Cryptography

Cunsheng DING, HKUST

COMP3631

Lecture 07: Several One-Key Block Ciphers

Outline of this Lecture

- The ASCII encodings
- The decimal expression of nonnegative integers
- The hexadecimal expression of nonnegative integers
- The binary expression of nonnegative integers
- The Data Encryption Standard (DES)
- The Triple DES
- The Advanced Encryption Standard (AES)
- A method for padding messages

Encoding of Keyboard Characters

The ASCII Encodings

- ASCII, stands for American Standard Code for Information Interchange.
- The standard ASCII is a 7-bit character code.
- The extended ASCII represents each keyboard character as an 8-bit binary string (one byte).

`space`	`00100000`
`! (Exclamation mark)`	`00100001`
`2`	`00110010`
`A`	`01000001`
`a`	`01100001`

Remark: An English message can be encoded into a finite binary string by ASCII.

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

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

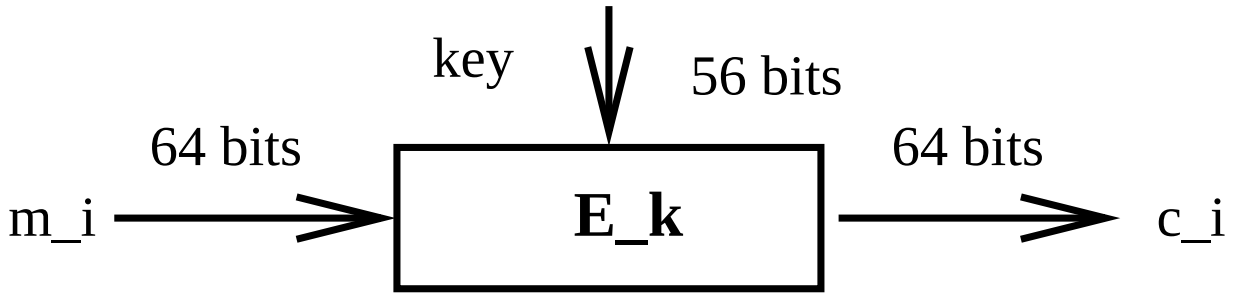
  This gives a bijection from the set $\{0, 1, 2, \ldots, 2^h - 1\}$ to the set of all binary strings of length h, denoted by $\{0, 1\}^h$.

Several One-Key Block Ciphers

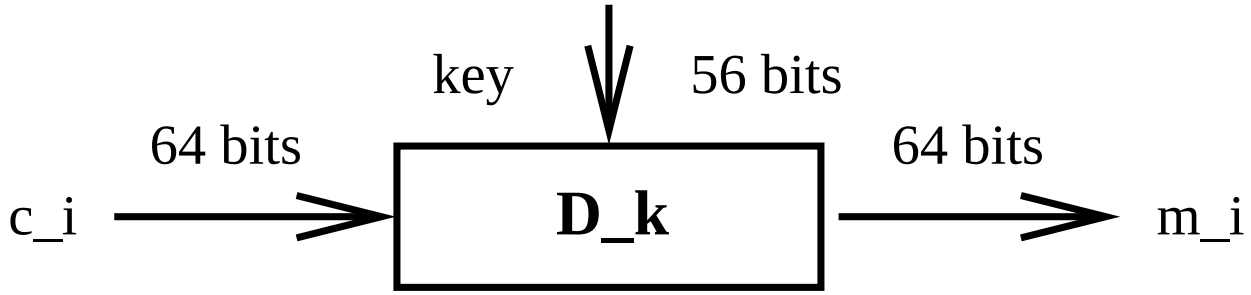
The Data Encryption Standard in Brief

- It is a one-key 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.
- Its design follows the iterative design paradigm introduced in Lecture 6.

