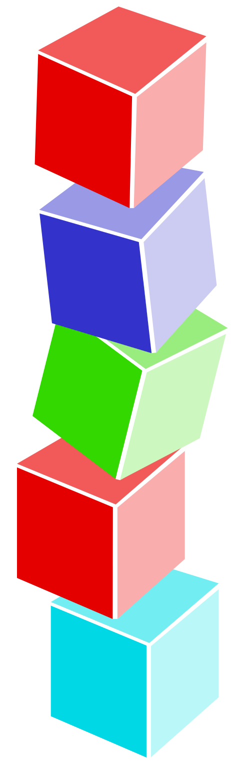
Cristina Nita-Rotaru

CS355: Cryptography

Lecture 7: Block ciphers. DES

Block ciphers

- Map n-bit plaintext blocks to n-bit ciphertext blocks (n: block length).
- For n-bit plaintext and ciphertext blocks and a fixed key, the encryption function is a bijection; $E : P_n \times K \rightarrow C_n$ s.t. for all key $k \in K$, $E(x, k)$ is an invertible mapping written $E_k(x)$.
- The inverse mapping is the decryption function, $y = D_k(x)$ denotes the decryption of plaintext x under k.



Block ciphers features

- Block size: in general larger block sizes mean greater security.
- Key size: larger key size means greater security (larger key space).
- Number of rounds: multiple rounds offer increasing security.
- Encryption modes: define how messages larger than the block size are encrypted, very important for the security of the encrypted message.

An insecure block cipher: Hill cipher

- Use linear equations
  - Each output bit is a linear combination of the input bits
  - the key k is a matrix
    - $C = k M$
    - $M = k^{-1} C$
  - Easily breakable by known-plaintext attack

Hill cipher: Example

- Consider the encryption defined by

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

- Consider the plaintext

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

- Corresponding ciphertext is

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \bmod 26$$

Hill cipher: Example (cont)

- To decipher need to computer inverse of

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

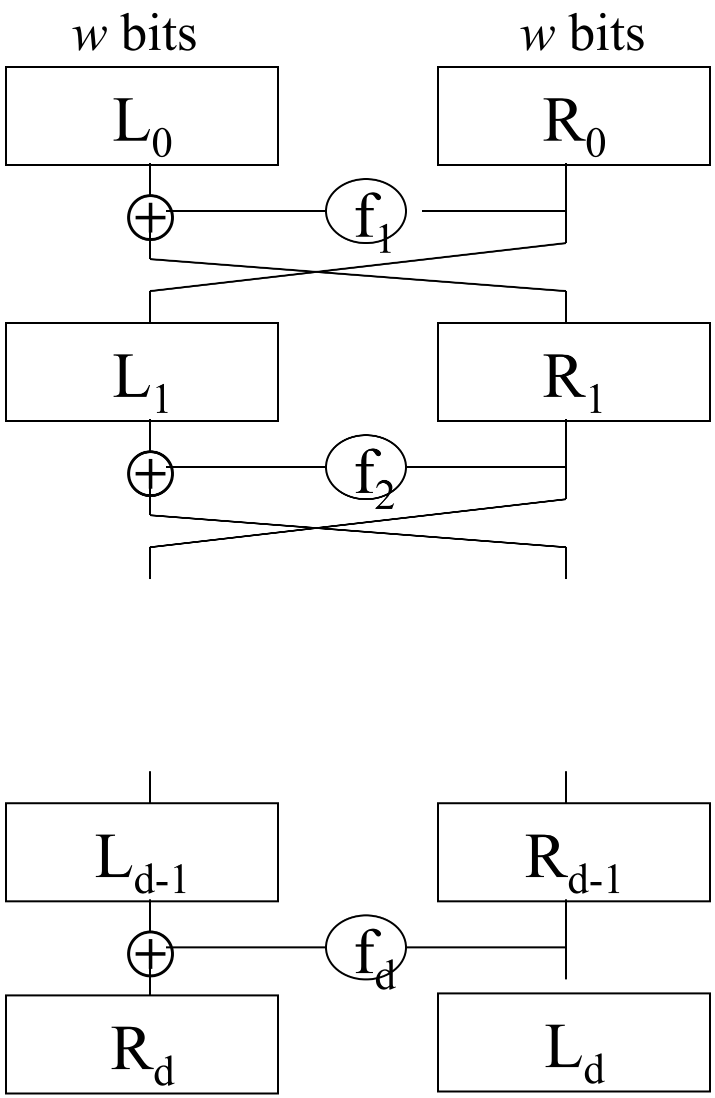
- Inverse is

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \bmod 26$$

Feistel network

- Symmetric structure used in the design on block ciphers such as DES, IDEA, RC5
- A Feistel Network is fully specified given
  - Block size: $n = 2w$
  - Number of rounds: d
  - Specification of each of the d round functions $f_1, \ldots, f_d: \{0,1\}^w \rightarrow \{0,1\}^w$
- Not used in AES

Feistel network



Encryption:

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

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

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

Decryption:

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

$\ldots$

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

A Word about NIST and standards

- ``Founded in 1901 NIST (former NBS) is a non-regulatory federal agency within the U.S. Commerce Department' s Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.''
- Cryptographic Standards & Applications.
- Federal Information Processing Standards (FIPS): define security standards.

