# Block Ciphers and DES

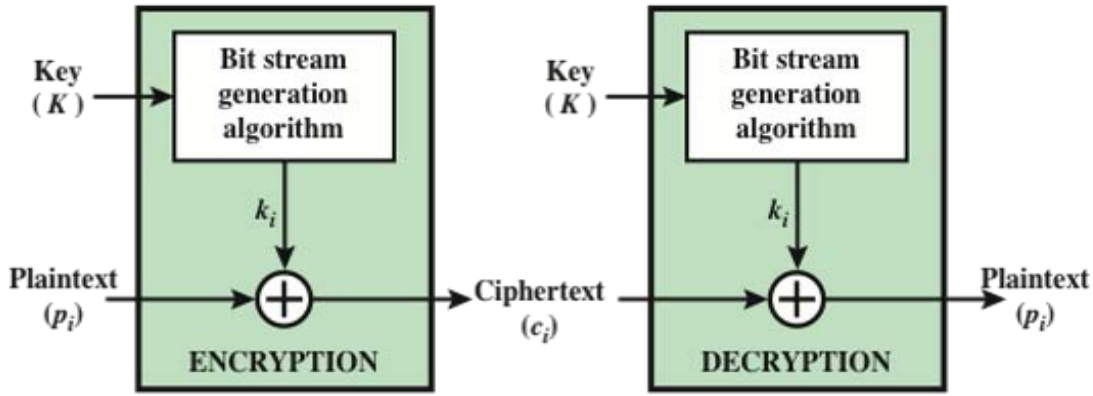
Yih-Kuen Tsay

Department of Information Management
National Taiwan University

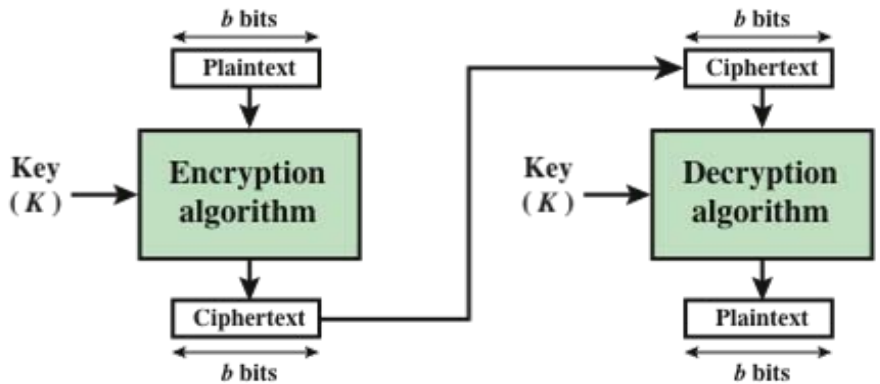
# Block vs. Stream Ciphers

- **Stream Cipher**: encrypt data one bit or one byte at a time.
  - RC4 (classic examples: Vigenère cipher, Vernam cipher)
- **Block Cipher**: encrypt data one block at a time; the size of a block ranges from several bytes to few tens of bytes.
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)
- Using certain modes of operation (to be discussed later), a block cipher can be used to achieve the effect of a stream cipher.
- Block ciphers have a broader range of applications.

# Block vs. Stream Ciphers (cont.)




(a) Stream Cipher Using Algorithmic Bit Stream Generator




(b) Block Cipher

Source: Figure 3.1, Stallings 2014

# Block Ciphers

- n-bit blocks of plaintext $\longrightarrow$ n-bit blocks of ciphertext
- $2^n!$ possible reversible mappings
- Similar to classical substitution cipher when the block size is small
- Arbitrary reversible mappings not practical for a large block size. The mapping itself is the key, requiring $n \times 2^n$ bits; e.g., $64 \times 2^{64} = 2^{70} \approx 10^{21}$.
- Approximation (such as the Feistel Cipher) needed

