Cryptography and Network Security

Block Ciphers + DES

cuu duong than cong . com

Lectured by
Nguyễn Đức Thái

cuu duong than cong . com

CuuDuongThanCong.com https://fb.com/tailieudientucntt

Outline

- Block Cipher Principles
- Feistel Ciphers
- The Data Encryption Standard (DES)

- (Contents can be found in Chapter 3, reference [1])

cuu duong than cong . com

Block Cipher vs. Stream Cipher

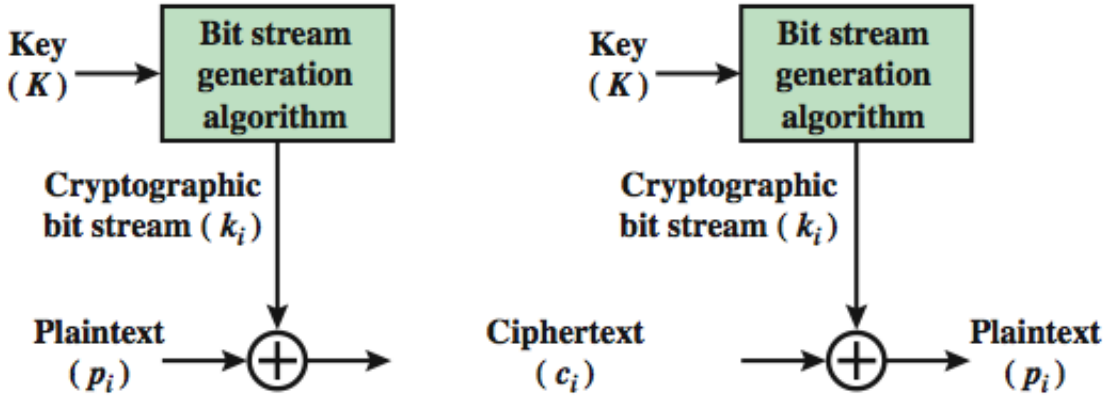
- A block cipher is one in which ***a block*** of plaintext is treated as ***a whole*** and used to produce a ciphertext block of ***equal length***
  - Typically, a block size of 64 or 128 bits is used

cuu duong than cong . com

- A stream cipher is one that encrypts a digital data stream ***one bit*** or ***one byte*** at a time

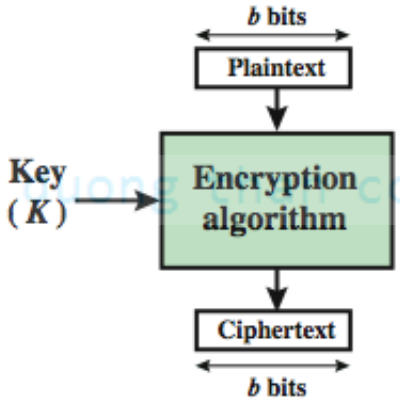
cuu duong than cong . com

Block Cipher vs. Stream Cipher



cuu duong than cong . com

(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

Block Cipher Principles

- Most symmetric block ciphers are *based on* ***a Feistel Cipher Structure***
- Needed since must be able to decrypt ciphertext to recover messages efficiently
- Block ciphers look like an extremely large substitution
- Would need table of 2^{64} entries for a 64-bit block
- Instead create from smaller building blocks
- Using idea of a product cipher