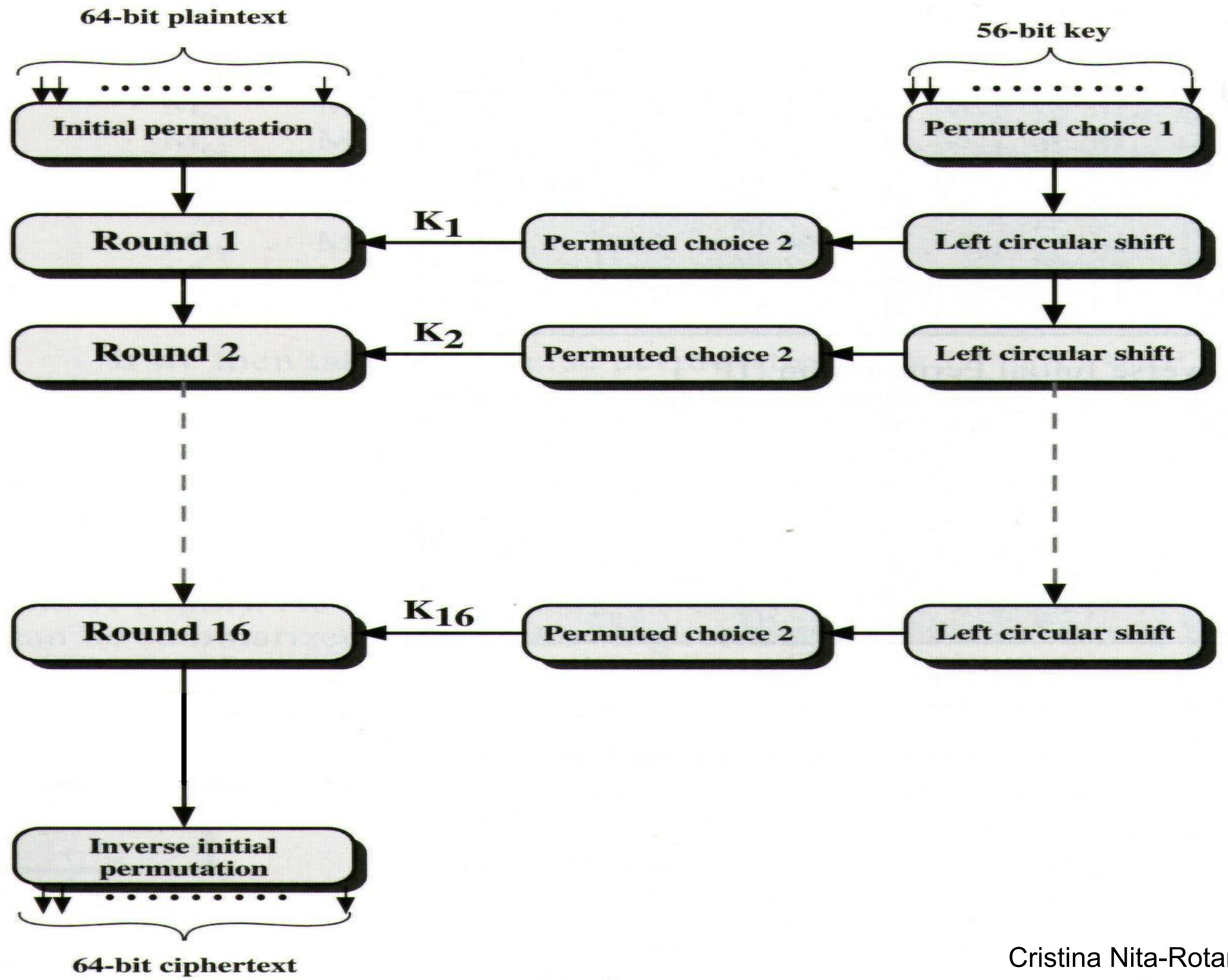
History of Data Encryption Standard (DES)