# Block Substitution

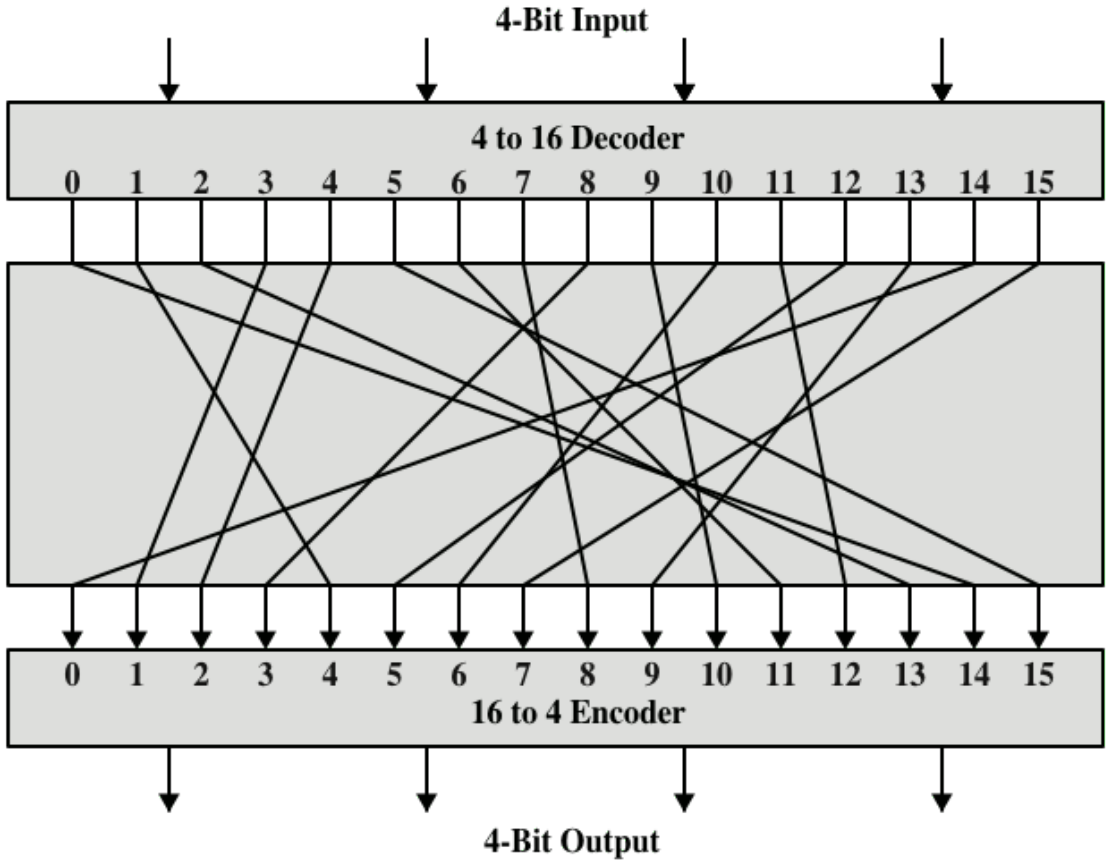



**Figure 3.2 General *n*-bit-*n*-bit Block Substitution (shown with $n = 4$)**

Source: Figure 3.2, Stallings 2014

# Substitution Cipher

| Plaintext | Ciphertext |
|---|---|
| 0000 | 1110 |
| 0001 | 0100 |
| 0010 | 1101 |
| 0011 | 0001 |
| 0100 | 0010 |
| 0101 | 1111 |
| 0110 | 1011 |
| 0111 | 1000 |
| 1000 | 0011 |
| 1001 | 1010 |
| 1010 | 0110 |
| 1011 | 1100 |
| 1100 | 0101 |
| 1101 | 1001 |
| 1110 | 0000 |
| 1111 | 0111 |

| Ciphertext | Plaintext |
|---|---|
| 0000 | 1110 |
| 0001 | 0011 |
| 0010 | 0100 |
| 0011 | 1000 |
| 0100 | 0001 |
| 0101 | 1100 |
| 0110 | 1010 |
| 0111 | 1111 |
| 1000 | 0111 |
| 1001 | 1101 |
| 1010 | 1001 |
| 1011 | 0110 |
| 1100 | 1011 |
| 1101 | 0010 |
| 1110 | 0000 |
| 1111 | 0101 |