cuu duong than cong . com

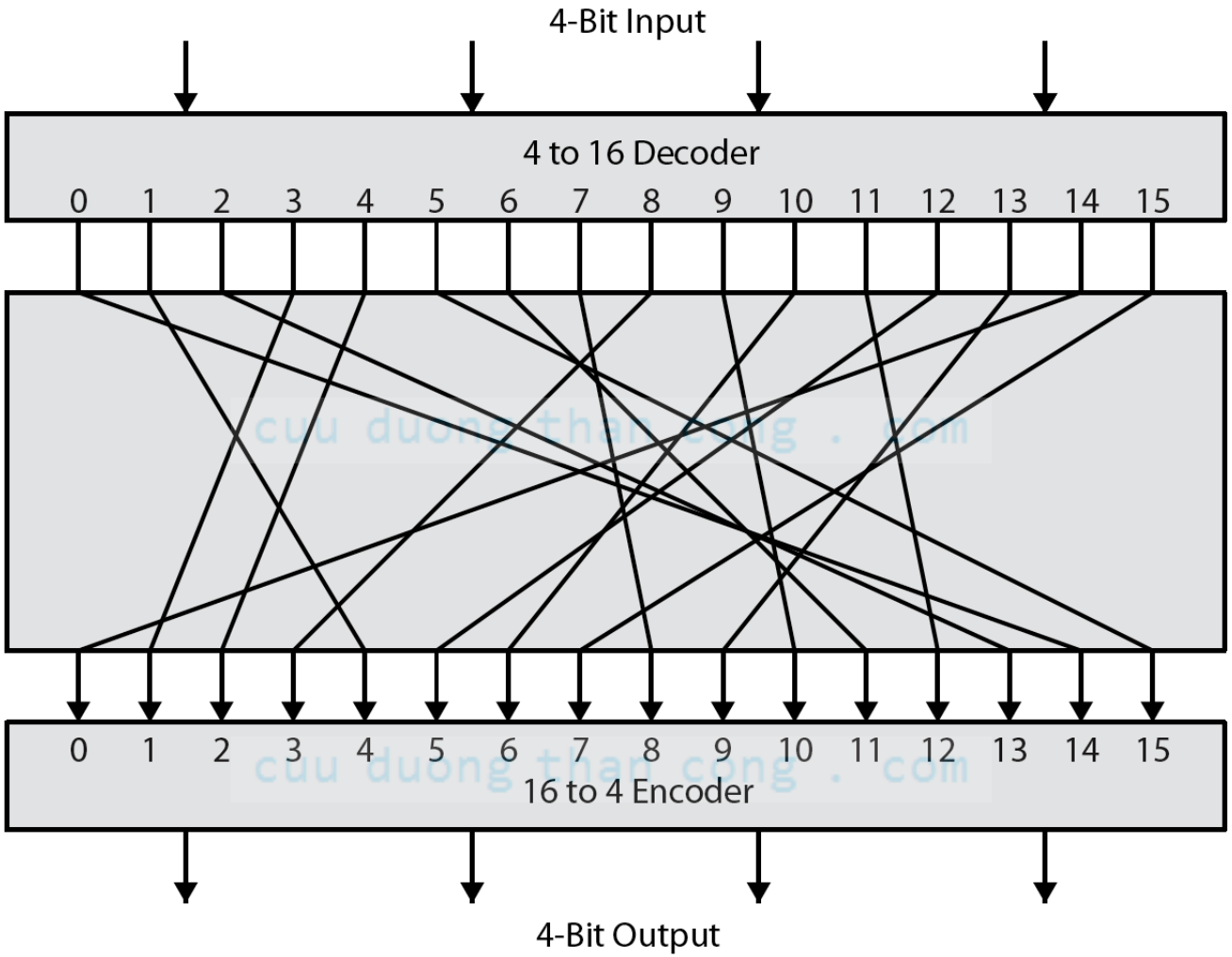
Feistel Cipher Structure

- Feistel cipher is a **block cipher** operates on a plaintext block of ***n bits*** to produce a ciphertext block of ***n bits***.
- There are ***possible different*** plaintext blocks and, for decryption to be possible, each must produce a unique ciphertext block.
- Such a transformation is called reversible, or nonsingular

