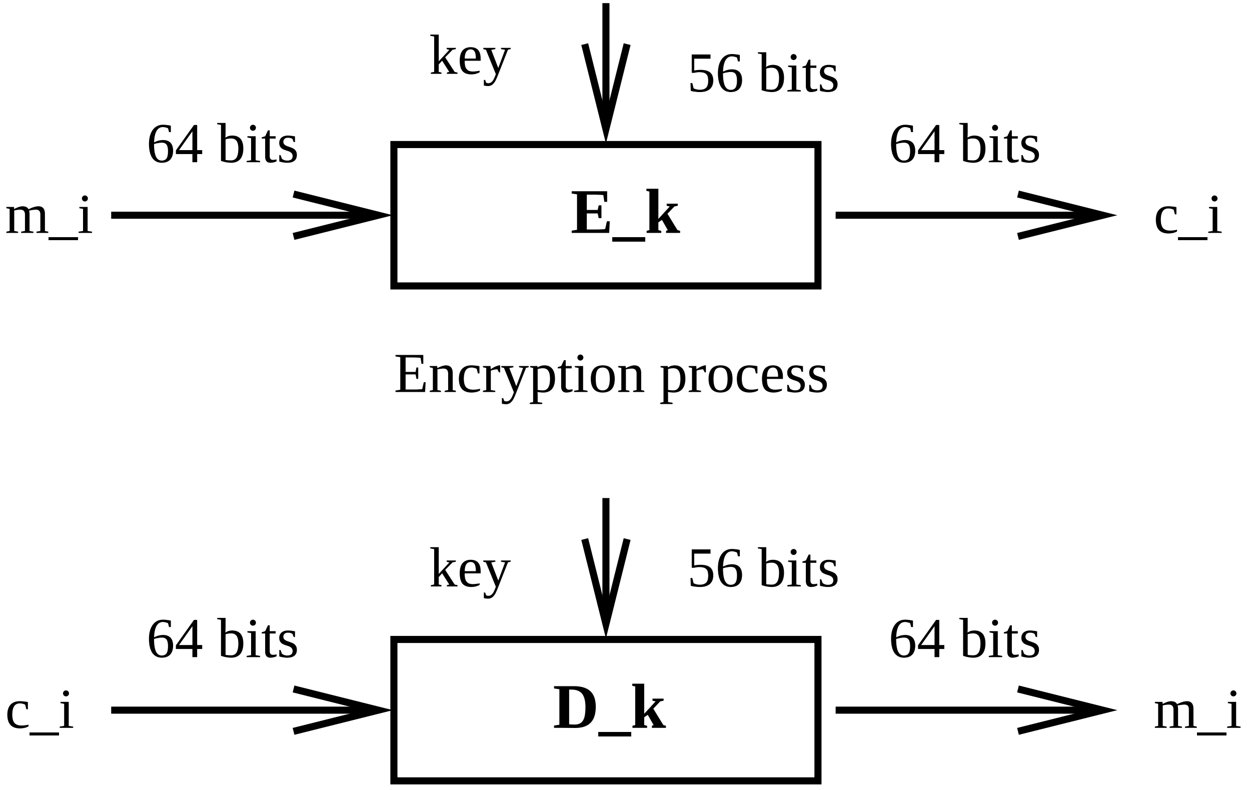
- $\mathcal{M}$, $\mathcal{C}$, $\mathcal{K}$ are respectively the plaintext space, ciphertext space, and key space;
- Any $k \in \mathcal{K}$ could be the encryption and decryption key; and
- u is a time-variable parameter stored in a memory device.
- E_k and D_k are encryption and decryption transformations 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-variable. We will see one-key stream ciphers today.