Source: Table 3.1, Stallings 2014

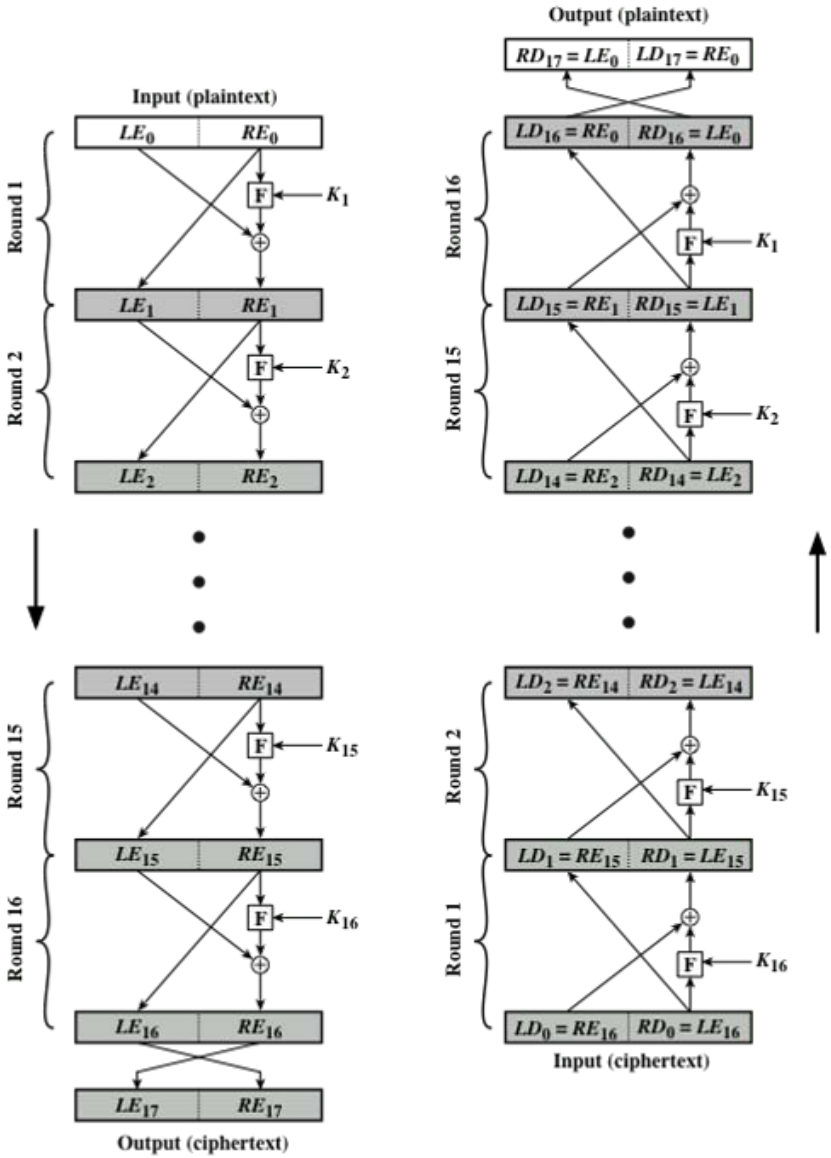
# Diffusion and Confusion

- Basic building blocks for any cipher
- Methods for thwarting statistical cryptanalysis
- Ideally, all statistics of the ciphertext should be independent of the particular key used.
- Diffusion: make the statistical relationship between the plaintext and ciphertext as complex as possible, by having each plaintext digit (bit) affect the value of many ciphertext digits (bits). Achieved by permutation plus some function.
- Confusion: make the statistical relationship between the ciphertext and the encryption key as complex as possible. Achieved by complex substitution (linear substitutions such as the Caesar cipher would add little confusion).

