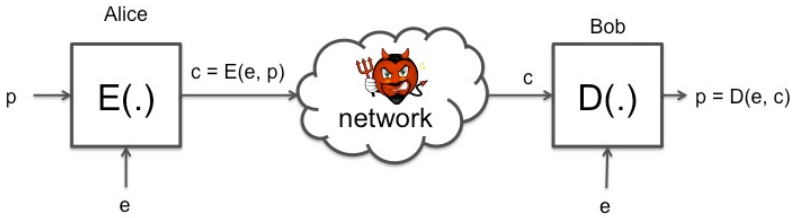
Data Encryption Standard

Symmetric Cryptography

Block cipher

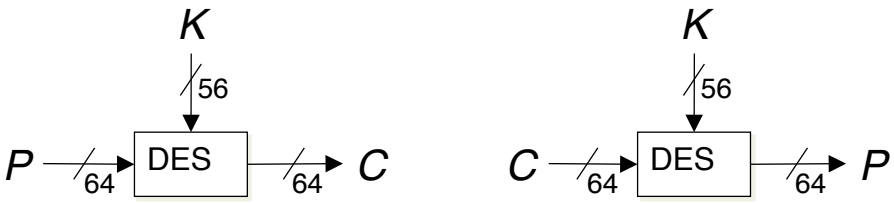
UNIVERSITÀ DI PISA

- Block ciphers break up the plaintext in blocks of fixed length *n* bits and encrypt one block at time



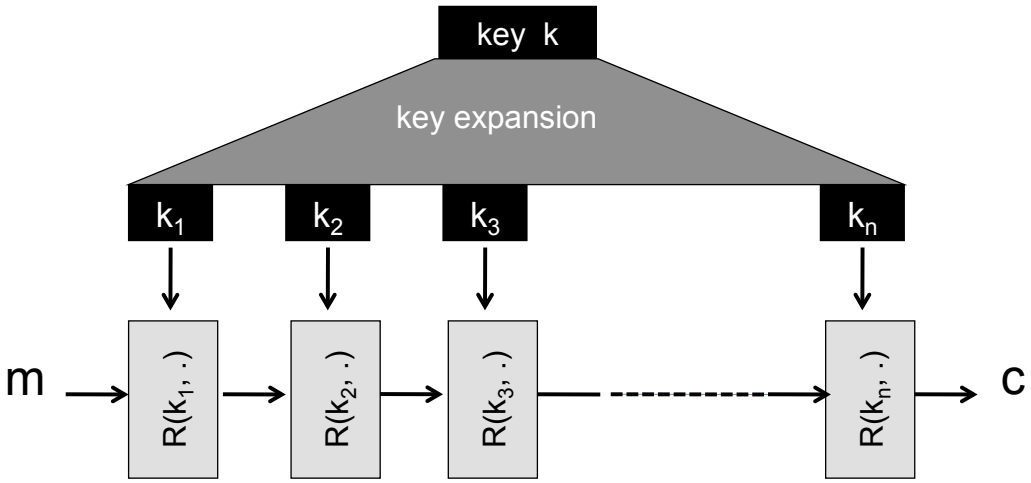
- E: $\{0,1\}^n \rightarrow \{0,1\}^n$ $\quad D$: $\{0,1\}^n \rightarrow \{0,1\}^n$
- E is a permutation (one-to-one, invertible)

Data Encryption Standard (DES)



- The input key *K* is actually specified as a 64-bit key, 8 bits of which (bits 8; 16, …, 64) may be used as parity bits.
- The 2^{56} keys implement (at most) 2^{56} of the 2^{64}! possible permutations on 64-bit blocks.

Block Ciphers Built by Iteration



R(k,m) is called a **round function**

for 3DES (n=48), for AES-128 (n=10)

Data Encryption Standard

UNIVERSITÀ DI PISA

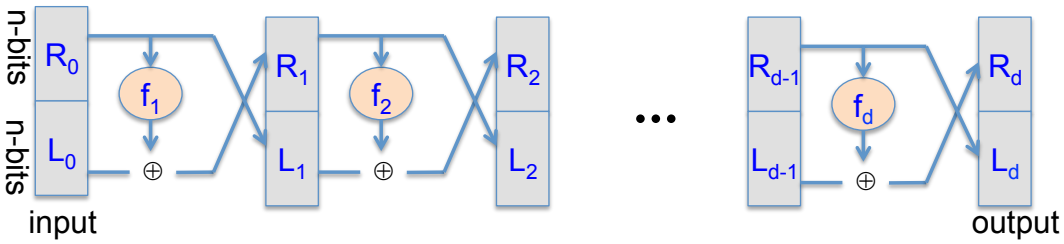
- On May 15, 1973, National Bureau of Standards published a solicitation for cryptosystems in the Federal Register
- DES was published in the Federal Register of March 17, 1975
- DES was developed by IBM as a modification of LUCIFER
- DES was considered a standard for “unclassified” applications on January 15, 1977 after much public discussion
- DES has been reviewed every 5 years
- The most recent review was January 1994
- It is not a standard since 1998.