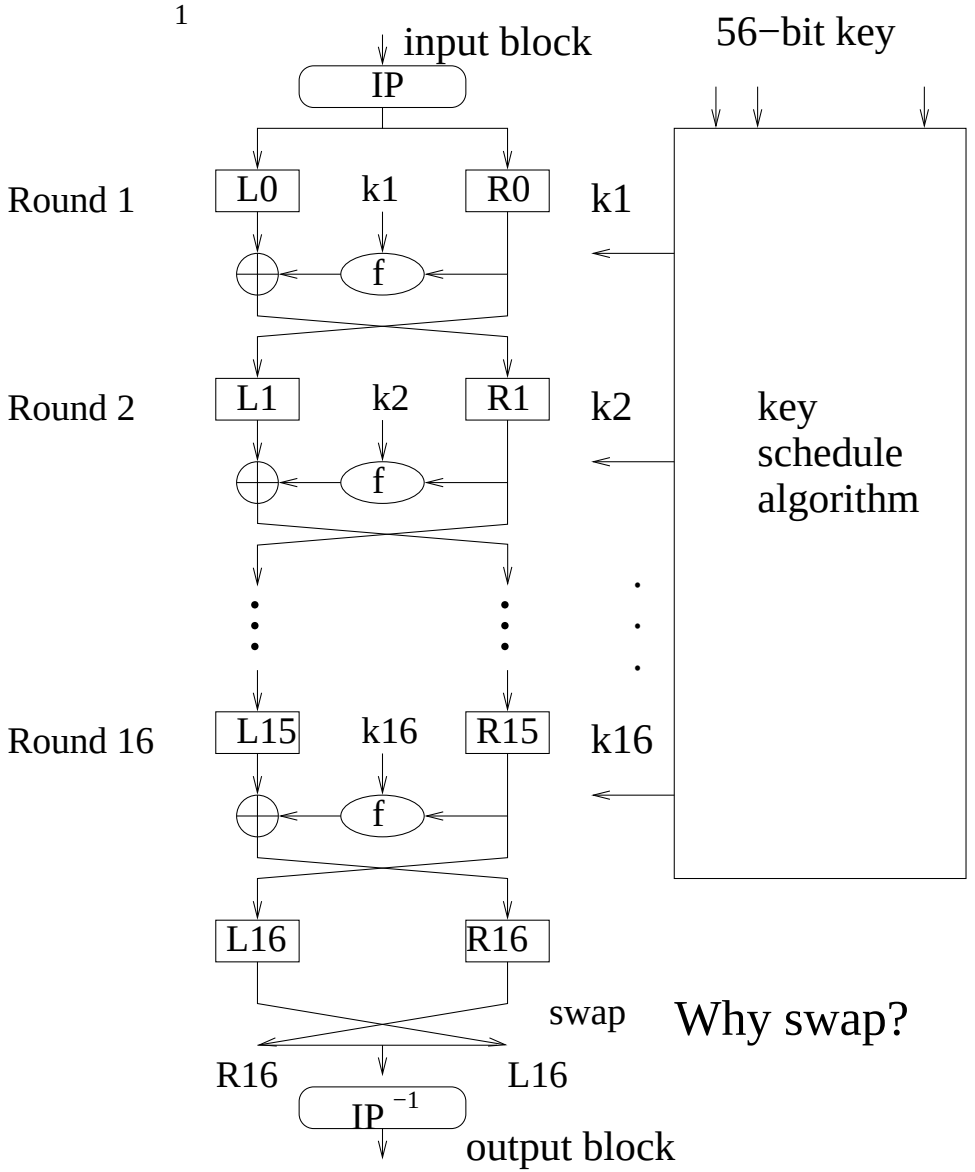
The DES Encryption and Decryption

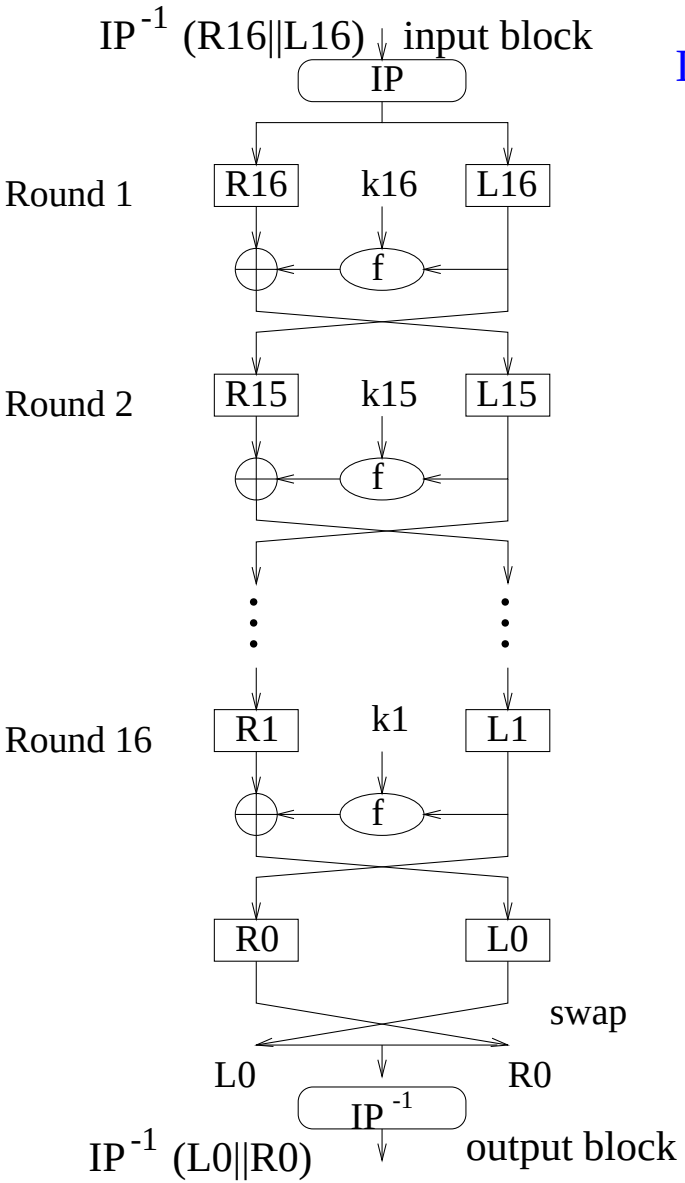


Encryption process



Decryption process


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


IP -1 (R16||L16)
input block
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

Decryption

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:

- 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 was 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 Triple DES

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

The key (k_1, k_2, k_3) of the Triple DES has 168 bits.