cuu duong than cong . com

cuu duong than cong . com

Ideal Block Cipher

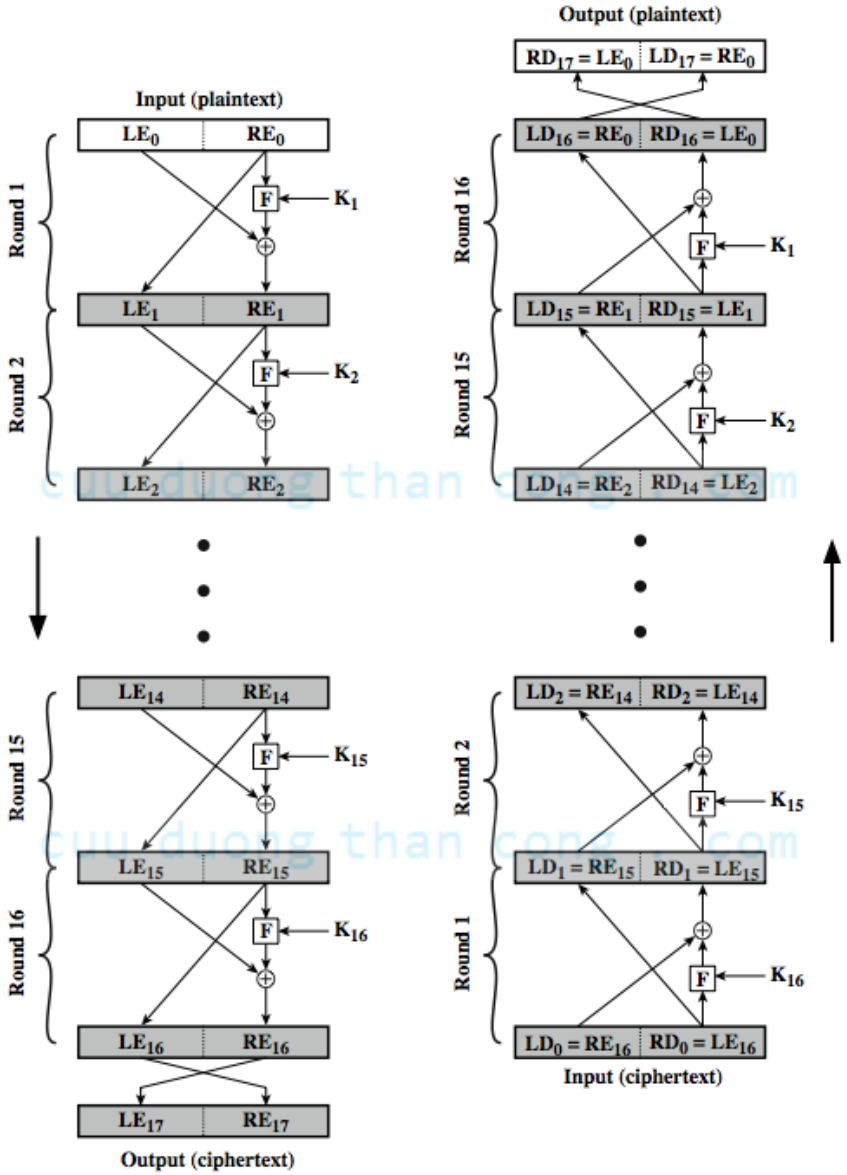


Ideal Block Cipher

- A ***4-bit input*** produces one of ***16 possible input*** states, which is mapped by the substitution cipher into a unique one of 16 possible output states, each of which is represented by ***4 ciphertext bits***.
- This is the most general form of block cipher and can be used to define any reversible mapping between plaintext and ciphertext.
- Feistel refers to this as the ***ideal block cipher***, because it allows for the maximum number of possible encryption mappings from the plaintext block

cuu duong than cong . com

Feistel Cipher Structure



Feistel Cipher Design Elements

- block size
- key size
- number of rounds
- subkey generation algorithm
- round function
- fast software en/decryption
- ease of analysis

cuu duong than cong . com

(See page 75, reference [1])