- 1967: Feistel at IBM
  - Lucifer: block size 128; key size 128 bit
- 1972: NBS (future NIST) asks for an encryption standard
- 1975: IBM developed DES (modification of Lucifer)
  - block size 64 bits; key size 56 bits
- 1975: NSA suggests modifications
- 1977: NBS adopts DES as encryption standard in (FIPS 46-1, 46-2)
- 2001: NIST adopts Rijndael as replacement to DES

DES features

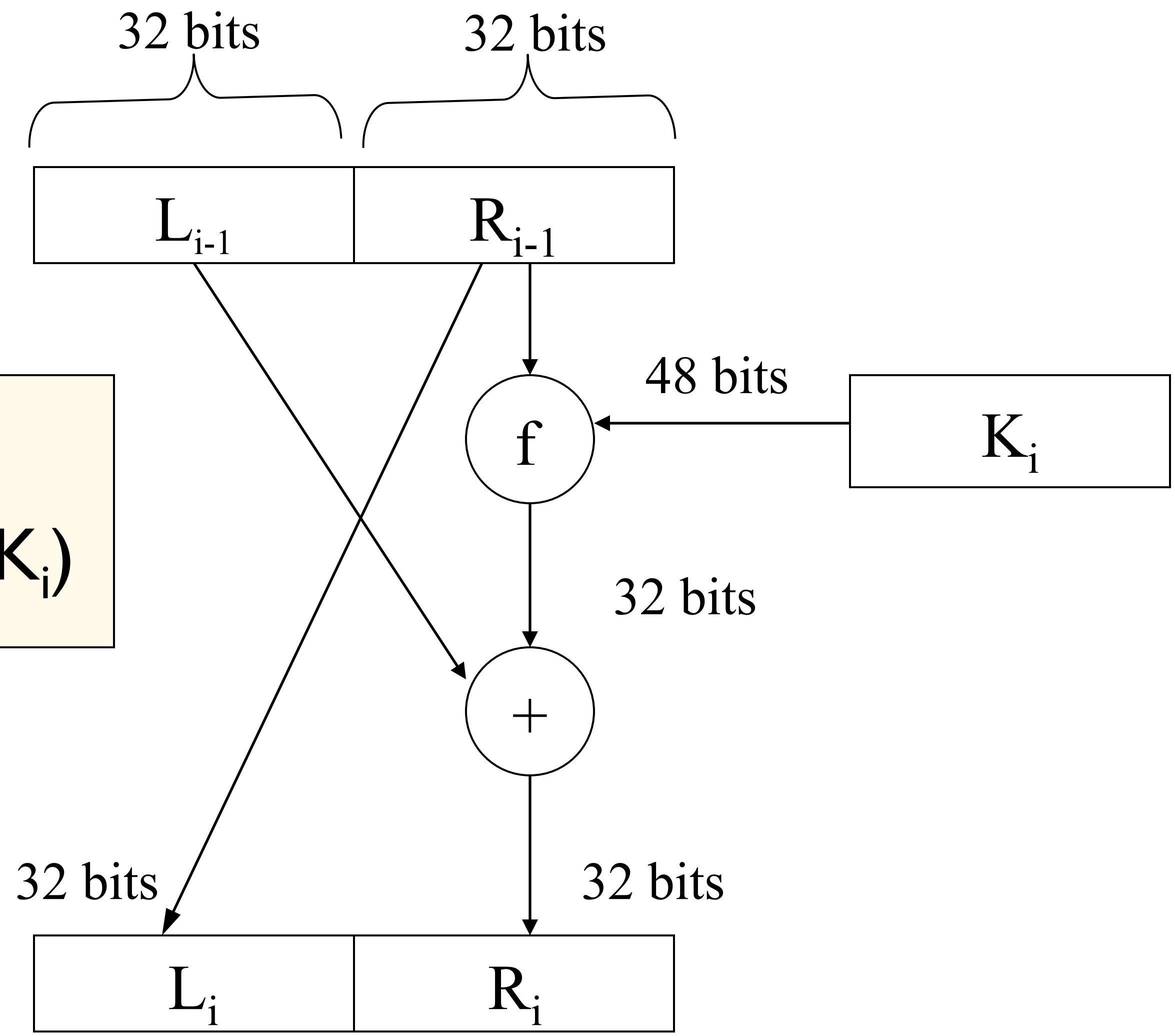
- Block size = 64 bits
- Key size = 56 bits
- Number of rounds = 16
- 16 intermediary keys, each 48 bits

DES rounds



64-bit plaintext
56-bit key
Initial permutation
Permuted choice 1
Round 1
K1
Permuted choice 2
Left circular shift
Round 2
K2
Permuted choice 2
Left circular shift
Round 16
K16
Permuted choice 2
Left circular shift
Inverse initial permutation
64-bit ciphertext