# The Feistel Cipher

- Approximate the ideal substitution cipher by a product cipher, i.e., two or more basic ciphers in sequence
- Alternate **substitutions** and **permutations** (cf. confusion and diffusion)
- Its structure used by many symmetric block ciphers currently in use

# Feistel Encryption and Decryption




Source: Figure 3.3, Stallings 2014

# Parameters of Feistel Networks

- Block size: typically 64 bits
- Key size: typically 128 bits
- Number of rounds: typically 16 rounds
- Subkey generation algorithm: the more complex the more secure
- Round function: the more complex the more secure

# Correctness of Feistel Decryption

Let's just check if the last round of decryption is correct.

Input: $LD_0 = LE_{17} = RE_{16}$ and $RD_0 = RE_{17} = LE_{16}$.

On the encryption side,

$$\begin{aligned} LE_{16} &= RE_{15} \\ RE_{16} &= LE_{15} \oplus F(RE_{15}, K_{16}) \end{aligned}$$

On the decryption side,

$$\begin{aligned} LD_1 &= RD_0 = LE_{16} = RE_{15} \\ RD_1 &= LD_0 \oplus F(RD_0, K_{16}) \\ &= RE_{16} \oplus F(RE_{15}, K_{16}) \\ &= [LE_{15} \oplus F(RE_{15}, K_{16})] \oplus F(RE_{15}, K_{16}) \\ &= LE_{15} \end{aligned}$$