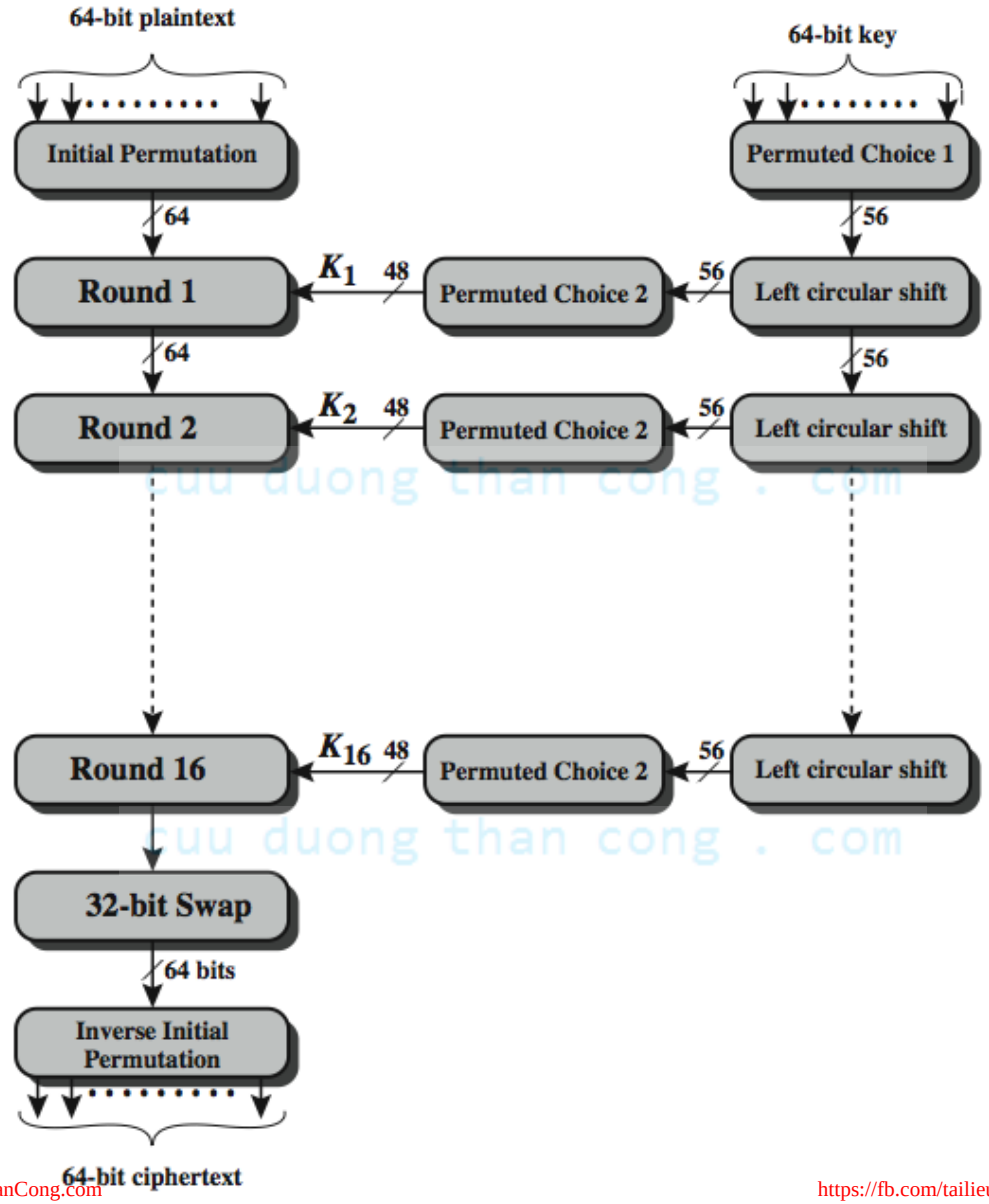
cuu duong than cong . com

Data Encryption Standard (DES)

- The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46).
- The algorithm itself is referred to as the Data Encryption Algorithm (DEA).
- For DES, data are encrypted in ***64-bit blocks*** using a ***56-bit key***.
- The algorithm transforms **64-bit input** in a series of steps into a **64-bit output**.
- The same steps, with the same key, are used to reverse the encryption

cuu duong than cong . com

DES Encryption Overview



cuu duong than cong . com

Data Encryption Standard (DES)

- There are two inputs to the encryption function: the ***plaintext*** to be encrypted and the ***key***.
- In this case, the ***plaintext must be 64 bits*** in length and the ***key is 56 bits*** in length
  - (actually, the function expects a 64-bit key as input. However, only 56 of these bits are ever used; the other 8 bits can be used as parity bits or simply set arbitrarily)

