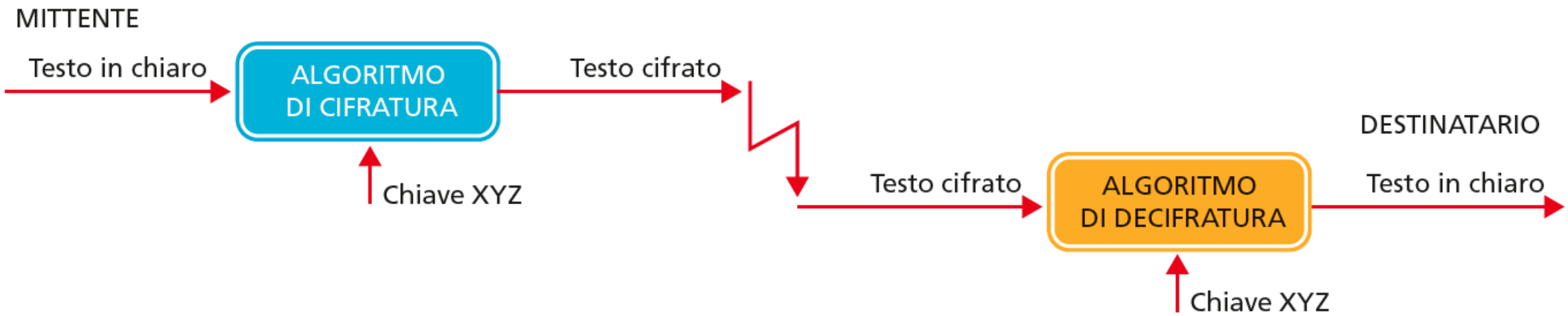
TECNICHE DI CRITTOGRAFIA PER L'INTERNET SECURITY

SISTEMI E RETI
Prof. Verga - Prof.ssa Dalbesio
A.S. 2023/24

CRITTOGRAFIA A CHIAVE SIMMETRICA

Si basa sull'utilizzo di una sola chiave, usata dal mittente per cifrare e dal destinatario per decifrare



CRITTOGRAFIA A CHIAVE SIMMETRICA

Metodo XOR con chiave K = 10100101

M	1	1	0	0	1	0	1	0
K	1	0	1	0	0	1	0	1
C	0	1	1	0	1	1	1	1

XOR

MITTENTE

DESTINATARIO

C	0	1	1	0	1	1	1	1
K	1	0	1	0	0	1	0	1
M	1	1	0	0	1	0	1	0

XOR

L'algoritmo di decifratura è identico a quello di cifratura

CRITTOGRAFIA A CHIAVE ASIMMETRICA

La crittografia a chiave asimmetrica (o pubblica) nasce per risolvere il problema della **distribuzione sicura** delle chiavi.

Essa utilizza due chiavi per ciascun soggetto, una **privata**, nota solo al soggetto, l'altra **pubblica**, distribuita a tutti.

CRITTOGRAFIA A CHIAVE ASIMMETRICA

Se per esempio abbiamo 3 soggetti A,B,C avremo che:

- A possiede: chiave privata di A, chiave pubblica di B e di C;
- B possiede: chiave privata di B, chiave pubblica di A e di C;
- C possiede: chiave privata di C, chiave pubblica di A e di B;