# Feistel Example

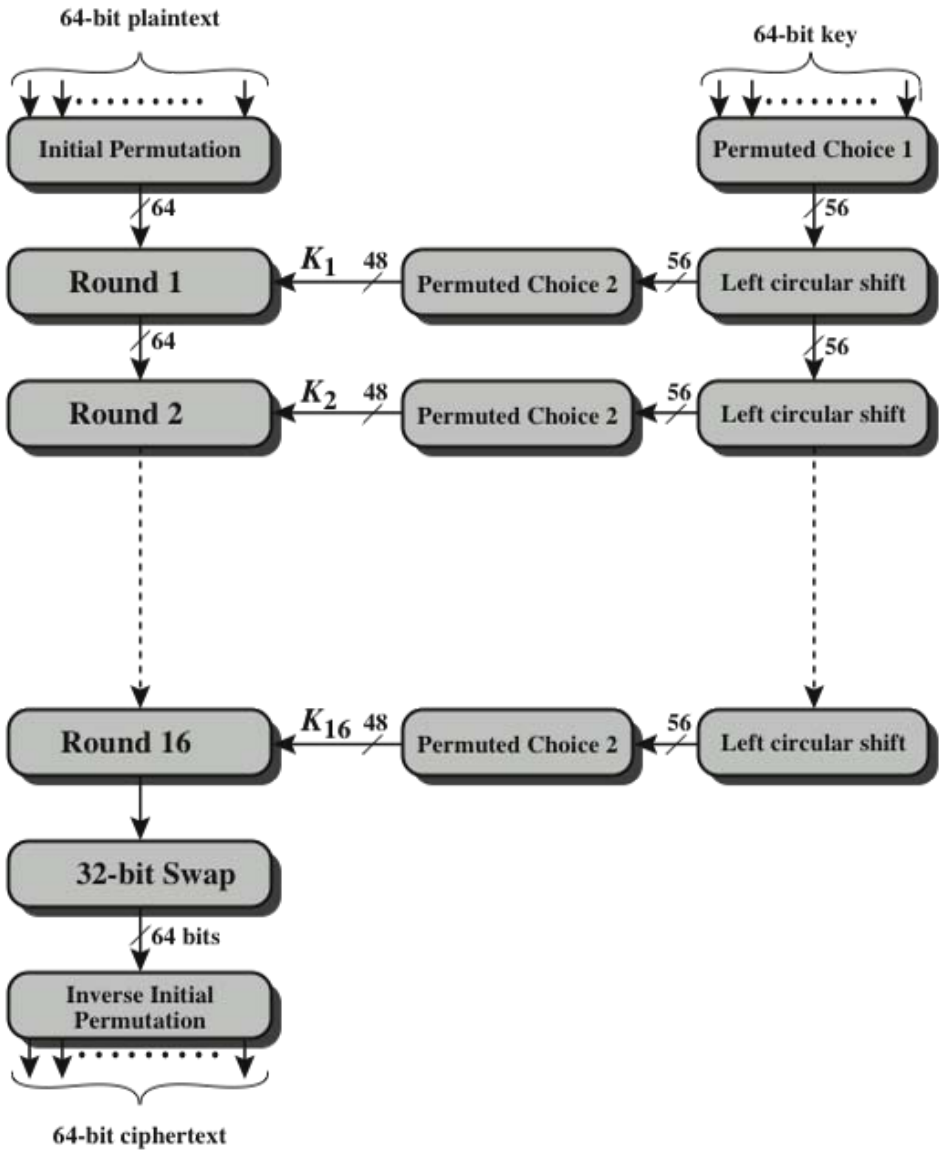

**Figure 3.4 Feistel Example**

Source: Figure 3.4, Stallings 2014

# The Data Encryption Standard (DES)

- Once most widely used (prior to the AES)
- Data encrypted in 64-bit blocks using a 56-bit key
- History:
  - LUCIFER (1971): developed by IBM; 128-bit keys.
  - Refined LUCIFER (1973): developed by IBM and NSA; 56-bit keys (to fit on a chip).
  - DES (1977): proposed by IBM and adopted (as FIPS PUB 46) by NBS, now NIST; a slightly modified version of the Refined LUCIFER; 56-bit keys.
  - Withdrawn by NIST in 2005.