The Data Encryption Standard in Brief

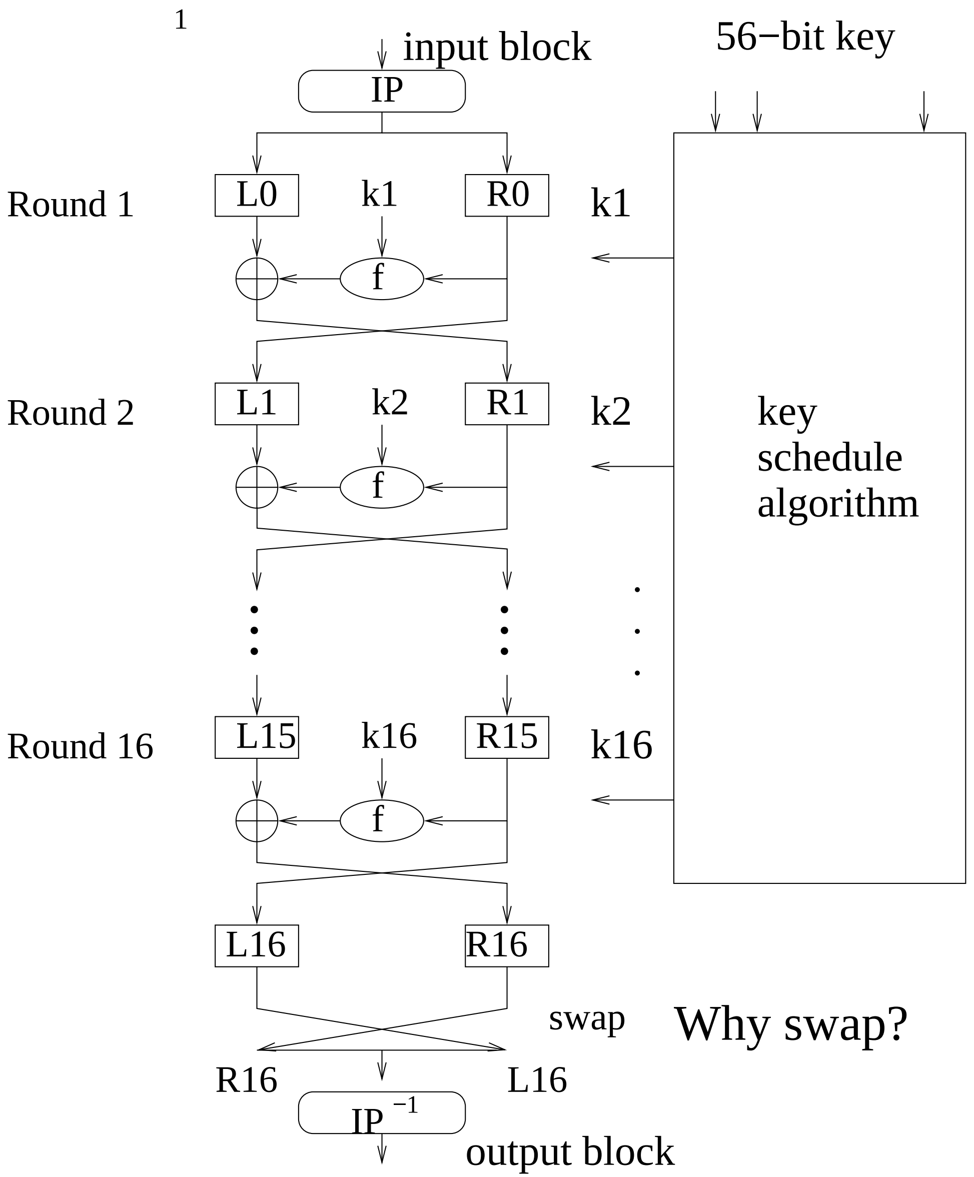
- It is a block cipher with key length 56 bits.
- It was designed by IBM in 1976 for the National Bureau of Standards (NBS), with approval from the National Security Agency (NSA).
- It had been used as a standard for encryption until 2000. In 2001 a new encryption standard, AES, replaced the DES, because its key length is too short.
- Although its wide spread use came to an end, its design idea is still used in most block ciphers.