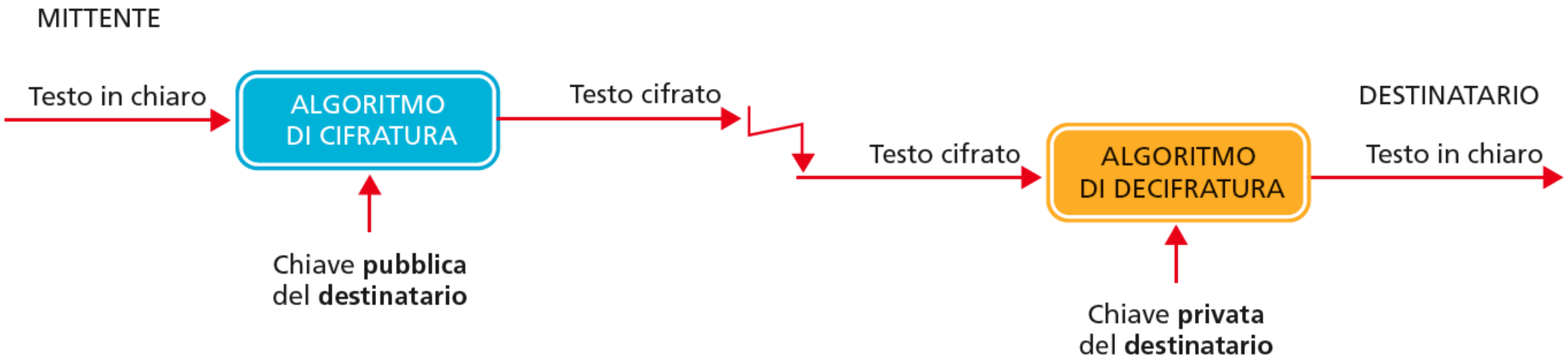
CRITTOGRAFIA A CHIAVE ASIMMETRICA

In generale, il numero di chiavi totale da generare, sarà sempre **2*N**, dove N è il numero di soggetti che voglio comunicare tra loro in sicurezza.

A seconda di come vengono impiegate queste coppie di chiavi, abbiamo 3 possibili utilizzi.