DES round i



$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

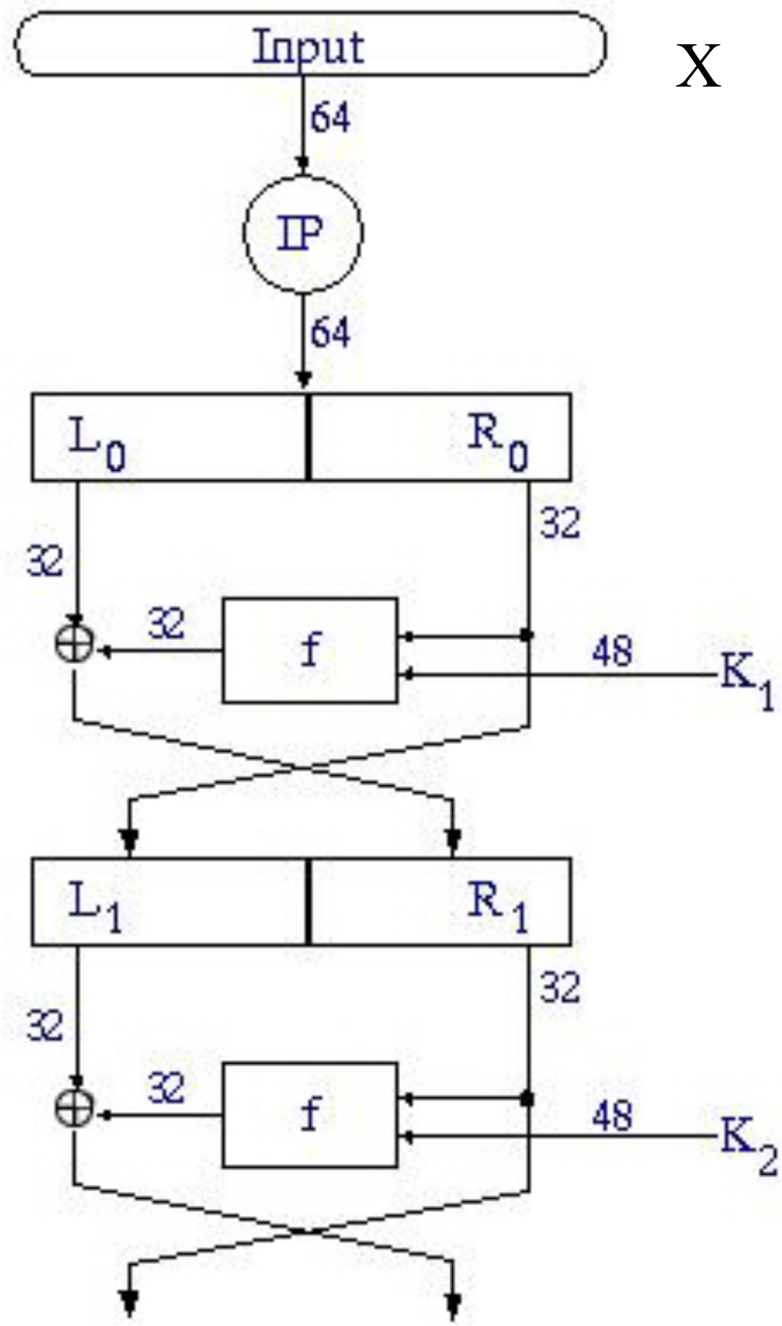
DES details

$IP(x) = L_0R_0$

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

