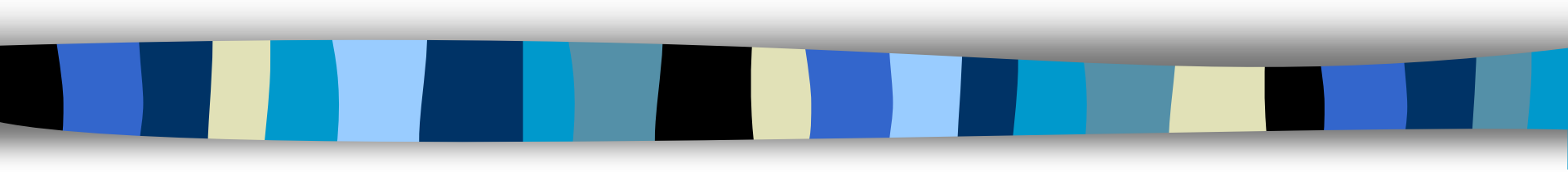
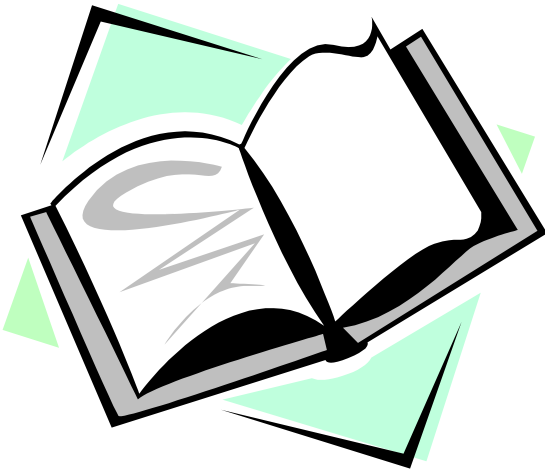
# Cryptography
# CS 555



## Topic 9: Block Cipher Construction & DES

# Outline and Readings

- Outline
  - Substitution-Permutation Networks
  - Feistel networks
  - DES
- Readings:
  - Katz and Lindell: 5.1,5.2,5.3



# Why Block Ciphers?

- Another way to defeat frequency analysis
  - Make the unit of transformation larger, rather than encrypting letter by letter, encrypting block by block
- Provide an efficient implementation for PRF and PRP
- Block ciphers are important building blocks for constructing encryption schemes

# Block Ciphers

- A block cipher is an efficient, keyed permutation $F: \{0,1\}^n \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$
  - $F_k(x) = F(k,x)$ is a bijection (permutation)
  - Block size: $\ell$
  - Key size: n