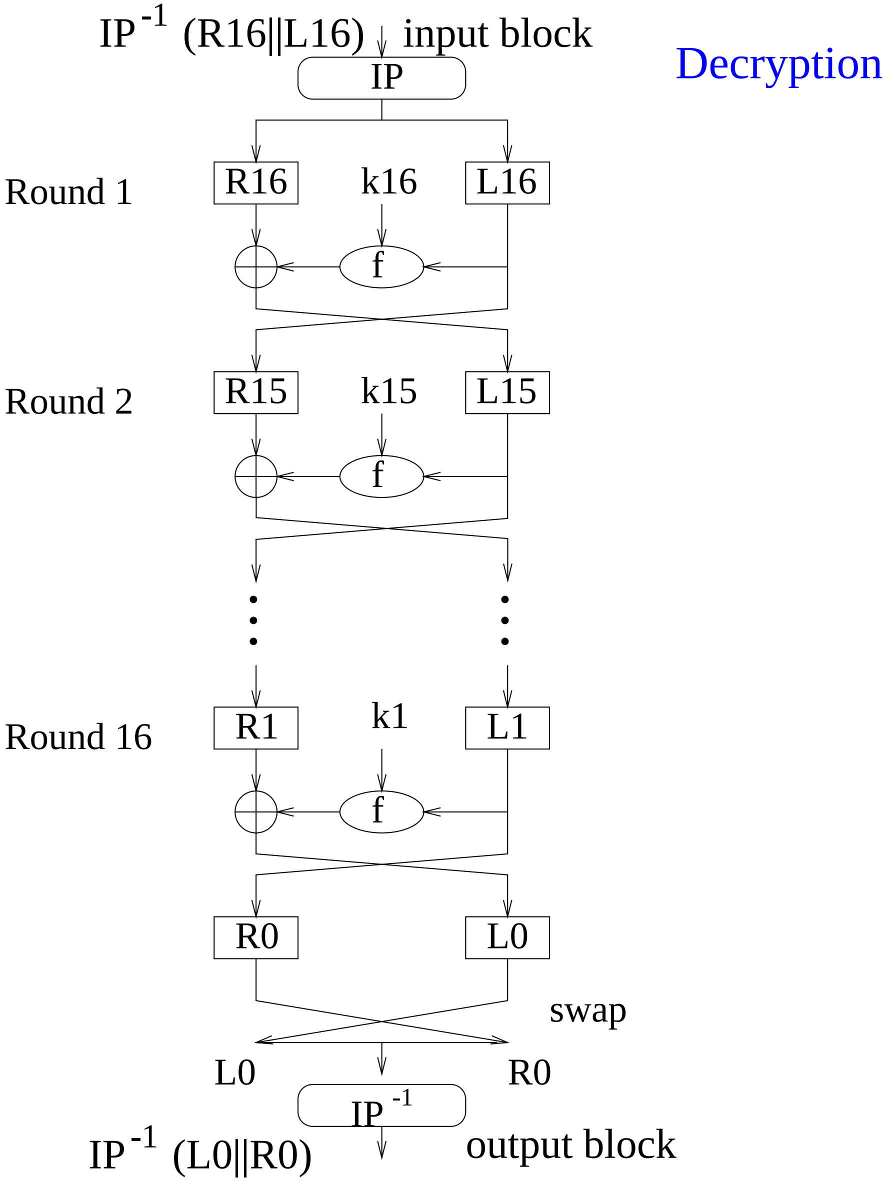
The DES Encryption and Decryption



Encryption process

Decryption process


1
input block
IP
56−bit key
Round 1
L0
k1
R0
k1
f
Round 2
L1
k2
R1
k2
f
key
schedule
algorithm
Round 16
L15
k16
R15
k16
f
L16
R16
swap
Why swap?
R16
L16
IP −1
output block


IP -1 (R16||L16)
input block
Decryption
IP
Round 1
R16
k16
L16
f
Round 2
R15
k15
L15
f
Round 16
R1
k1
L1
f
R0
L0
swap
L0
R0
IP -1
IP -1 (L0||R0)
output block

DES Design Criteria

Remark: Details of the building blocks and their design criteria are out of the scope of this course, and can be found in the reading materials posted on the course webpage.