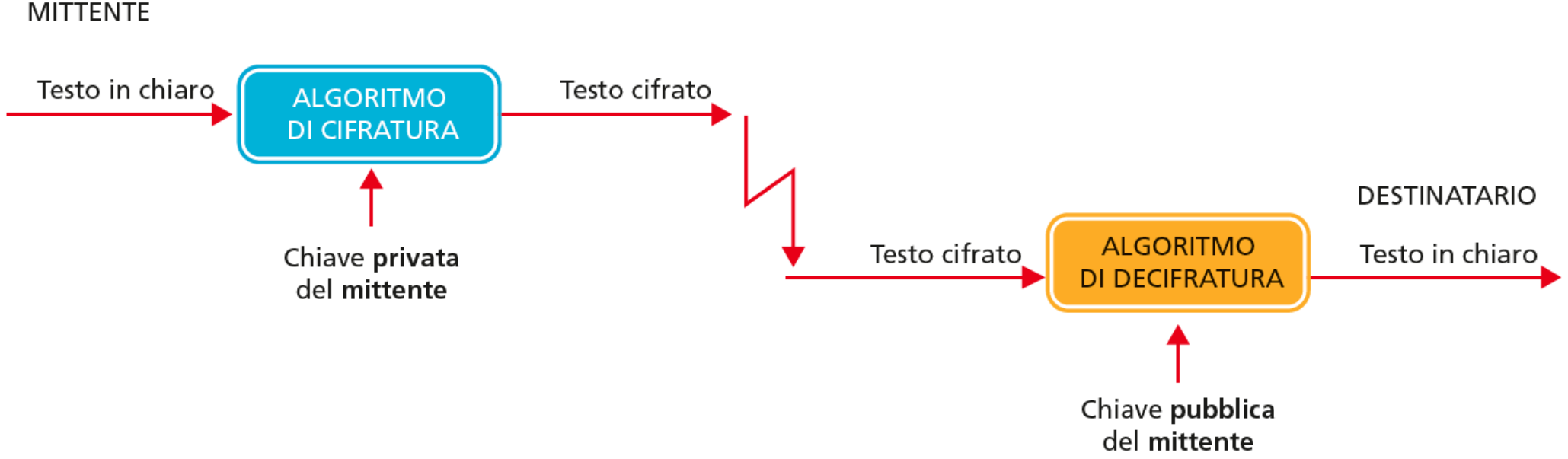
CRITTOGRAFIA A CHIAVE ASIMMETRICA

1. Assicura la riservatezza del dialogo: **confidenzialità**.



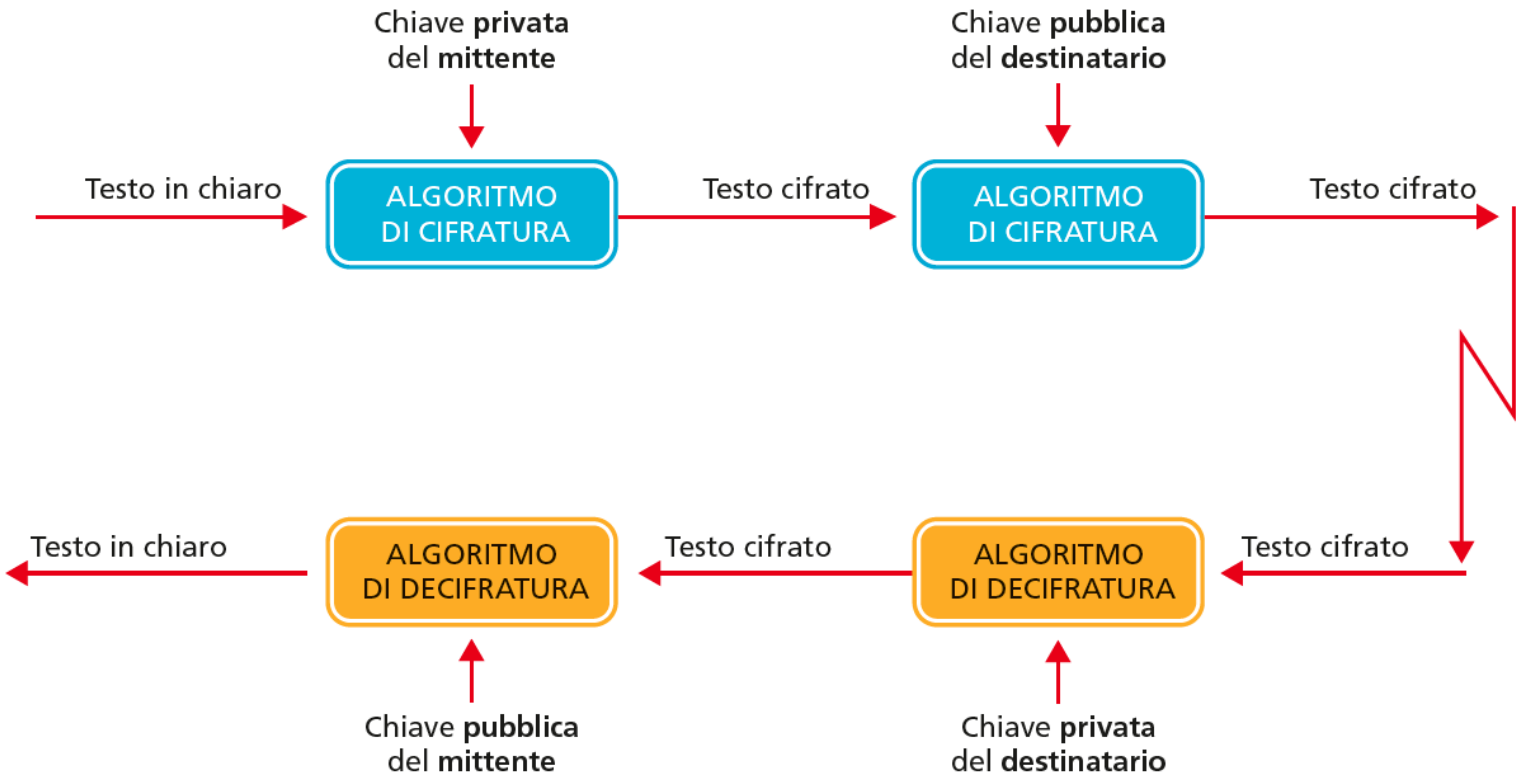
CRITTOGRAFIA A CHIAVE ASIMMETRICA

2. Garantisce l'identità del mittente: **autenticazione**.



CRITTOGRAFIA A CHIAVE ASIMMETRICA

3. Garantisce: **confidenzialità**, **autenticazione** e **integrità**.



CRITTOGRAFIA A CHIAVE ASIMMETRICA

La caratteristica vincente della crittografia a chiave asimmetrica è il fatto di non dover condividere la stessa chiave (quella privata) con nessuno, quindi di non doverla distribuire, con i rischi che questo comporterebbe. Viene distribuita solo la chiave pubblica.

CRITTOGRAFIA A CHIAVE ASIMMETRICA

- Per leggere un testo cifrato inviato da qualcuno occorre soltanto la chiave privata del destinatario (caso 1: confidenzialità).
- Per scrivere e inviare a qualcuno un testo cifrato occorre soltanto la chiave privata del mittente (caso 2: autenticazione).
- In ogni caso, serve solo la chiave privata, che è quella che non viene distribuita.
- Occorre che le 2 chiavi (privata e pubblica) siano matematicamente correlate.

ALGORITMI A CHIAVE SIMMETRICA: DES

Il capostipite dei moderni algoritmi di crittografia a chiave simmetrica è il **DES (Data Encryption Standard)**, creato nel 1976 per il governo degli Stati Uniti.

Il problema principale della crittografia a chiave simmetrica è la segretezza della chiave legata alla sua distribuzione. Occorre quindi che anche l'algoritmo (e non solo la chiave) si faccia carico dell'onere di garantire la sicurezza e per far questo dovrà per forza essere abbastanza complesso.