# DES Encryption




Source: Figure 3.5, Stallings 2014

# Permutation Tables for DES

**(a) Initial Permutation (IP)**

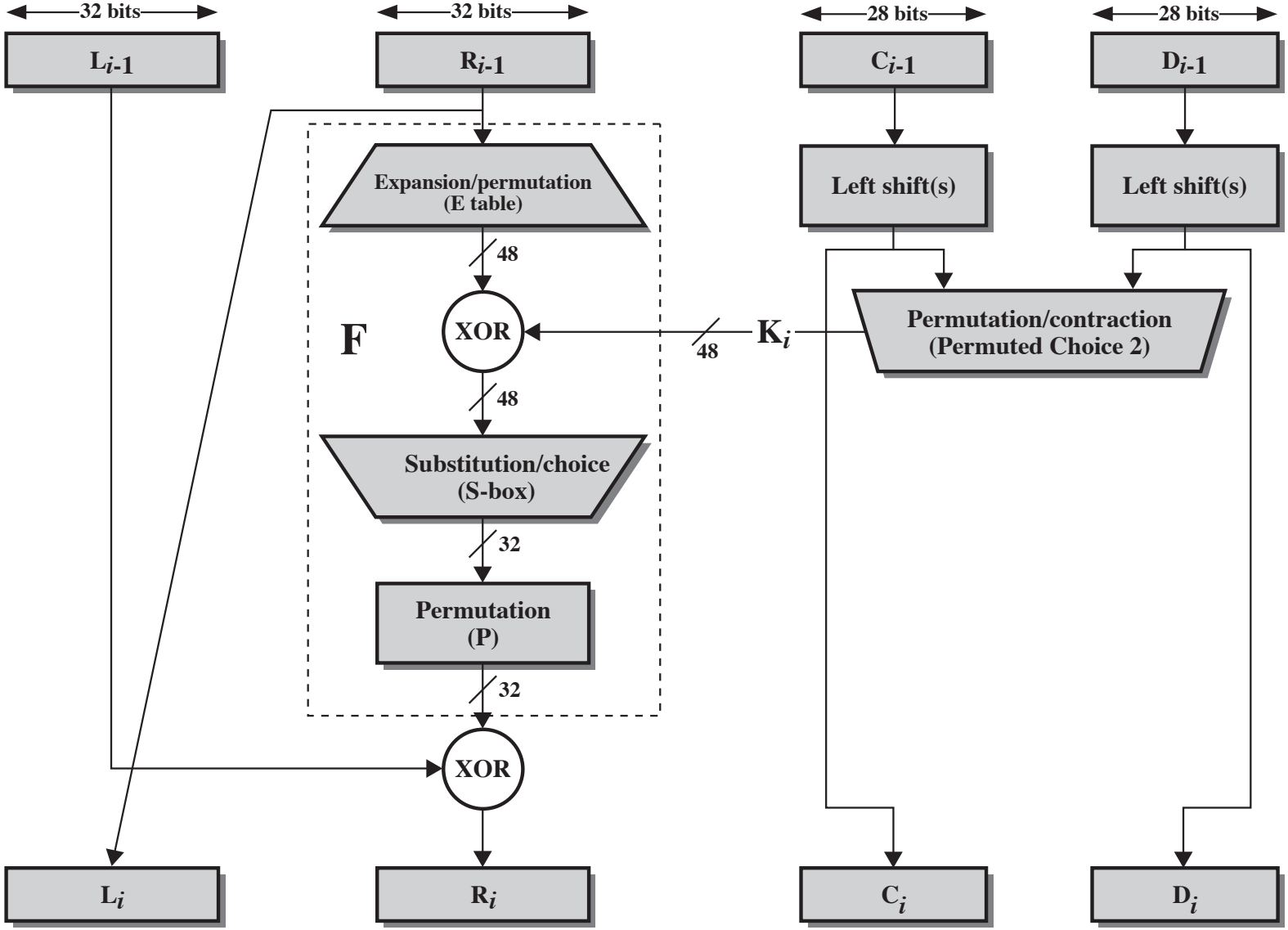
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