$y = IP^{-1}(R_{16}L_{16})$



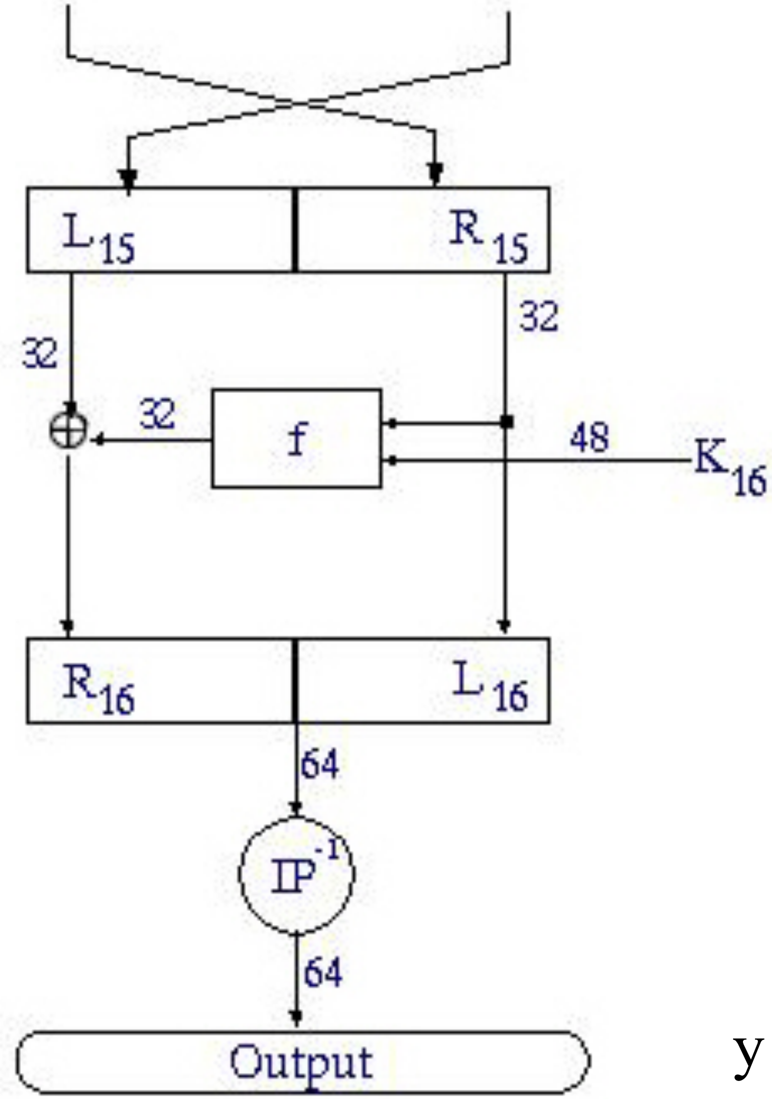
DES details

$IP(x) = L_0R_0$

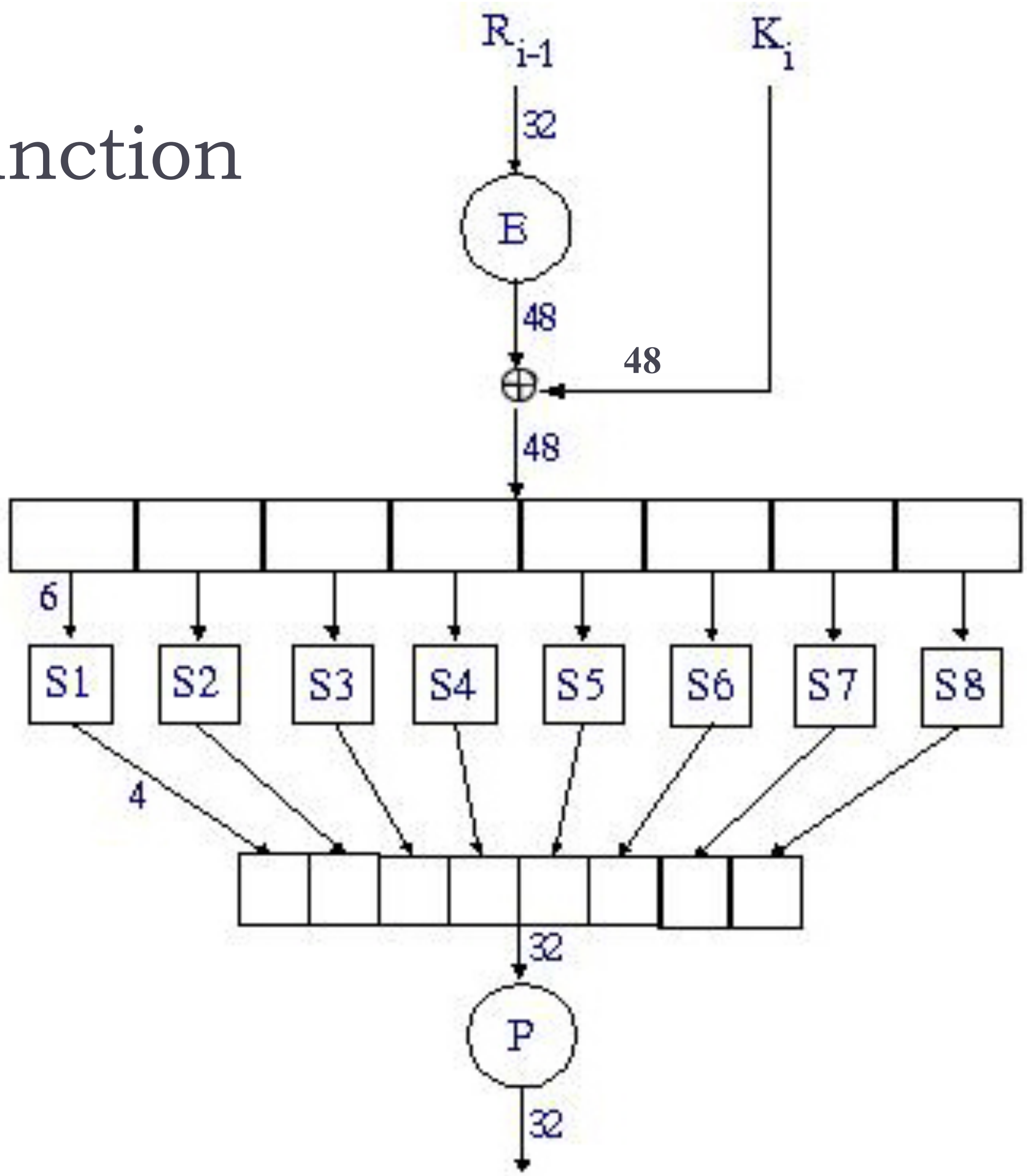
$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