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

Remark: Triple DES (also written as 3DES) is still widely used in real-world security systems

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.

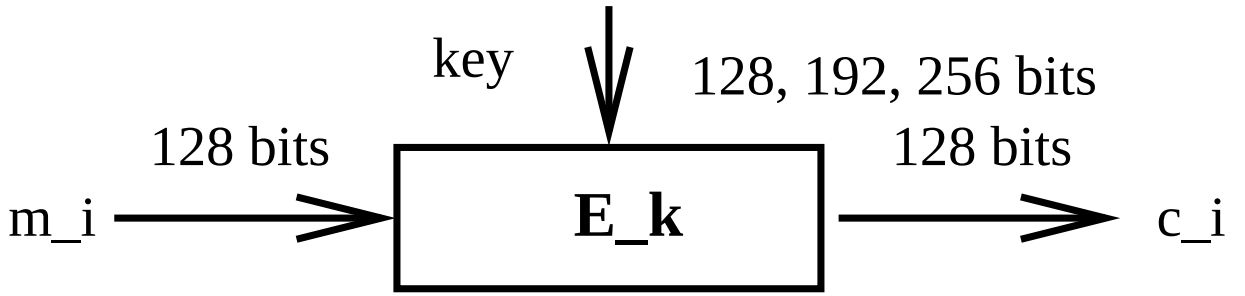
The Advanced Encryption Standard (AES)

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

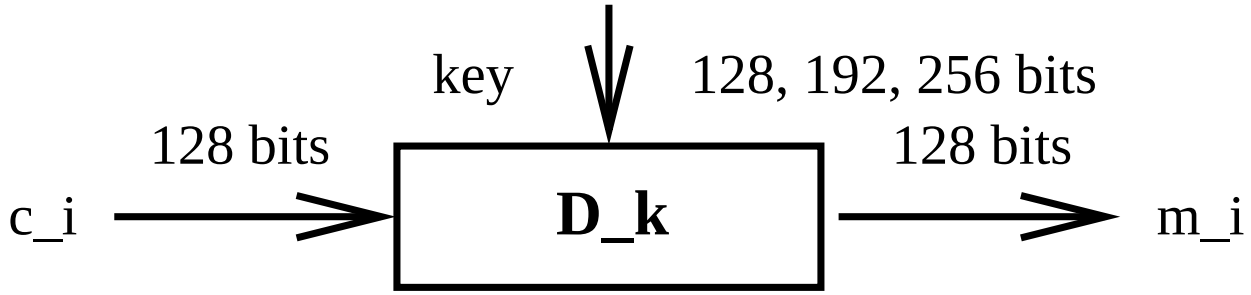
Designers: Joan Daemen and Vincent Rijmen from Belgium.

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

The AES Encryption and Decryption



Encryption process



Decryption process

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, 7th Edition, Pearson Education, 2017.

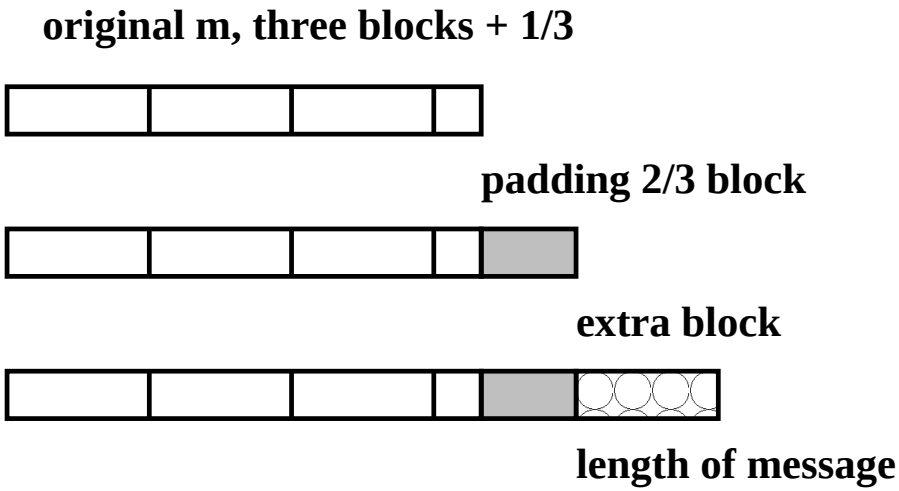
Remark: We will introduce the AES in technical details in the next lecture.

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



- 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.
- The extra block is the binary expression of the number of the message bits in the padded block and is a complete block.
- Padding is done even if the last block is a complete block. In this case, the padded block is of the form 10...0 and the extra block is 00...0.

Online Demonstrations of Some Ciphers

In the following URL, you find the demo of DES and AES in different modes with/without padding, and demonstrations of many other ciphers:

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