Basic idea: Feistel Network

UNIVERSITÀ DI PISA

Given functions $f_1, \ldots, f_d$: $\{0,1\}^n \longrightarrow \{0,1\}^n$

Goal: build invertible function $F: \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$



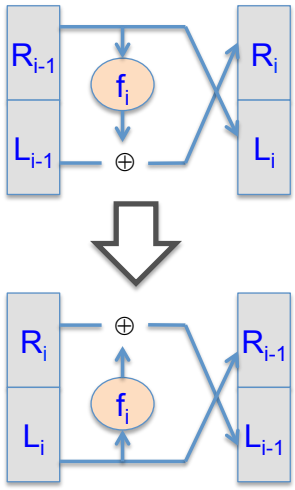
In symbols:
$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f_i\left(R_{i-1}\right) \end{cases}$$

Feistel net is invertible

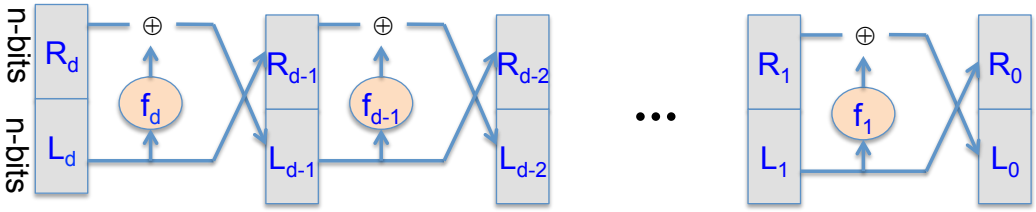
Theorem: for all $f_1, \ldots, f_d$: $\{0,1\}^n \longrightarrow \{0,1\}^n$ Feistel network F: $\{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$ is invertible

Proof: *construct inverse*

In symbols: $\begin{cases} R_{i-1} = L_i \\ L_{i-1} = R_i \oplus f_i(L_i) \end{cases}$



Decryption circuit



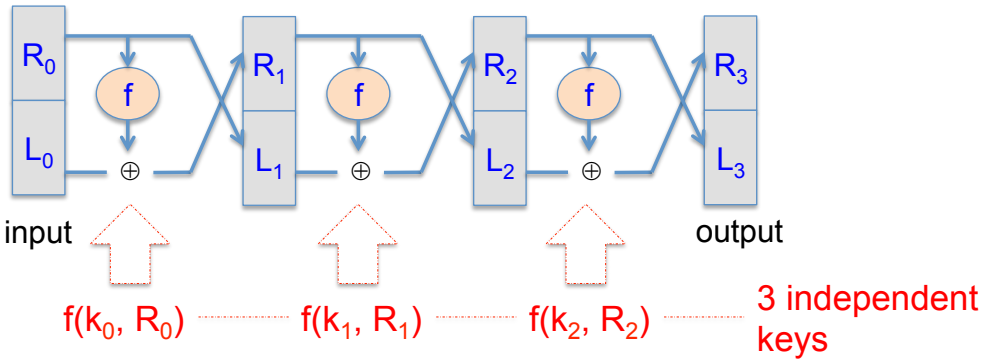
- Inversion is basically the same circuit, with $f_1, \ldots, f_d$ applied in reverse order
- General method for building invertible functions (block ciphers) from arbitrary functions.
- Used in many block ciphers … **but not AES**

Luby-Rackoff '85

UNIVERSITÀ DI PISA

Theorem.