Further information may be found in:

- B. Schneier, Applied Cryptography, 2nd Edition, John Wiley & Sons, 1996, pp. 293–294.
- D. Coppersmith, The Data Encryption Standard (DES) and Its Strength Against Attacks, IBM Journal of Research and Development, May 1994.

Security of DES

Question: Is DES really secure?

Answer: It is not regarded as secure only because its key length is too short, in view of today's hardware technology. So DES has been replaced by the AES – Advanced Encryption Standard (Rijndael).

In the public literature there is no practical attack on DES that is based on the structure of DES. But it is possible that some secret organization has a practical attack.

- D. Coppersmith, The Data Encryption Standard (DES) and Its Strength Against Attacks, IBM Journal of Research and Development, May 1994.

The DES Variants

Triple DES: Let E_k and D_k be the encryption and decryption function of DES.

Encryption: $c = E_{k_1}(D_{k_2}(E_{k_3}(m)))$.

Decryption: $m = D_{k_3}(E_{k_2}(D_{k_1}(c)))$.

Key length 168 bits. If $k_1 = k_3 \neq k_2$, it is called Triple DES with two keys.

Other Variants: DES with Independent Subkeys, and CRYPT(3) (used in Unix system), etc.

Reference: B. Schneier, Applied Cryptography, 2nd Edition, John Wiley & Sons, 1996, pp. 294–300.

The Advanced Encryption Standard (AES)

Background: The key length of DES is too short and should be replaced. NIST issued a call for proposals for a new Advanced Encryption Standard in 1997.

The basic requirements are:

- Its security strength should be equal to or better than 3DES and should be much more efficient.
- AES must be a symmetric block cipher with a key length of 128 bits, and support for key lengths 192 and 256 bits.