# Truly Random Permutation

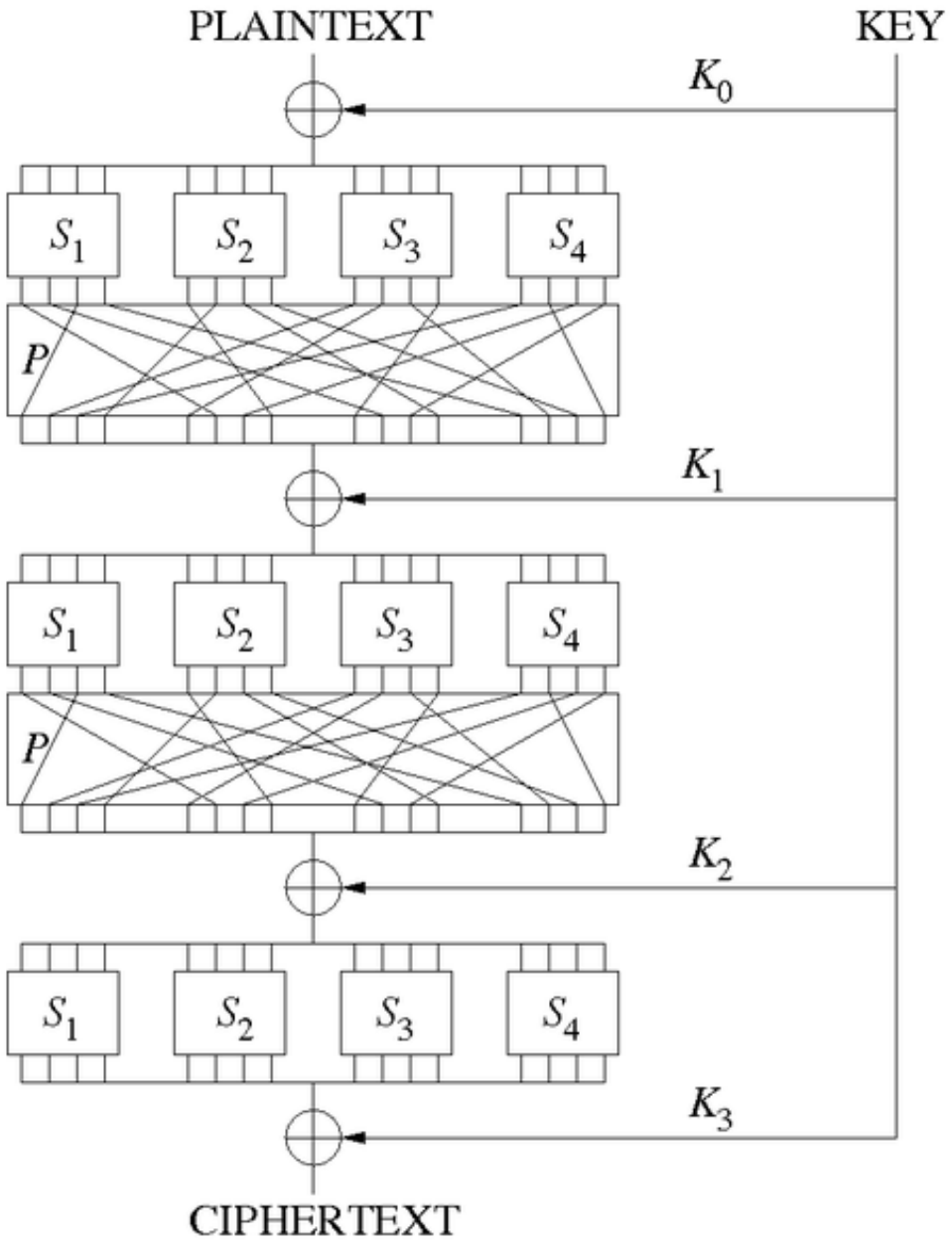
- The truly random permutation is a substitution cipher from $\{0,1\}^n$ to $\{0,1\}^n$
  - total number of keys: $2^n!$
  - insecure when n is small
  - impractical when n is large: key length
    $s = \log(2^n!) > (n-1)2^{n-1}$
  - Block ciphers approximate random permutation for large n
  - Use a subset of the $2^n!$ possible permutations

# Confusion-Diffusion Paradigm

- Construct block cipher from many smaller random (or random-looking) permutations
- Confusion: e.g., for block size 128, uses 16 8-bit random permutation
  - $F_k(x) = f_1(x_1) \ldots f_{16}(x_{16})$
  - Where key k selects 16 8-bit random permutation.
  - Does $F_k(\cdot)$ look like a random permutation?
- Diffusion: bits of $F_k(x)$ are permuted (re-ordered)
- Multiple rounds of confusion and diffusion are used.

# Substitution-Permutation Networks

- A variant of the Confusion-Diffusion Paradigm
  - $\{f_i\}$ are fixed and are called s-boxes
  - Sub-keys are XORed with intermediate result
    - Sub-keys are generated from the master key according to a key schedule
- Each round has three steps
  - Message XORed with sub-key
  - Message divided and went through s-boxes
  - Message goes through a mixing permutation (bits reordered)




