IL DES

a cura di:

Gabriel Sassone && Stefano Tortora

Tabella del codice ASCII utilizzata dal DES per convertire il messaggio in chiaro binari

Il codice ASCII ridotto (SP=spazio; RC=ritorno carrello; NR=nuova riga)

A	01000001	a	01100001	0	00110000
B	01000010	b	01100010	1	00110001
C	01000011	c	01100011	2	00110010
D	01000100	d	01100100	3	00110011
E	01000101	e	01100101	4	00110100
F	01000111	f	01100110	5	00110101
G	01001000	g	01100111	6	00110110
H	01001001	h	01101000	7	00110111
I	01001001	i	01101001	8	00111000
J	01001010	j	01101010	9	00111001
K	01001011	k	01101011	.	00101110
L	01001100	l	01101100	,	00101100
M	01001101	m	01101101	:	00111010
N	01001110	n	01101110	;	00111011
O	01001111	o	01101111	!	00100001
P	01010000	p	01110000	?	00111111
Q	01010001	q	01110001	+	00101011
R	01010010	r	01110010	-	00101101
S	01010011	s	01110011	=	00111101
T	01010100	t	01110100	(	00101000
U	01010101	u	01110101	)	00101001
V	01010110	v	01110110	«	00100010
W	01010111	w	01110111	/	00101111
X	01011000	x	01111000	SP	00100000
Y	01011001	y	01111001	RC	00001101
Z	01011010	z	01111010	NR	00001010

Tab.1

Passi effettuati a partire dal testo in chiaro C per ottenere il testo cifrato C'

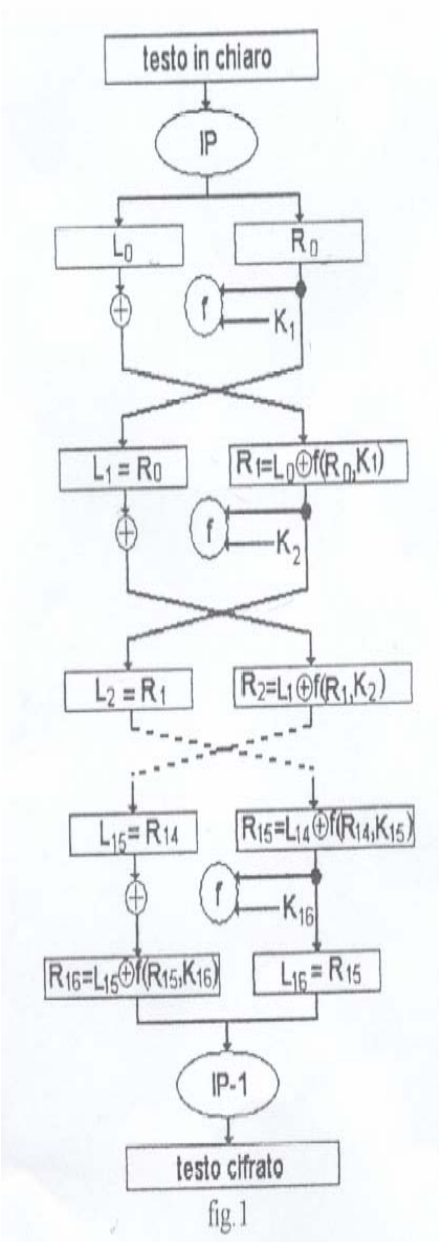

fig.1

1. Permutazione iniziale IP
2. Suddivisione del testo in L_0 e R_0
3. Ad R_0 viene applicata la funzione f
4. XOR tra L_0 e R_0
5. R_0 ⇨ L_1 e R_1 ⇨ risultato del passo 4
6. I passi 3 e 5 vengono ripetuti 16 volte
7. R_{16} e L_{16} vengono giustapposti tra loro
8. Permutazione finale IP^{-1}