Let f: $K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a secure PRF ⇒
3-round Feistel F: $K^3 \times \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$ is
a secure PRP

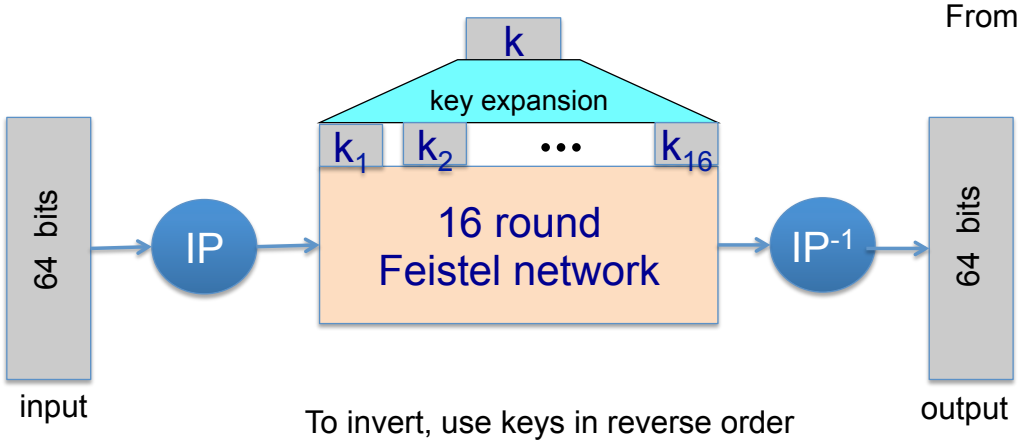


DES: 16 round Feistel net

UNIVERSITÀ DI PISA

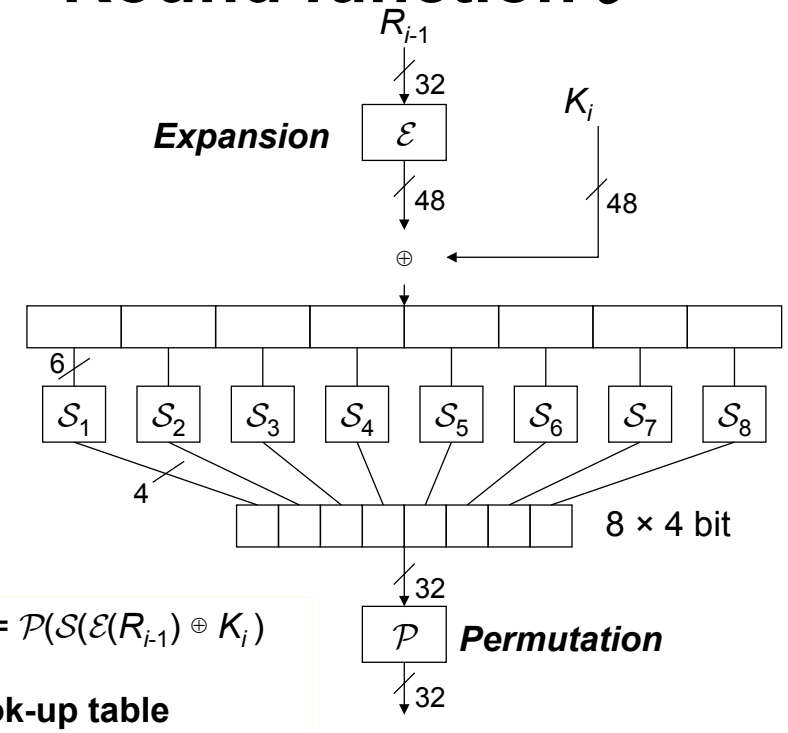
$f_1, \ldots, f_{16}$: $\{0,1\}^{32} \longrightarrow \{0,1\}^{32}$, $f_i(x) = \mathbf{F}(k_i, x)$

From K



To invert, use keys in reverse order

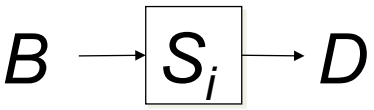
Round function $\mathcal{F}$



$\mathcal{F}(R_{i-1}, K_i) = \mathcal{P}(\mathcal{S}(\mathcal{E}(R_{i-1}) \oplus K_i))$

$S()$ is **a look-up table**

S-boxes



$B = b_1b_2b_3b_4b_5b_6$

$Row \rightarrow b_1b_6$ (outer bits)

Column $\rightarrow b_2b_3b_4b_5$ (inner bits)

row	column number															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1																
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2																
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6																
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

S-boxes

UNIVERSITÀ DI PISA

$S_i: \{0,1\}^6 \longrightarrow \{0,1\}^4$

S_5		Middle 4 bits of input															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

$S_5(011011) \rightarrow 1001$

S-box: a bad choice

UNIVERSITÀ DI PISA

Suppose:

$S_i(x_1, x_2, \ldots, x_6) = (x_2 \oplus x_3,\ x_1 \oplus x_4 \oplus x_5,\ x_1 \oplus x_6,\ x_2 \oplus x_3 \oplus x_6)$

or written equivalently: $S_i(\mathbf{x}) = A_i \cdot \mathbf{x} \pmod 2$

$$\begin{bmatrix} 0&1&1&0&0&0 \\ 1&0&0&1&1&0 \\ 1&0&0&0&0&1 \\ 0&1&1&0&0&1 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_4 \oplus x_5 \\ x_1 \oplus x_6 \\ x_2 \oplus x_3 \oplus x_6 \end{bmatrix}$$

We say that **S_i is a linear function**.