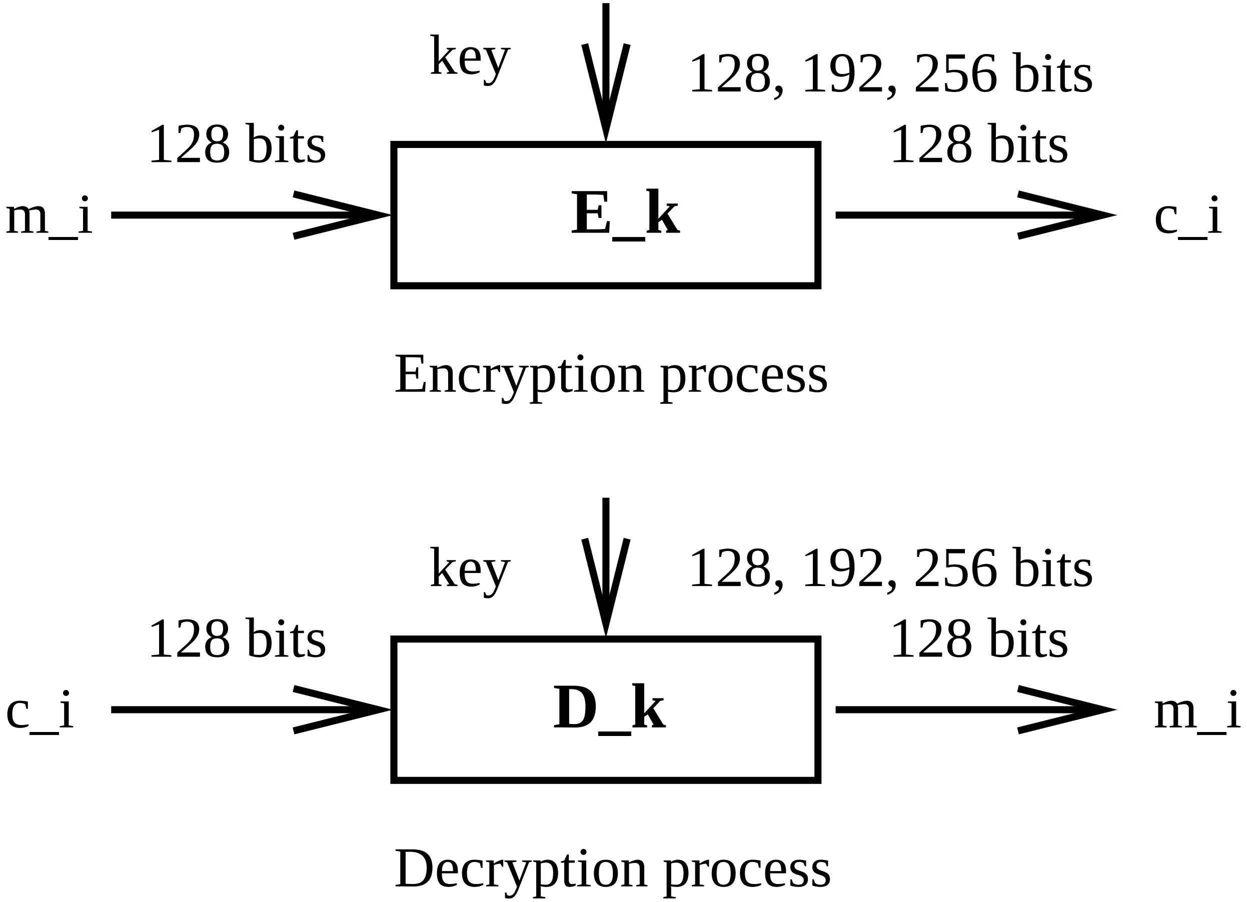
The Advanced Encryption Standard (AES)

Rijndael: Many international proposals were received. After three rounds of selection and evaluation, in 2000 Rijndael was selected as the new AES by NIST.

Designers: Joan Daemen and Vincent Rijmen from Belgium.

- Key lengths: 128, 192, 256 bits.
- Plaintext block length: 128 bits.

The AES Encryption and Decryption



The Advanced Encryption Standard (AES)