Taken from http://en.wikipedia.org/wiki/Substitution-permutation_network

# Design Principles of Substitution-Permutation Networks

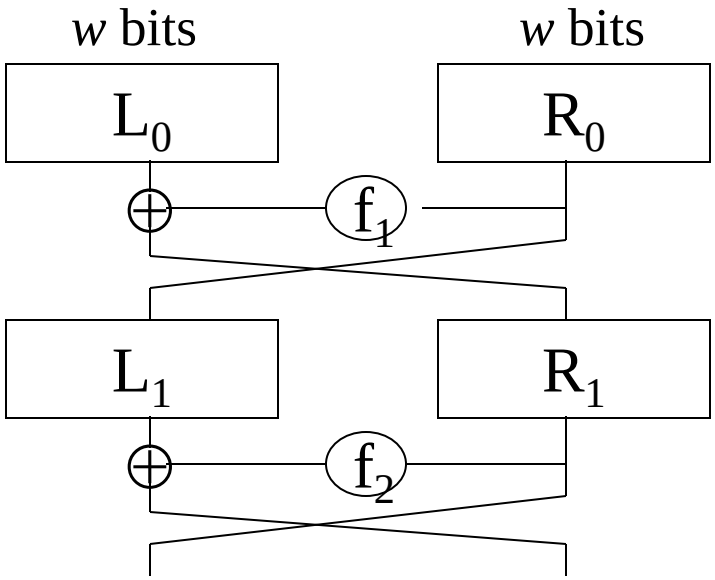
- Design Principle 1. S-boxes are invertible

- Design Principle 2. The avalanche effect: small changes in input result in large changes in output.
  - A single-bit difference in each s-box results in changes in at least two bits in output
  - The mixing permutation distributes the output bits of any s-box into different s-boxes
  - The above, with sufficient number of rounds, achieves the avalanche effect.

# Feistel Network

- A high-level structure that constructs an invertible function from non-invertible components
  - Components do not need to be invertible
  - Can thus behave “more randomly”
- A Feistel Network is fully specified given
  - the block size: n = 2w
  - number of rounds: d
  - d round functions $f_1, \ldots, f_d: \{0,1\}^w \rightarrow \{0,1\}^w$
- Used in DES, IDEA, RC5, and many other block ciphers; but not in AES

# Feistel Network



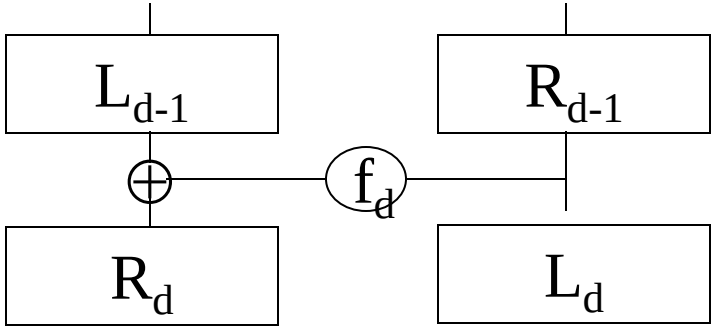

Encryption:

$L_1=R_0$ $R_1=L_0 \oplus f_1(R_0)$

$L_2=R_1$ $R_2=L_1 \oplus f_2(R_1)$

…

$L_d=R_{d-1}$ $R_d=L_{d-1} \oplus f_d(R_{d-1})$




Decryption:

$R_{d-1}=L_d$ $L_{d-1}=R_d \oplus f_d(L_d)$

…

$R_0=L_1$; $L_0=R_1 \oplus f_1(L_1)$

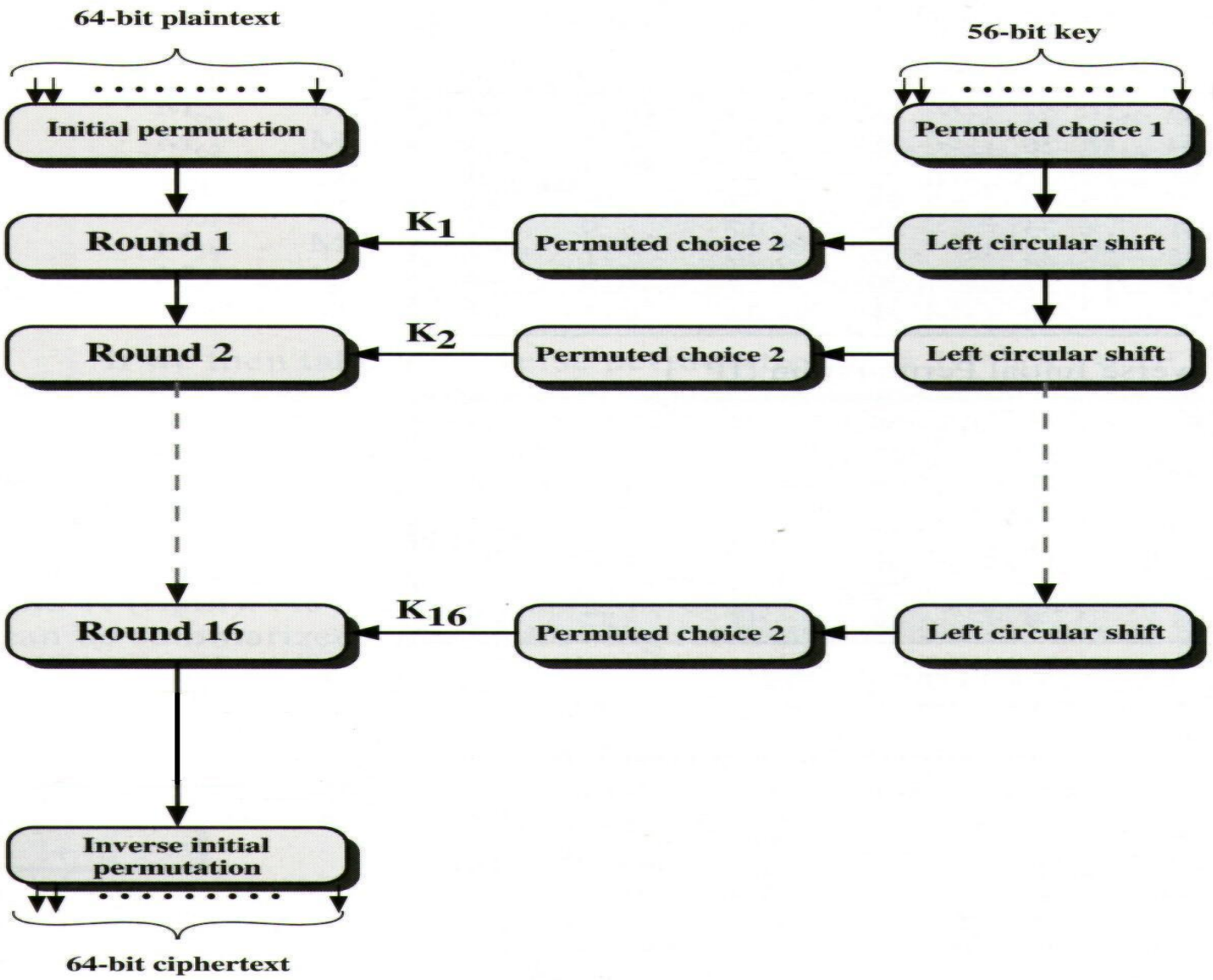
# Feistel Network

- Always invertible no matter what the round function is.
- Each round function is similar to that in the substitution-permutation network
  - Except that the s-boxes do not need to be invertible