ALGORITMI A CHIAVE SIMMETRICA: DES

Claude Shannon, ingegnere e matematico statunitense, negli anni quaranta del secolo scorso, mostrò che per ottenere cifrari *pratici* ma resistenti all'analisi statistica dell'attaccante, l'algoritmo di cifratura deve avere almeno due caratteristiche: **Confusion** e **Diffusion**.

ALGORITMI A CHIAVE SIMMETRICA: DES

Confusion: rendere confusa la relazione tra il testo in chiaro e quello cifrato, tipicamente tramite la sostituzione dei caratteri in chiaro con caratteri diversi.

Diffusion: alterare la struttura del testo in chiaro spargendo i caratteri su tutto il testo cifrato, tipicamente permutando (trasponendo) i caratteri del testo in chiaro.

ALGORITMI A CHIAVE SIMMETRICA: DES

Ognuna di queste due tecniche, confusione e diffusione, se usate anche congiuntamente una sola volta, non garantiscono la sicurezza. Quindi, l'idea di base è quella di ripetere molte volte una serie di operazioni di confusione e diffusione (tramite sostituzioni e permutazioni) ovvero di utilizzare quelle che Shannon chiamava **SPN** (**Substitution Permutation Network**).

ALGORITMI A CHIAVE SIMMETRICA: DES

Nel **DES** confusione e diffusione sono soddisfatte attraverso una serie (round) di permutazioni del messaggio e combinazioni del messaggio con la chiave.

Le sue caratteristiche principali sono:

- Il **testo in chiaro** da cifrare viene suddiviso in **blocchi** di dimensione fissa pari a **64 bit**;
- **Chiave a 64 bit**, dei quali 8 non vengono utilizzati, quindi 2^{56} possibili chiavi diverse (più di 7,2 miliardi).