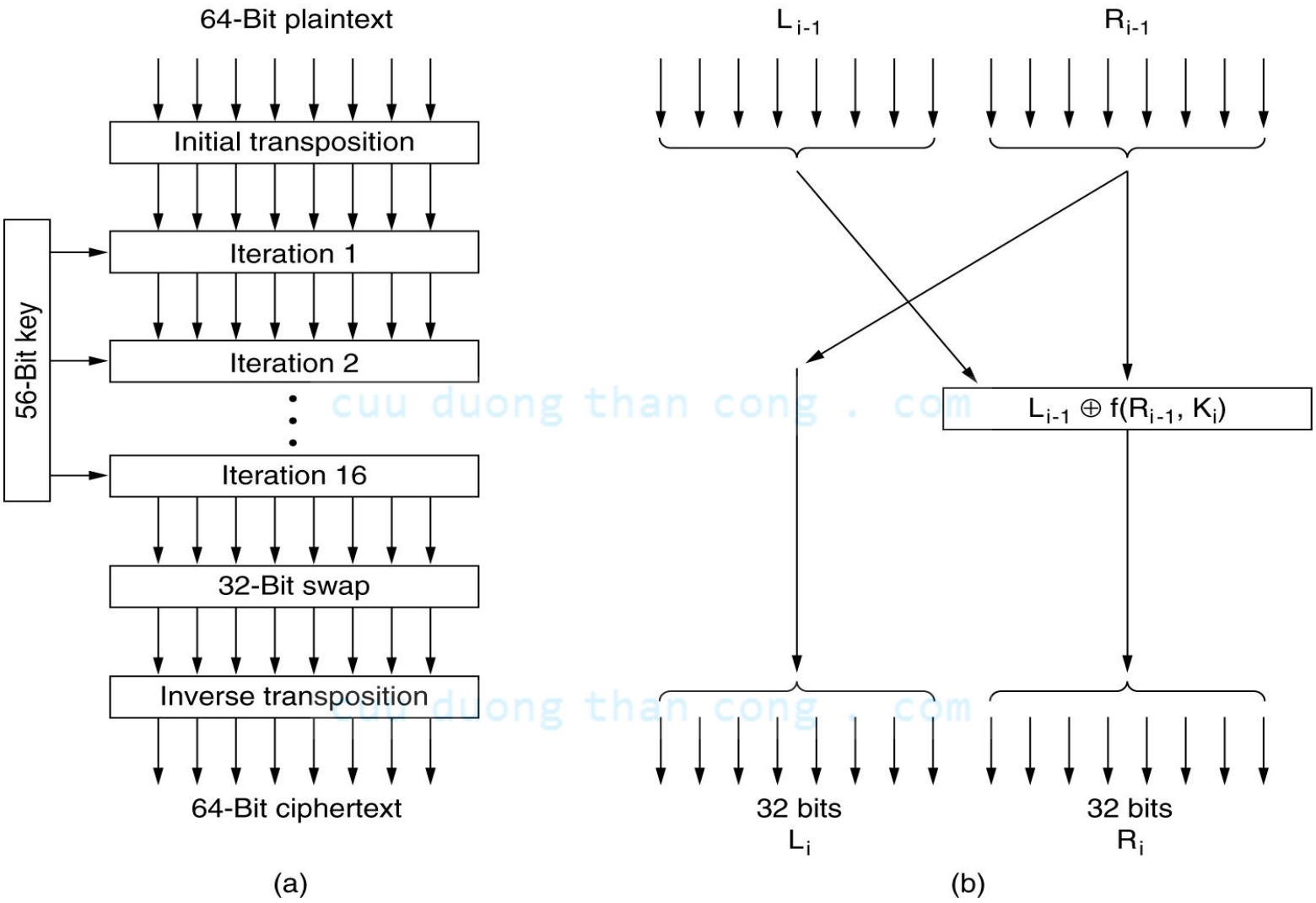
cuu duong than cong . com

Data Encryption Standard (DES)

- Looking at the left-hand side of the figure, we can see that the processing of the plaintext proceeds in three phases.
- ***First***, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input.
- This is followed by a phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions.
- The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key.
- The left and right halves of the output are swapped to produce the preoutput.
- ***Finally***, the preoutput is passed through a permutation that is the inverse of the initial permutation function, to produce the 64-bit ciphertext

cuu duong than cong . com

DES Encryption Overview



The data encryption standard. (a) General outline. (b) Detail of one iteration. The circled + means exclusive OR.

CuuDuongThanCong.com https://fb.com/tailieudientucntt

Initial Permutation

- This is the first step of the data computation
- IP reorders the input data bits
- even bits to LH half, odd bits to RH half
- quite regular in structure (easy in h/w)
- no cryptographic value