Schema delle operazioni effettuate dal DES per criptare un messaggio

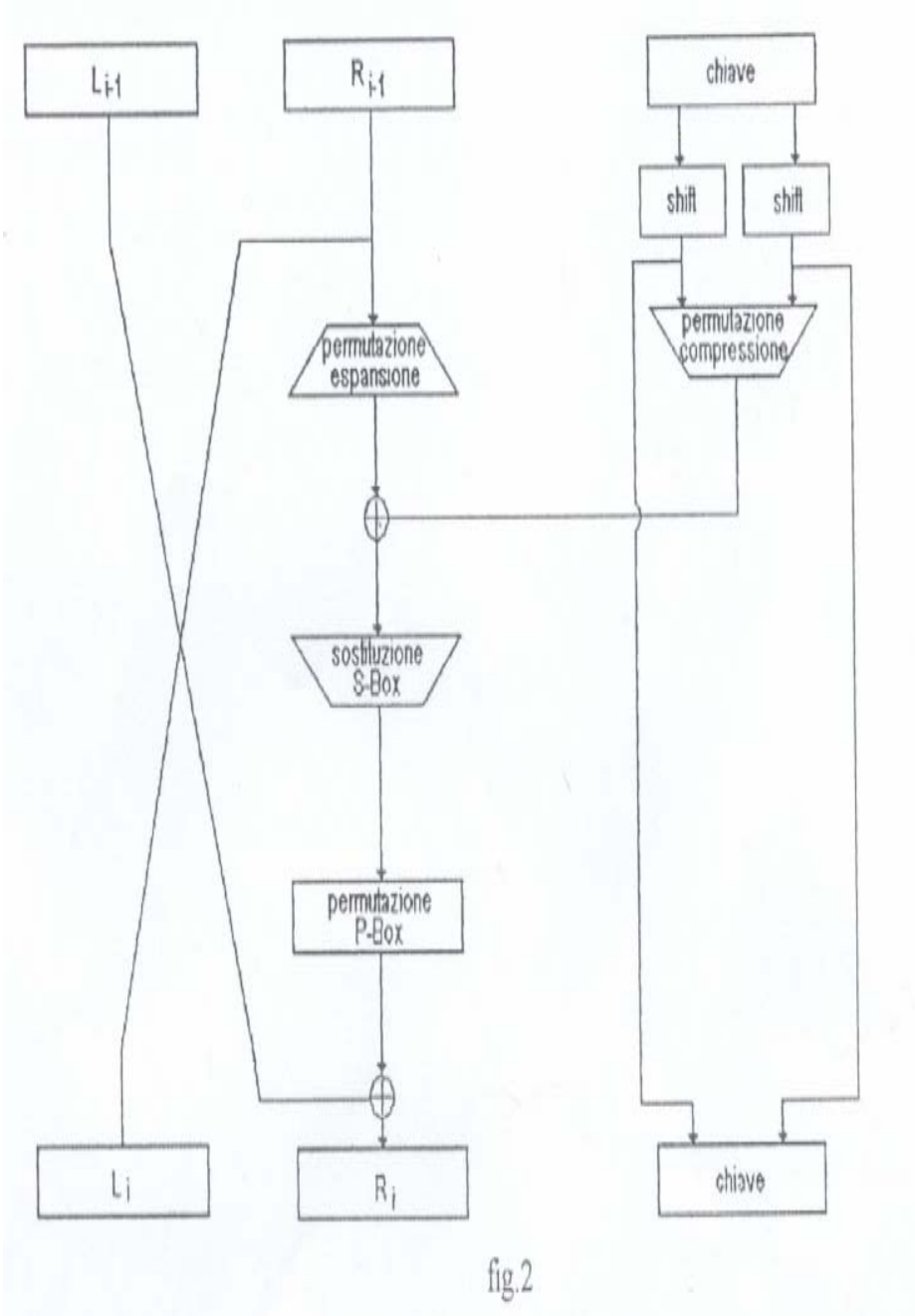

fig.2

Dettaglio di tutte le Operazioni DEL DES

La Permutazione iniziale

Permutazione iniziale

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

Tab.2

La Trasformazione della chiave

Permutazione della chiave

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

Tab.3

Numero di bit della chiave shiftati per ogni round

round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
#posizioni	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Tab.4