S-box: a bad choice

Then entire DES cipher would be linear: ∃ fixed binary matrix B s.t.

$$\text{DES}(k,m) = \begin{matrix} 64 \\ \\ \end{matrix} \overbrace{\boxed{B}}^{832} \times \begin{bmatrix} m \\ k_1 \\ k_2 \\ \vdots \\ k_{16} \end{bmatrix} = \boxed{c} \pmod 2$$

But then: $\text{DES}(k,m_1) \oplus \text{DES}(k,m_2) \oplus \text{DES}(k,m_3) =$

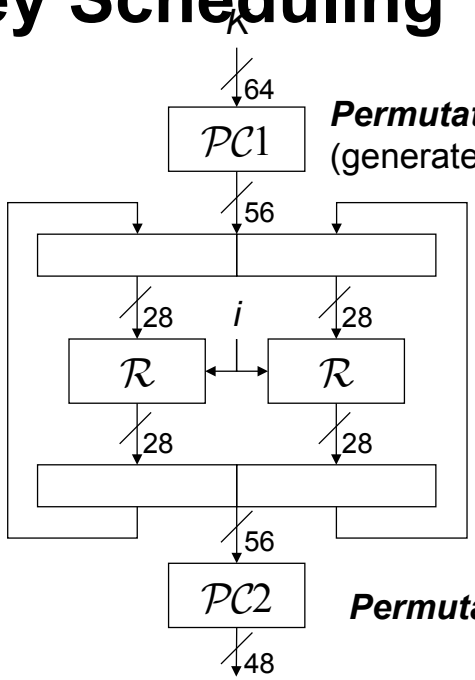
$$B \cdot \begin{pmatrix} m_1 \\ k \end{pmatrix} \oplus B \cdot \begin{pmatrix} m_2 \\ k \end{pmatrix} \oplus B \cdot \begin{pmatrix} m_3 \\ k \end{pmatrix} = B \cdot \begin{pmatrix} m_1 \oplus m_2 \oplus m_3 \\ k \end{pmatrix}$$

Choosing S-box and P-box

- Choosing S-boxes and P-box at random would result in an insecure block cipher
  - (key recovery after ≈2^{24} outputs) [BS'89]
- Several rules used in choice of S and P boxes:
  - ***No output bit should be close to a linear function of the input bits***
  - S-boxes are 4-to-1 maps

Key Scheduling

- $\mathcal{R}$ e $\mathcal{PC}2$ guarantee that, at each round, a different subset of bits is extracted
- Each bit of the key participates to 14 rounds on average



Permutation and compression
(generate the first sub-key)

Left rotation
(1 *bit per round = 1, 2, 9, 16; 2 bit otherwisei*)

Permutation and compression

K_i (i-th subkey)

DES in practice

- DES can be efficiently implemented either in hardware or in software
  - Arithmetic operations are
    - exclusive-or
    - E, S-boxes, IP, IP-1, key scheduling can be done in constant time by **table-lookup (sw)** or by **hard-wiring them into a circuit**
- One very important DES application is in banking transactions
  - DES is used to encrypt PINs and account transactions carried out at ATM
  - DES is also used in government organizations and for inter-bank transactions

Empirical properties of DES

Empirically, DES fulfills these reqs:

- Each CT bits depends on all key bits and PT bits
- There are no evident statistical relationships between CT and PT
- The change of one bit in the PT (CT) causes the change of every bit in the CT (PT) with 0.5 probability

Strength of DES

attack method	data complexity		storage complexity	processing complexity
exhaustive precomputation	–	1	2^{56}	1 (table lookup)
exhaustive search	1	–	negligible	2^{55}
linear cryptanalysis	2^{43} (85%)	–	for texts	2^{43}
	2^{38} (10%)	–	for texts	2^{50}
differential cryptanalys	–	2^{47}	for texts	2^{47}
	2^{55}	–	for texts	2^{55}