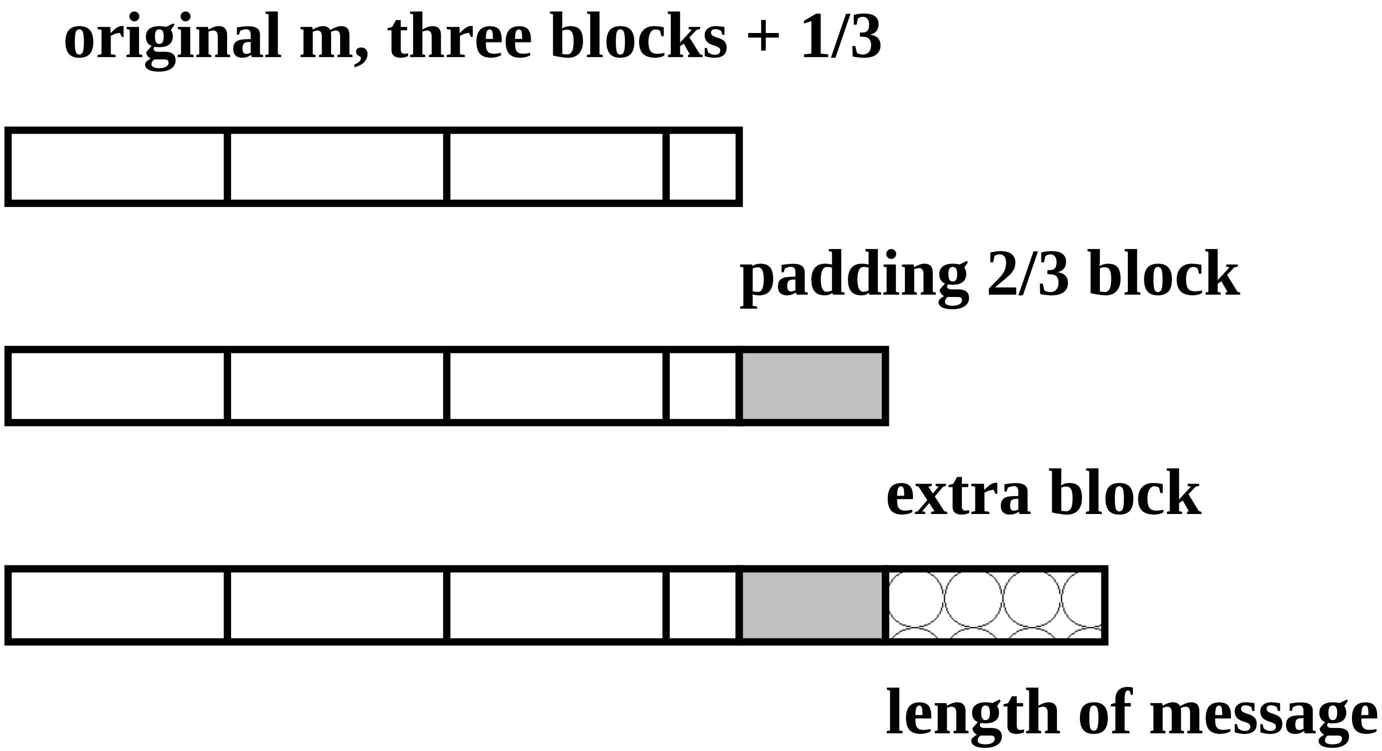
References:

- J. Daemen and V. Rijmen, The Design of Rijndael, Springer-Verlag, 2001.
- W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd Edition, Pearson Education, 2003.

Why Padding Messages

Question: If you use AES to encrypt your message, you need to break it into blocks, each with 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



original m, three blocks + 1/3

padding 2/3 block

extra block

length of message

Five Modes of Operations for Block Ciphers

- Electronic Codebook (ECB) Mode
- Cipher Block Chaining (CBC) Mode
- Cipher Feedback (CFB) Mode (not introduced in COMP4631)
- Output Feedback (OFB) Mode (not introduced in COMP4631)
- Counter Mode (not introduced in COMP4631)

Assumptions on the Underlying Block Cipher

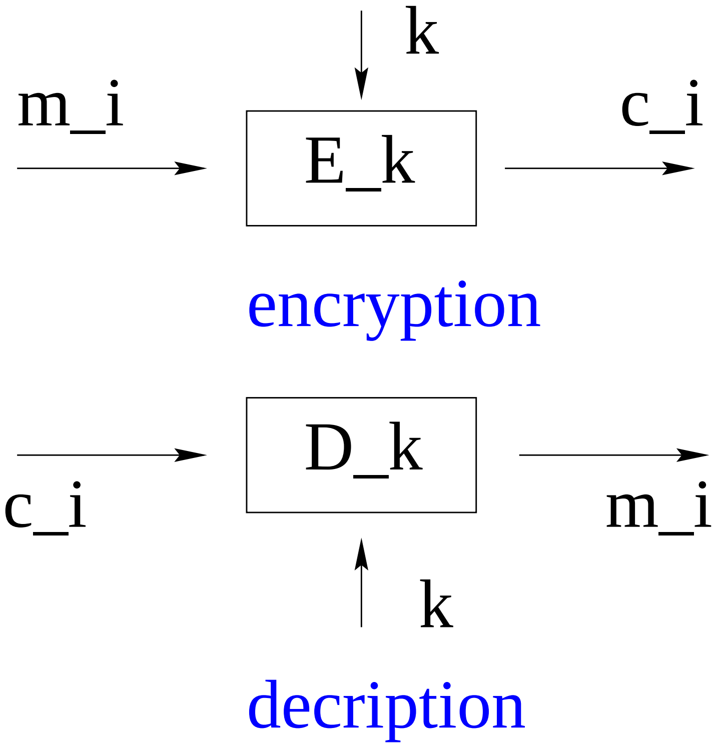
The underlying block cipher $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$ maps a plaintext block of n bits into a ciphertext of n bits. Padding the last block if necessary.