ALGORITMI A CHIAVE SIMMETRICA: DES

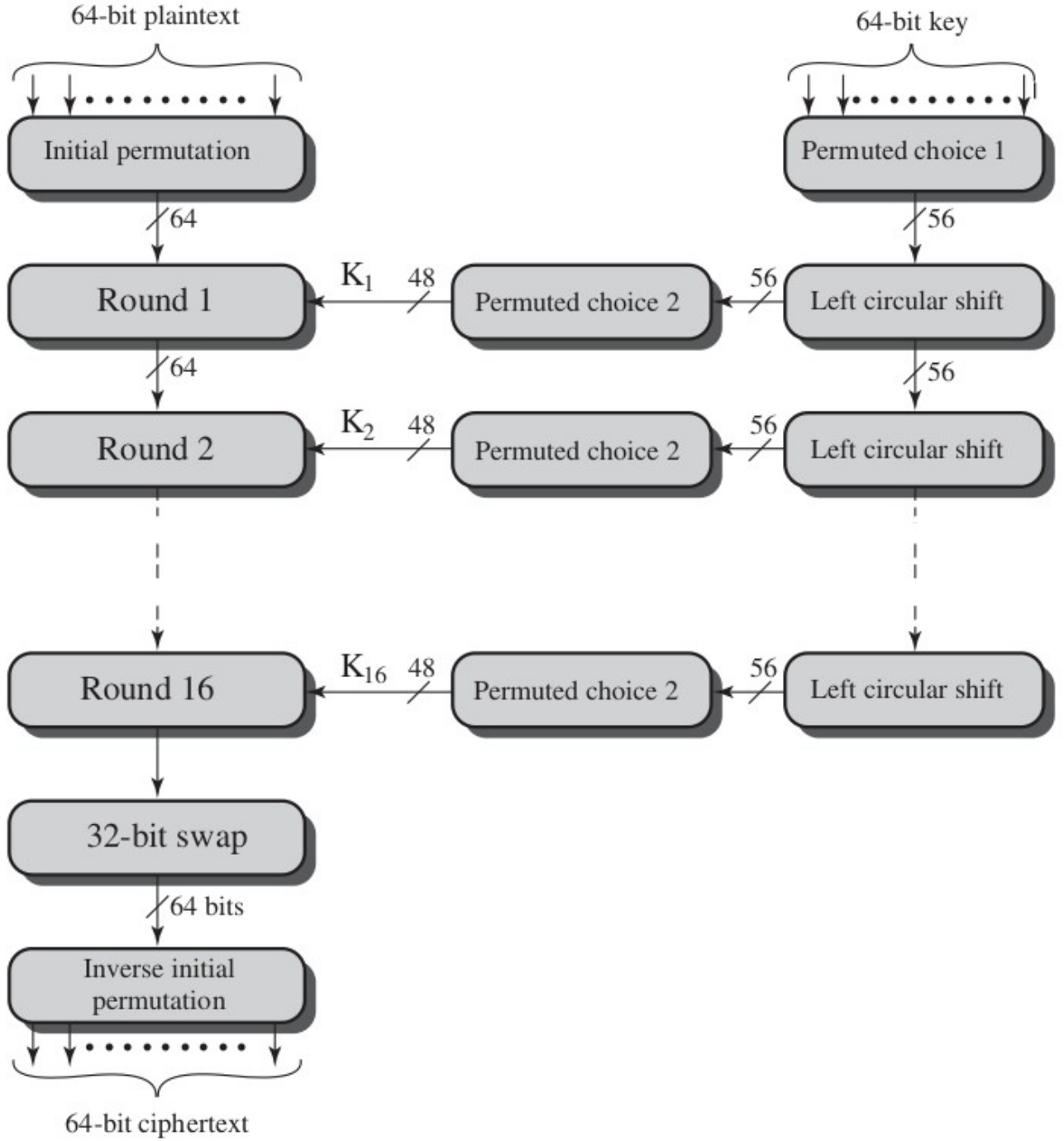
L'algoritmo consiste nelle seguenti fasi:

1. Il plaintext di 64 bit passa attraverso una permutazione iniziale che ricombina i bit;
2. Segue una fase di 16 round che coinvolge operazioni di sostituzioni e permutazioni.
3. Scambio di posizione tra le due metà (destra e sinistra) dell'output dell'ultimo round
4. Permutazione finale (inversa della permutazione iniziale)

NOTA: La chiave di 56 bit subisce un processo di trasformazione in modo da creare 16 sottochiavi da 48 bit tutte diverse fra loro, una per ogni round.