**(b) Inverse Initial Permutation ($IP^{-1}$)**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

Source: Table 3.2, Stallings 2010

# Single Round of DES




Source: Figure 3.6, Stallings 2010

# Permutation Tables for DES (cont.)

**(c) Expansion Permutation (E)**

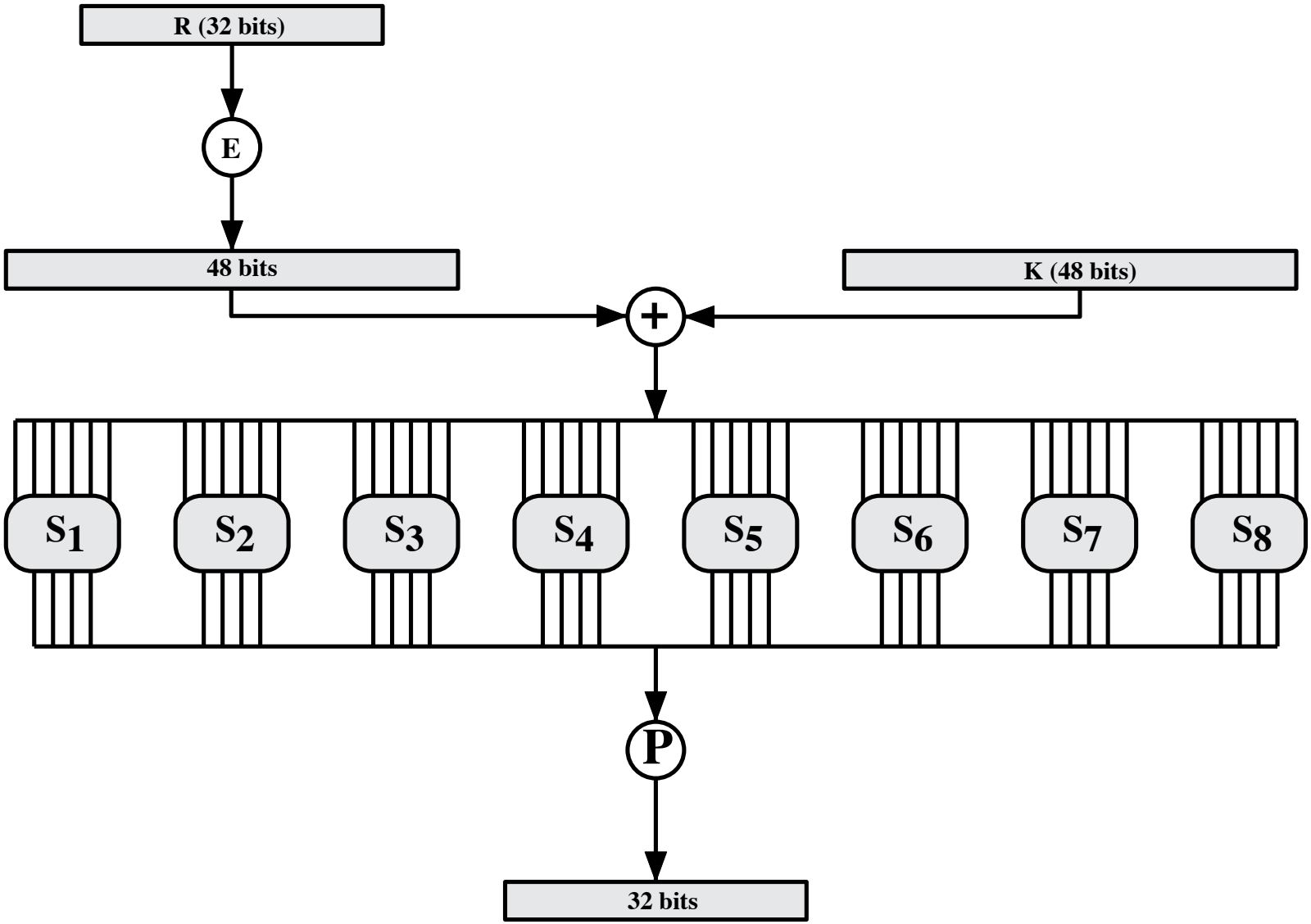
| | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

**(d) Permutation Function (P)**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

Source: Table 3.2, Stallings 2010

# Calculation of F(R,K)




Source: Figure 3.7, Stallings 2010

# DES S-Boxes

$S_1$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

$S_2$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |

$S_3$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |

$S_4$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |

$S_5$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |

$S_6$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |

$S_7$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |

$S_8$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

Source: Table 3.3, Stallings 2010

# DES Key Scheduling

**(a) Input Key**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 |
| 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |

Source: Table 3.4, Stallings 2010

# DES Key Scheduling (cont.)

**(b) Permuted Choice One (PC-1)**

| | | | | | | |
|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 |

**(c) Permuted Choice Two (PC-2)**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 |
| 15 | 6 | 21 | 10 | 23 | 19 | 12 | 4 |
| 26 | 8 | 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 |
| 51 | 45 | 33 | 48 | 44 | 49 | 39 | 56 |
| 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

**(d) Schedule of Left Shifts**

| Round Number | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bits Rotated | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

Source: Table 3.4, Stallings 2010

# The Avalanche Effect

- The avalanche effect of an encryption algorithm refers to the property that a small change in either the plaintext or the key should produce a significant change in the ciphertext.
- In particular, a change in one bit of the plaintext or the key should produce a change in many bits of the ciphertext.
- DES exhibits a strong avalanche effect.