Permutazione con compressione

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

Tab.5

La Permutazione con Espanzione

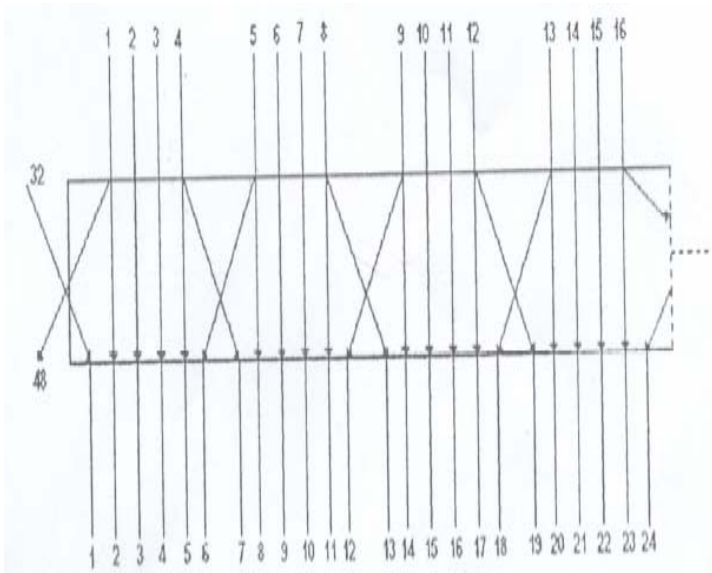

fig.3

Permutazione con espansione

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

Tab.6

La Sostituzione S-Box

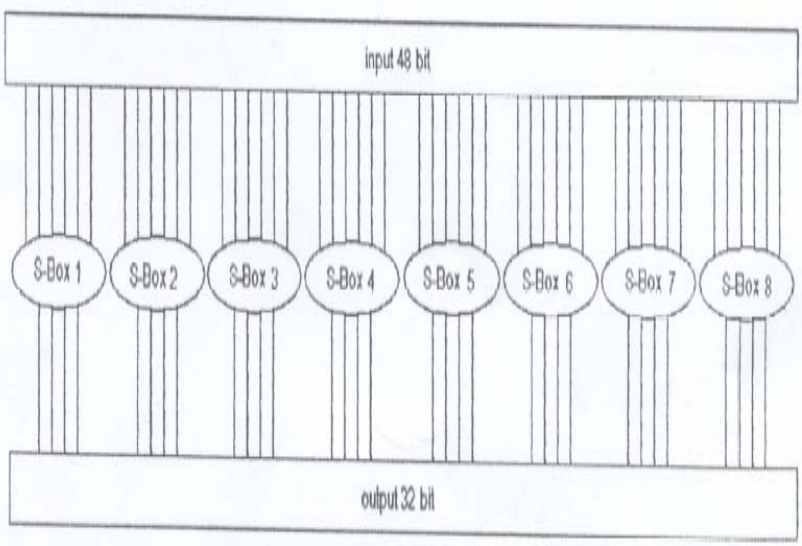

fig.4

Tavole delle S-Box

S-Box1	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-Box2	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-Box3	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-Box4	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-Box5	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-Box6	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-Box7	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-Box8	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

Tab.7

La permutazione P-Box

Permutazione P-Box

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

Tab.8

La permutazione finale

Permutazione finale 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

Tab.9

Decriptare Il DES

Per Decriptare il DES viene usato esattamente lo stesso algoritmo appena descritto; deve essere però utilizzata la sequenza inversa di sottochiavi: ossia se era stata utilizzata per criptare il messaggio la chiave K con sottosequenze K^1,K^2 .. K^{16} verrà utilizzata per decripare il messaggio la chiave K’ con le sottosequenze K^{16}, K^{15}..K^1.

La tabella degli shift deve essere vista da destra e gli shift vanno fatti verso sinistra.

Le Chiavi deboli

Le Chiavi deboli sono quelle costituite da soli 1 o da soli 0 o quelle che nell'atto della suddivisione una delle due parti è costituita da soli 1 o da soli 0. Nella Creazione delle 16 sottochiavi viene generata sempre la stessa sottochiave .

Chiavi deboli (con bit di parità)

0101	0101	0101	0101
1F1F	1F1F	0E0E	0E0E
E0E0	E0E0	F1F1	F1F1
FEFE	FEFE	FEFE	FEFE

Tab.10

Le Chiavi semideboli sono quelle coppie di chiavi (k^1,K^2) per le quali vale la seguente regola: un testo criptato con K^1 può essre decriptato con K^2 e viceversa. Nella Creazione delle 16 sottochiavi vengono generate solo due sottochiavi ed utilizzate ciascuna otto volte.

Chiavi semideboli

01FE	01FE	01FE	01FE	e	FE01	FE01	FE01	FE01
1FE0	1FE0	0EF1	0EF1	e	E01F	E01F	F01E	F10E
01E0	01E0	01F1	01F1	e	E001	E001	F101	F101
1FFE	1FFE	0EFE	0EFE	e	FE1F	FE1F	FE0E	FE0E
011F	011F	010E	010E	e	1F01	1F01	0E01	0E01
E0FE	E0FE	F1FE	F1FE	e	FEE0	FEE0	FEF1	FEF1

Tab.11

Le possibili chiavi sono quelle chiavi che nella creazione delle 16 sottochiavi vengono generate solo due sottochiavi ed utilizzate ciascuna otto volte.