$y = IP^{-1}(R_{16}L_{16})$

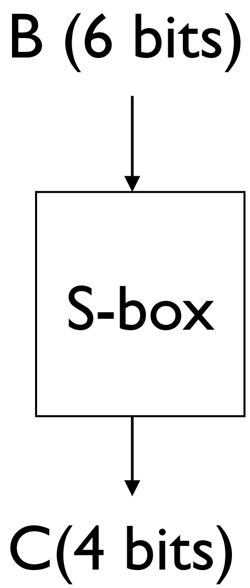


DES f function



S-boxes

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



$$B = b_1b_2b_3b_4b_5b_6$$

b_1b_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

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

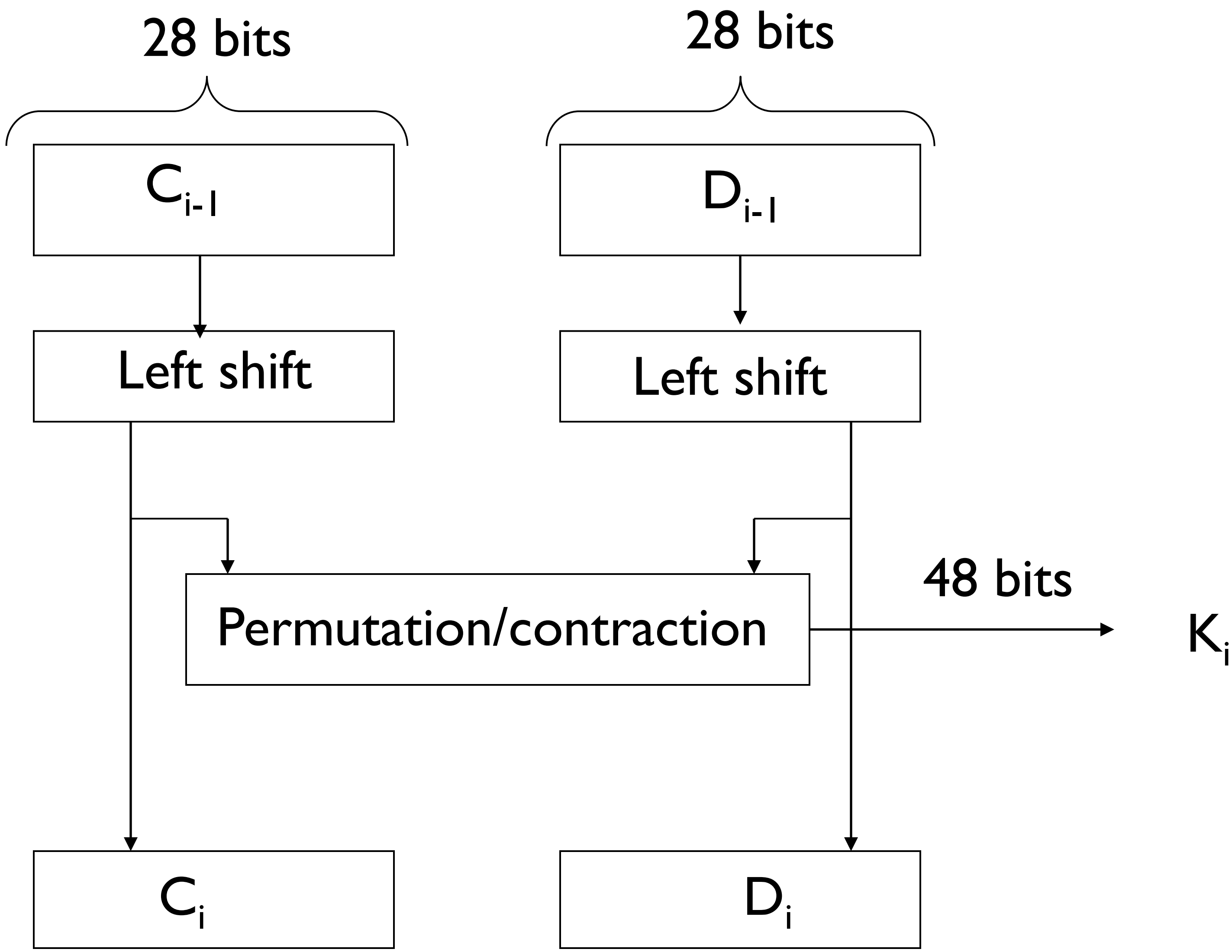
$S(i, j) < 16$, can be represented with 4 bits