cuu duong than cong . com

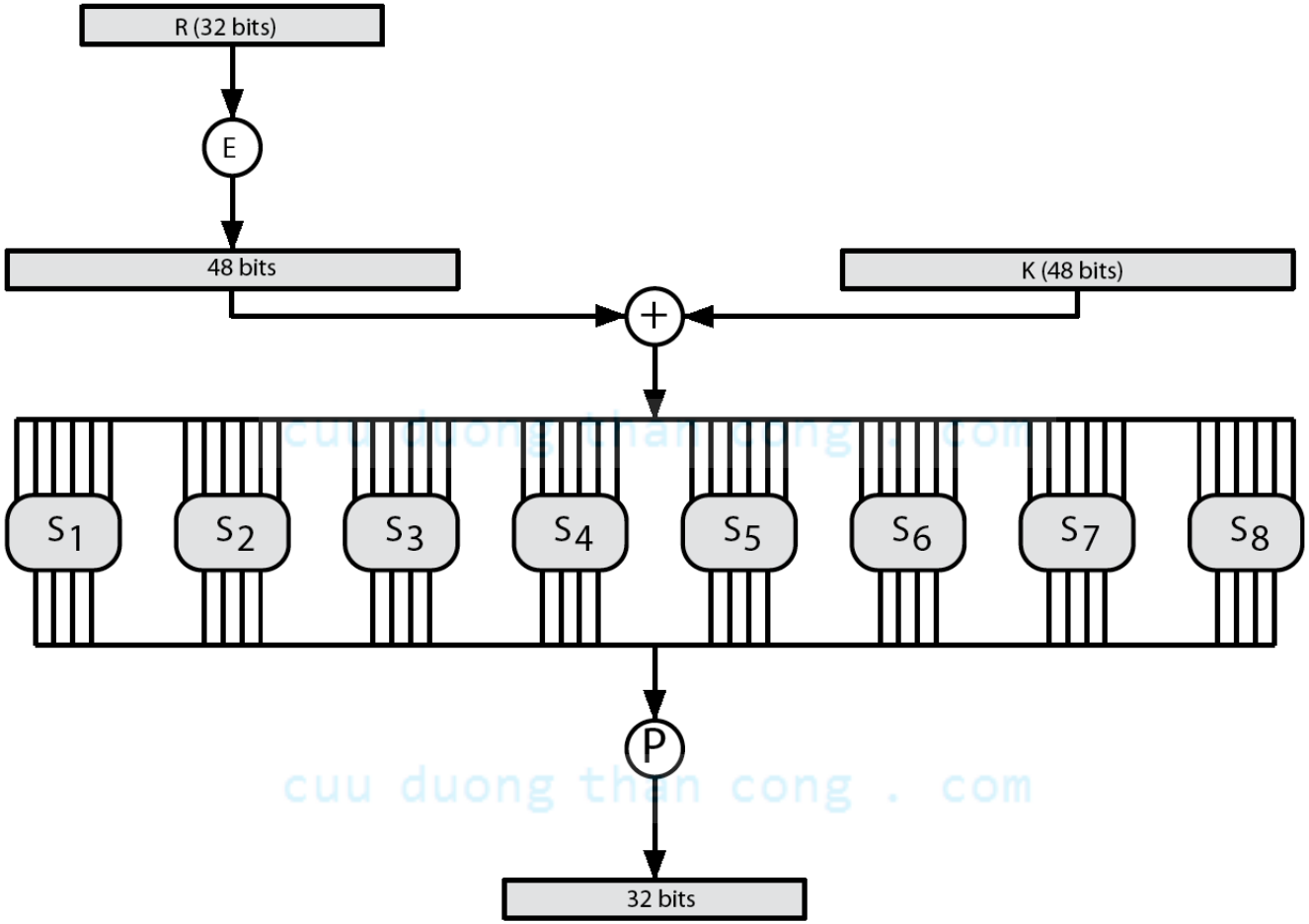
cuu duong than cong . com

DES Round Structure

- Uses two 32-bit L & R halves (*L = Left, R = Right*)
- As for any Feistel cipher can describe as:
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
- F takes 32-bit R half and 48-bit subkey:
  - expands R to 48-bits using perm E
  - adds to subkey using XOR
  - passes through 8 S-boxes to get 32-bit result
  - finally permutes using 32-bit perm P

cuu duong than cong . com

DES Round Structure



cuu duong than cong . com

Summary (1/2)

- A ***block cipher*** is an encryption/decryption scheme in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
- Many block ciphers have a Feistel structure.
- Such a structure consists of a number of ***identical rounds*** of processing.
- In each round, a substitution is performed on one half of the data being processed, followed by a permutation that interchanges the two halves.
- The original key is expanded so that a different key is used for each round.

Summary (2/2)

- The Data Encryption Standard (DES) has been the ***most widely used*** encryption algorithm until recently.
- It exhibits the classic Feistel structure.
- DES uses a 64-bit block and a 56-bit key.
- Two important methods of cryptanalysis are differential cryptanalysis and linear cryptanalysis.
- DES has been shown to be highly resistant to these two types of attack.

cuu duong than cong . com

References

[1] *Cryptography and Network Security*, Principles and Practice, William Stallings, Prentice Hall, Sixth Edition, 2013

cuu duong than cong . com

cuu duong than cong . com