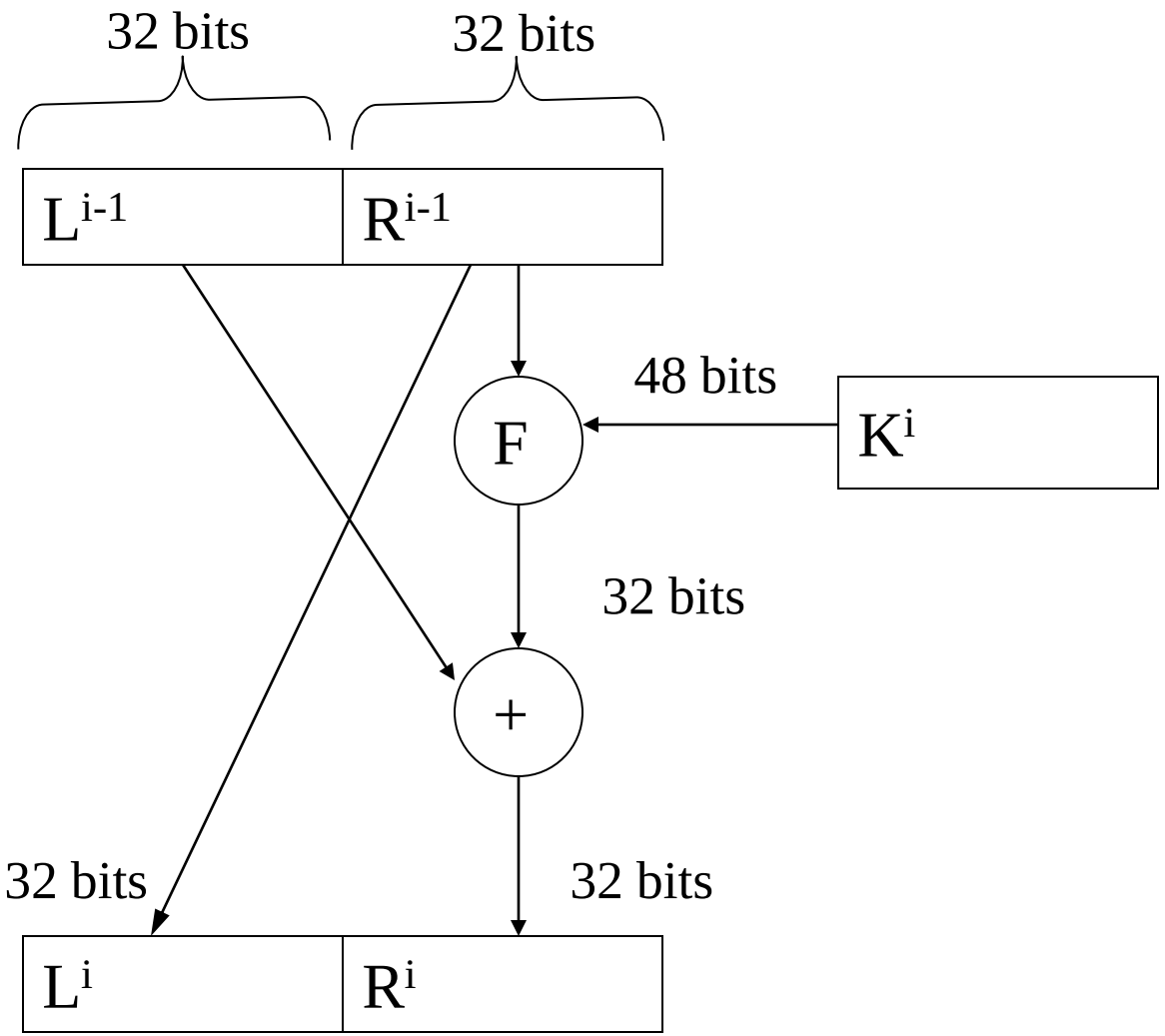
# Data Encryption Standard (DES)

- Designed by IBM, with modifications proposed by the National Security Agency
- US national standard (and de facto international standard) from 1977 to 2001
- Block size 64 bits; Key size 56 bits; 16-round Feistel network
- Designed mostly for hardware implementations
- Considered insecure now because of short key length
  - vulnerable to brute-force attacks