DES: Passi dell'algoritmo

16 Round



DES: Permutazione iniziale e finale

Le operazioni di permutazione iniziale e finale riordinano i dati utilizzando due matrici (8x8) di permutazione casuale. Se per esempio il primo numero della matrice è 58, allora il 58° bit diventa il 1° bit del testo permutato; il 50° diventa il 2° e così via.

(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

DES: Dettagli di un singolo round

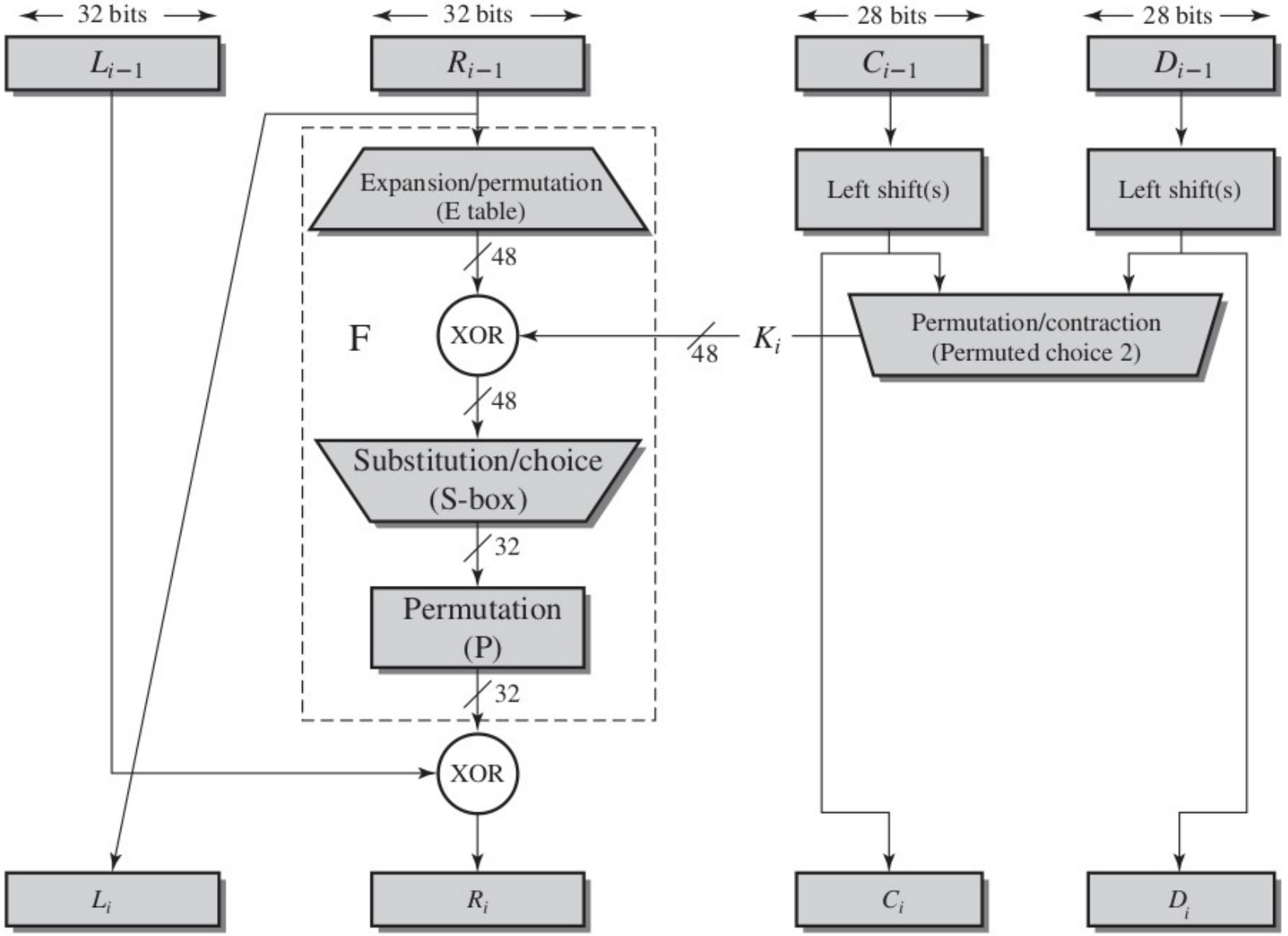
- L'input viene suddiviso in 2 parti: sinistra (L) e destra (R)
- Il round i-esimo genera:

$$L_i = R_{i-1}$$

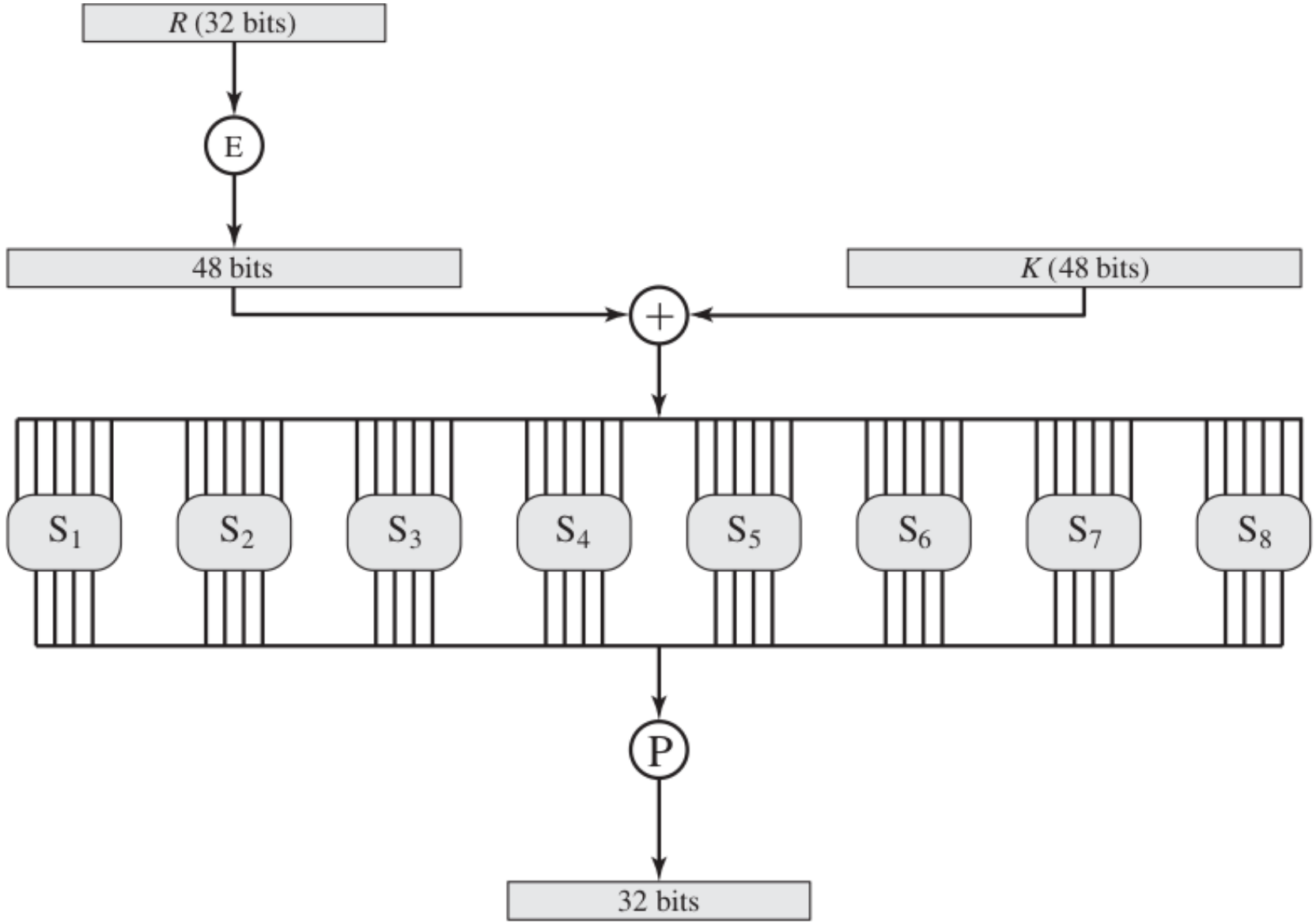
$$R_i = L_{i-1} \oplus F\left(R_{i-1}, K_i\right)$$