B =101111

$b_1 b_6$ = 11 = row 3

$b_2 b_3 b_4 b_5$= 0111 = column 7

DES key generation



DES weak keys

- DES uses 16 48-bits keys generated from a master 56-bit key
- Weak keys: keys make the same sub-key to be generated in more than one round.
- Result: reduce cipher complexity
- Weak keys can be avoided at key generation.
- DES has 4 weak keys

  0000000 0000000

  0000000 FFFFFFF

  FFFFFFF 0000000

  FFFFFFF FFFFFFF

DES decryption

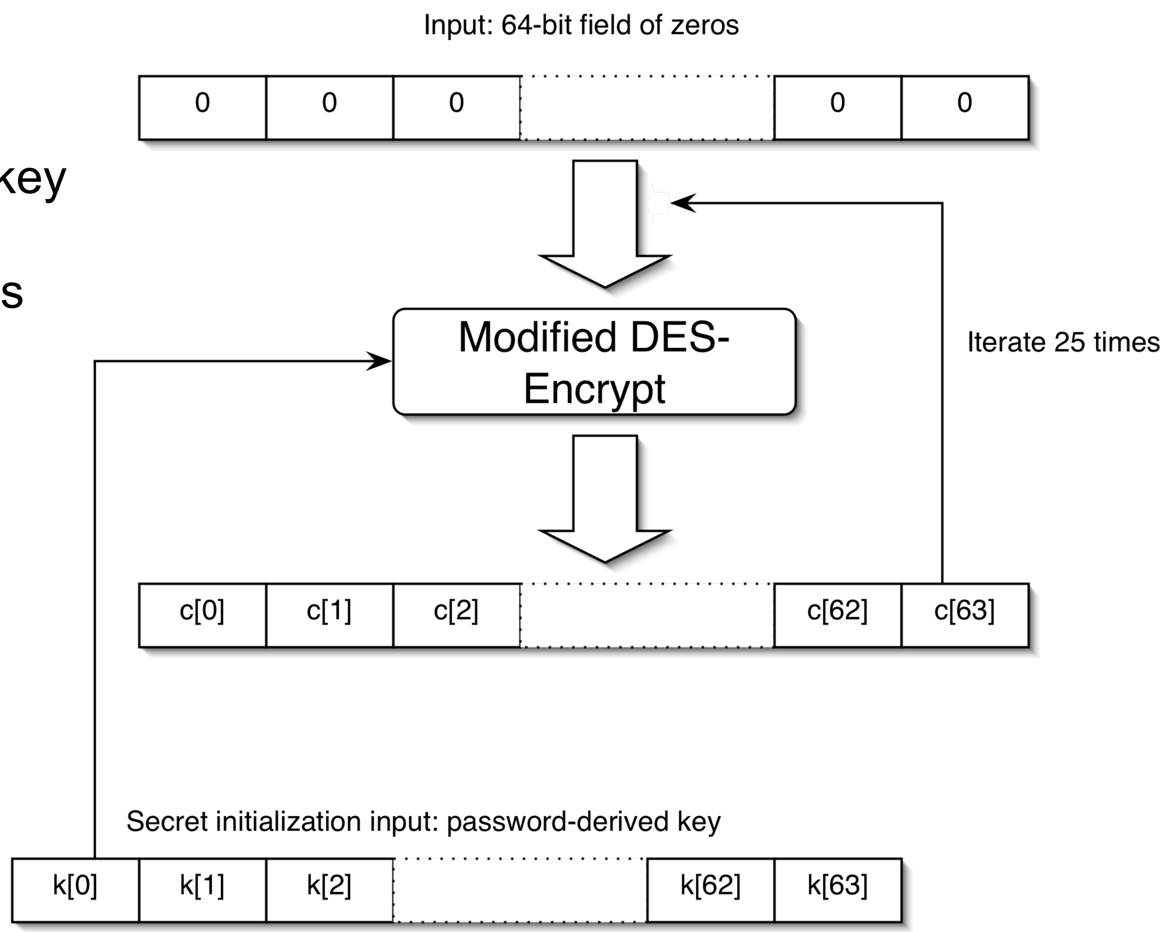
- Decryption uses the same algorithm as encryption, except that the subkeys K1, K2, …K16 are applied in reversed order
- **WHY DOES THE DECRYPTION WORKS ?**