# Avalanche Effect in DES

| (a) Change in Plaintext | | (b) Change in Key | |
|---|---|---|---|
| Round | Number of bits that differ | Round | Number of bits that differ |
| 0 | 1 | 0 | 0 |
| 1 | 6 | 1 | 2 |
| 2 | 21 | 2 | 14 |
| 3 | 35 | 3 | 28 |
| 4 | 39 | 4 | 32 |
| 5 | 34 | 5 | 30 |
| 6 | 32 | 6 | 32 |
| 7 | 31 | 7 | 35 |
| 8 | 29 | 8 | 34 |
| 9 | 42 | 9 | 40 |
| 10 | 44 | 10 | 38 |
| 11 | 32 | 11 | 31 |
| 12 | 30 | 12 | 33 |
| 13 | 30 | 13 | 28 |
| 14 | 26 | 14 | 26 |
| 15 | 29 | 15 | 34 |
| 16 | 34 | 16 | 35 |

Source: Table 3.5, Stallings 2006

# Breaking DES

- Searching the 56-bit key space (about $7.2 \times 10^{16}$ keys)
  - The "DES Cracker" machine by the Electronic Frontier Foundation (1998)
    - It cost less than $250,000 to build
    - The attack took less than three days
- Exploiting the characteristics of DES
  - Weakness in the S-boxes (none found so far)
  - Timing attacks (unlikely to succeed)
    (Timing attacks exploit the fact that an encryption or decryption implementation may take different amounts of time on different inputs.)

# Exhaustive Key Search

| Key size (bits) | Cipher | Number of Alternative Keys | Time Required at $10^9$ decryptions/s | Time Required at $10^{13}$ decryptions/s |
|---|---|---|---|---|
| 56 | DES | $2^{56} \approx 7.2 \times 10^{16}$ | $2^{55}$ ns = 1.125 years | 1 hour |
| 128 | AES | $2^{128} \approx 3.4 \times 10^{38}$ | $2^{127}$ ns = $5.3 \times 10^{21}$ years | $5.3 \times 10^{17}$ years |
| 168 | Triple DES | $2^{168} \approx 3.7 \times 10^{50}$ | $2^{167}$ ns = $5.8 \times 10^{33}$ years | $5.8 \times 10^{29}$ years |
| 192 | AES | $2^{192} \approx 6.3 \times 10^{57}$ | $2^{191}$ ns = $9.8 \times 10^{40}$ years | $9.8 \times 10^{36}$ years |
| 256 | AES | $2^{256} \approx 1.2 \times 10^{77}$ | $2^{255}$ ns = $1.8 \times 10^{60}$ years | $1.8 \times 10^{56}$ years |
| 26 characters (permutation) | Monoalphabetic | $26! = 4 \times 10^{26}$ | $2 \times 10^{26}$ ns = $6.3 \times 10^{9}$ years | $6.3 \times 10^{6}$ years |

(Note: the exponents are distorted, due to graphics incompatibility.)

Source: Table 3.5, Stallings 2014

# Block Cipher Design Principles

- **Number of rounds**: chosen so that known cryptanalytic efforts require greater effort than a brute-force key search attack.
- **Design of function F**
  - Design criteria for F: nonlinearity, strict avalanche, bit independence, etc.
  - S-Box design: any change to the input vector to an S-box results in random-looking changes to the output.
    In DES, S-Boxes are the main component of the function F and the only non-linear part of the entire DES.
- **Key schedule algorithm**: maximize the difficulty of deducing individual subkeys and of working back to the main key.

# Function F and S-Box Design Criteria

- **Nonlinearity**
- **Strict avalanche**:
  Any output bit should change with probability $\frac{1}{2}$ when any single input bit is inverted.
- **Guaranteed avalanche**:
  Guaranteed avalanche of order $\gamma$ ensures that, for a 1-bit input change, at least $\gamma$ output bits change.
- **Bit independence**:
  Any two output bits should change independently when any single input bit is inverted.

# S-Box Design Approaches

- Random with or without testing
- Man-made: manual with simple supporting math
- Math-made: applying math principles to achieve proven security