- La funzione F:
  - Espande R a 48 bit mediante una permutazione/espansione;
  - Effettua lo XOR del risultato con la sottochiave;
  - Invia il tutto a 8 S-BOX per ottenere un output di 32 bit;
  - Infine esegue una permutazione finale dei 32 bit.

DES: Dettagli di un singolo round



DES: Dettagli di un singolo round



DES: Dettagli di un singolo round

(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

DES: Le S-BOX

Vi sono 8 S-Box che sono funzioni che accettano in ingresso 6 bit e ne producono 4.

- Ogni S-Box è una matrice 4x16 contenente interi tra 0 e 15;
- I bit 1 e 6 selezionano la riga;
- I bit 2-5 selezionano la colonna;
- Il risultato è l'espansione binaria dell'elemento selezionato della matrice;
- L'output delle S-Box dipende sia dai dati che dalla chiave.

DES: Le S-BOX

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

DES: Le S-BOX

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

DES: Esempio di funzionamento di una S-Box

primo e ultimo bit

input 101110

10

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	0110	0111	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	7	8	13	6	2	**11**	15	12	9	7	3	10	5	0
11	15	12	10	2	4	9	1	7	5	11	3	14	10	0	6	13

Box S1

output 11 in binario = 1011

DES: Generazione delle sottochiavi

- Alla chiave iniziale di 64 bit, vengono eliminati un bit ogni otto bit consecutivi (per un totale di 8 bit);
- I 56 bit rimanenti, vengono inizialmente permutati (PC-1) e poi suddivisi in due metà (C e D) da 28 bit ciascuna;
- Ad ogni round, C e D subiscono uno shift a sinistra in modo circolare di una o due posizioni (a seconda del numero del round);
- Tali valori, oltre a rappresentare gli input per il round successivo, vengono sottoposti ad un'operazione di permutazione/contrazione (PC-2) in modo da generare la chiave a 48 bit.

DES: Generazione delle sottochiavi

(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

(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

DES: Generazione delle sottochiavi

(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

DES: Decifratura

Per decifrare un testo cifrato con DES si utilizza lo stesso algoritmo di cifratura, avendo cura di generare le sottochiavi K_i in ordine inverso.

DES: Considerazioni

Effetto valanga: un cambiamento di pochi bit nel plaintext deve provocare un cambiamento di quanti più bit nel ciphertext.

DES possiede un forte effetto valanga.

Nonostante la lunghezza della chiave a 56 bit, il DES fu violato nel 1998 in soli 3 giorni. Nel 1999 tale tempo fu ridotto a 22 ore.

Altra preoccupazione riguarda la criptoanalisi. Al centro dell'attenzione stanno ovviamente eventuali debolezze nascoste nelle 8 S-Box.

3-DES

3 applicazioni consecutive di DES con tre chiavi diverse e maggior sicurezza per via della chiave più lunga.

In base alla scelta delle chiavi il sistema 3DES offre 3 alternative:

- Le 3 chiavi sono diverse ed indipendenti (sicurezza a 168 bit);
- K1 = K3 e K2 diversa (sicurezza a 128 bit);
- K1=K2=K3 (sicurezza a 56 bit, usato per garantire la compatibilità con DES).