Unix crypt

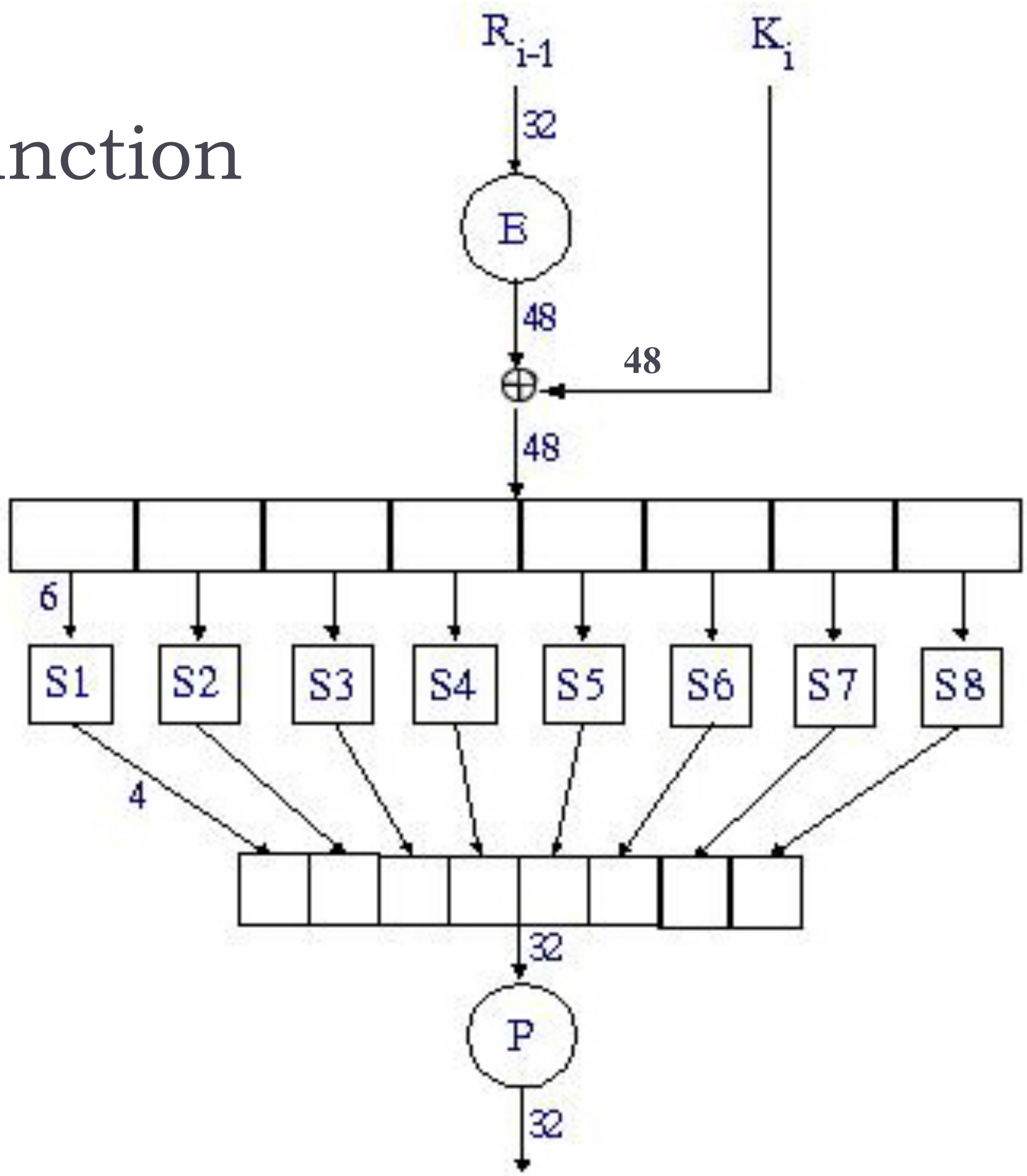
25 rounds

Password used as key

Salt used to address dictionary attacks



DES f function



Modified f function: Use of a salt

- 12-bit Salt is chosen randomly, stored with the password
- Salt creates 4096 different DES: if the ith bit of the salt is set (non-zero), then the bits i and i+24 of the output of the expansion function are swapped.
- Result: same password will have different encryptions in the password file
- Dictionary attack is still possible!

Summary

- DES numbers: 56 bit key, encrypts 64 bit blocks, uses 16 rounds
- Uses a Feistel network with same function f in all rounds
- S-boxes the only non-liniar element of DES
- Variant of DES with a modified f function used by UNIX crypt function