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

Electronic Codebook Mode (ECB)

Electronic Codebook Mode: Pictorial

Remarks: No internal memory.



Electronic Codebook Mode: Mathematical

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

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

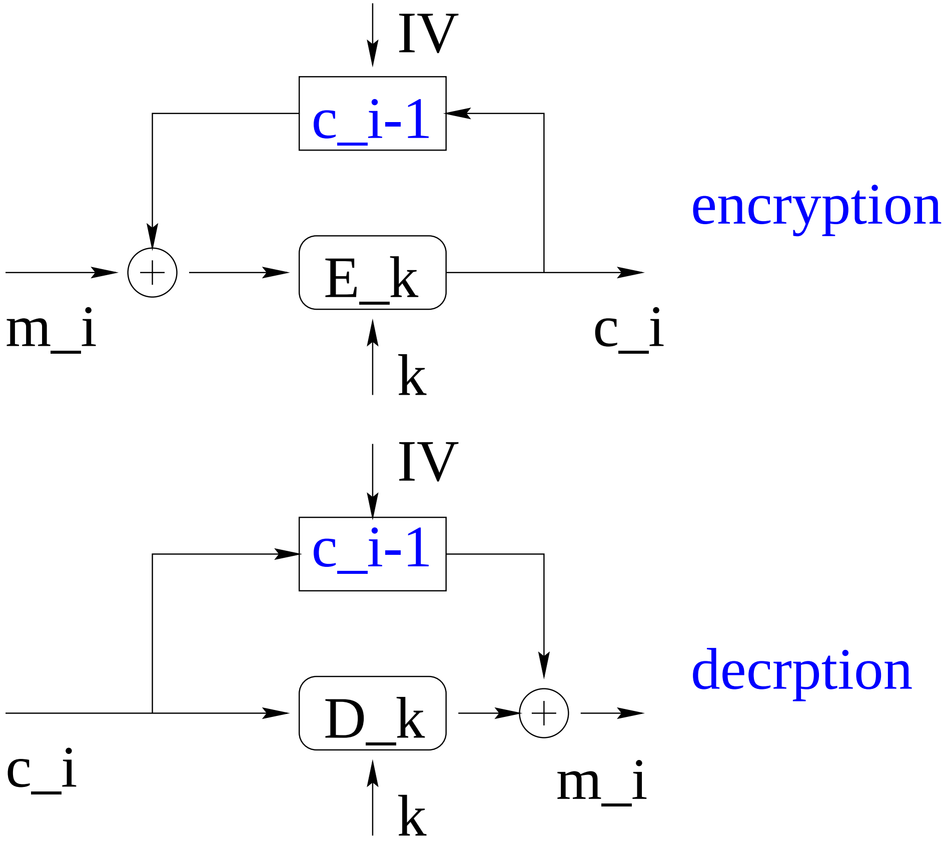
Application: secure transmission of single values (e.g., encryption key), not for lengthy message.

Remark: Same plaintext block is always encrypted to the same ciphertext block.

Cipher Block Chaining Mode (CBC)

Cipher Block Chaining Mode: Pictorial

Choose any n-bit vector IV as the initial value, and define $c_0 = IV$. It is stored in a register (memory device) with n bit memory.



Cipher Block Chaining Mode: Mathematical

Operation: Set $t = n$. 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 $i \geq 1$.

Application: general-purpose block-oriented transmission, authentication.