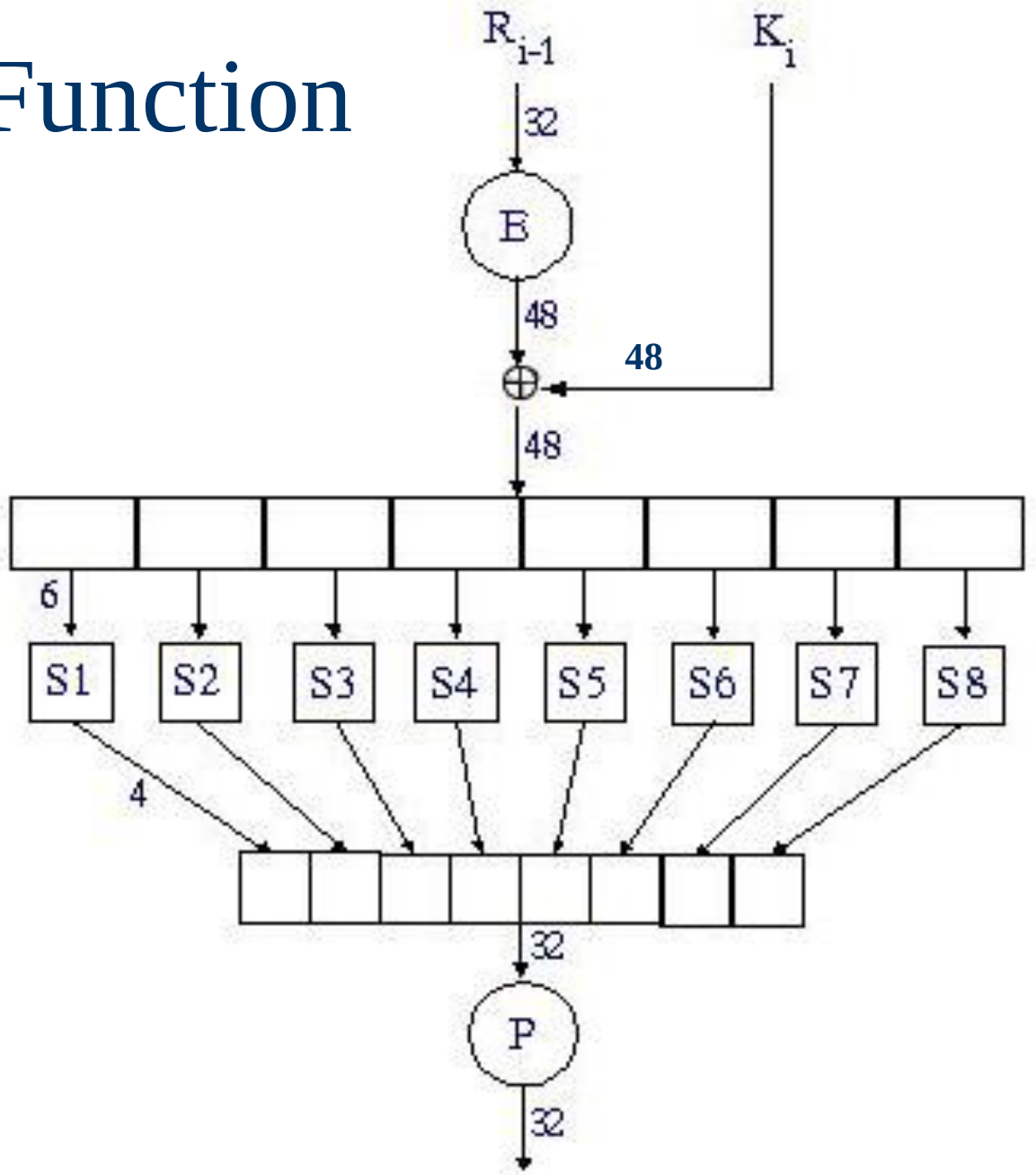
# DES Structure



# DES Round i

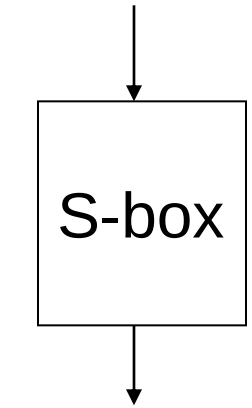


# DES f Function



# S-boxes

- S-boxes are the only non-linear elements in DES design




$B = b_1 b_2 b_3 b_4 b_5 b_6$

$b_1 b_6$ = r = row  c = column

S = matrix 4 x 16, values from 0 to 15

C = Binary representation of S(r,c)

8 S-boxes

# About the S-boxes …

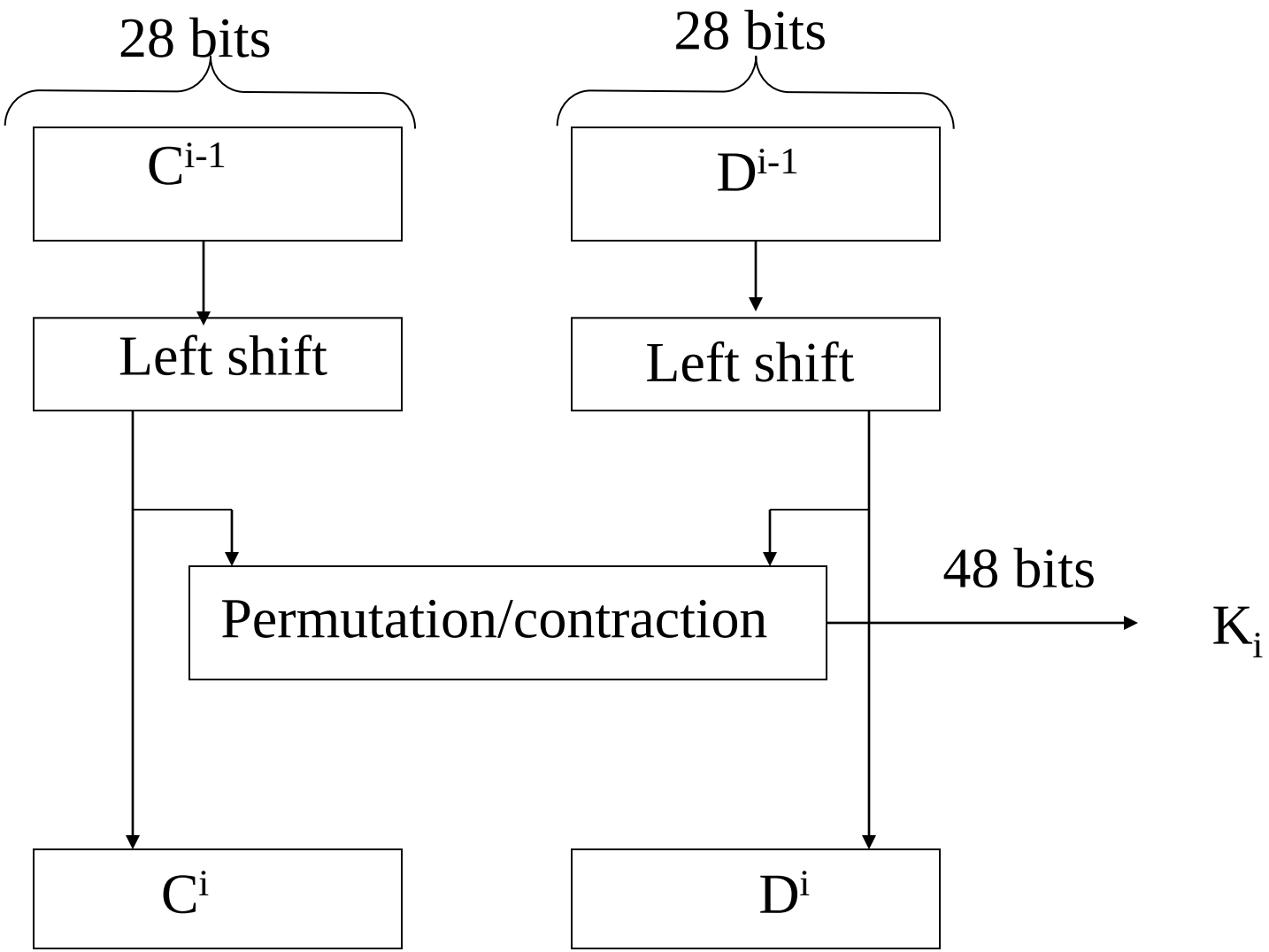
Example: $S_1$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

$S(i, j) \in \{0,1,\ldots,15\}$, corresponds to 4 bits

- Each row is a permutation of {0,1,…,15}.
- Changing one bit in input changes at least two bits in output

# DES Key Scheduling



# DES Weak Keys

- Definition: A DES weak key is a key K such that $E_K(E_K(x))=x$ for all x, i.e., encryption and the decryption is the same
  - these keys make the same sub-key to be generated in all rounds.
- DES has 4 weak keys (only the 56-bit part of it)

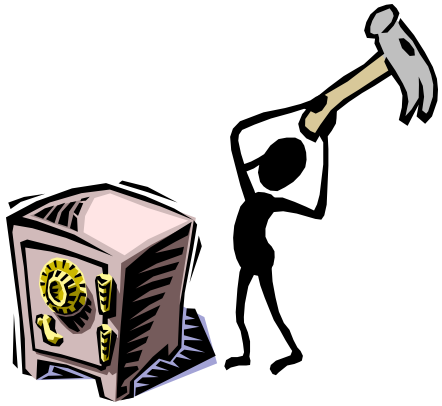
  0000000 0000000

  0000000 FFFFFFF

  FFFFFFF 0000000

  FFFFFFF FFFFFFF
- Weak keys should be avoided at key generation.

# Exhaustive Key Search of DES



**Brute Force:**

- Known-Plaintext Attack
- Try all $2^{56}$ possible keys
- Requires constant memory
- Time-consuming
- DES challenges: (RSA)
  - msg="the unknown message is :xxxxxxxx"
  - CT=" C1 | C2 | C3 | C4"
  - 1997 Internet search: 3 months
  - 1998 EFF machine (costs $250K): 3 days
  - 1999 Combined: 22 hours

# Coming Attractions …

- Block cipher security & AES
- Reading: Katz & Lindell: 5.4,5.5,5.6