

### Data Encryption Standard (DES)

- 15 maggio 1973, richiesta pubblica per uno standard della NBS, oggi NIST (27 agosto 1974, seconda richiesta)
- Modifica di *Lucifer*, sviluppato da IBM (chiave da 128 a 56 bit) reso noto nel 1975
- 1976: due workshop
- Standard pubblicato 15 gennaio 1977
- Riaffermato per successivi 5 anni nel 1983, 1987, 1992
- DES challenges (giugno 1997, luglio 1998, gennaio 1999)
- Advanced Encryption Standard (AES)

DES 0

### Data Encryption Standard

DES 1

### Lunghezza della Chiave

Nello standard DES la chiave è lunga 64 bit  
8 byte di cui l'ottavo bit è di parità

bit di parità  
è lo xor dei precedenti 7 bit

DES 2

### Struttura del DES

DES 3

### Permutazione Iniziale IP

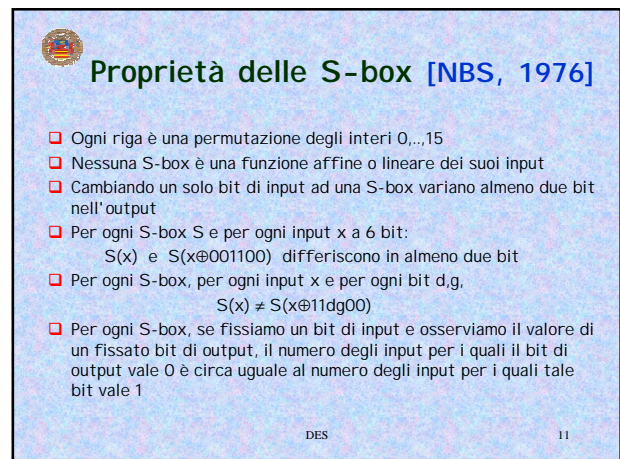
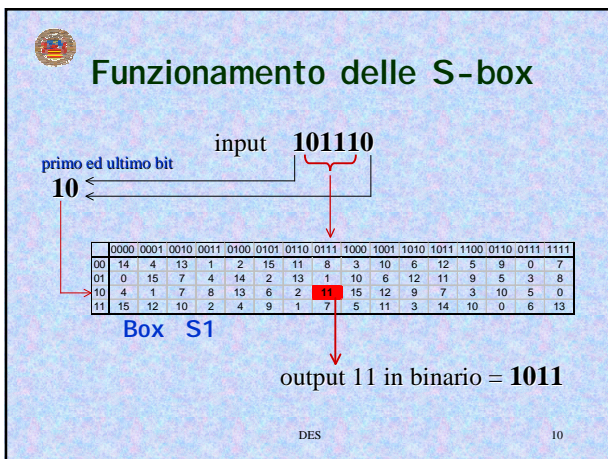
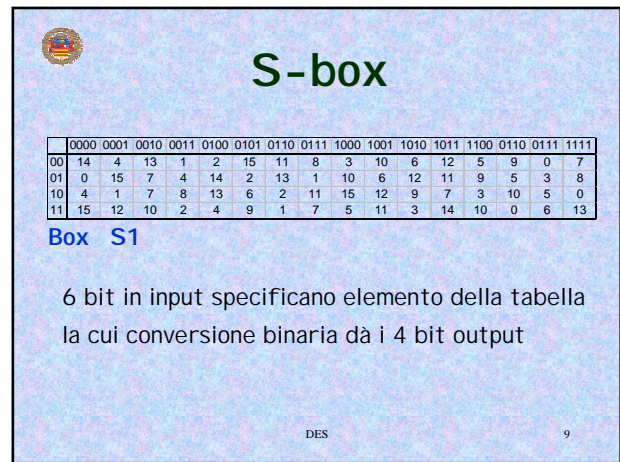
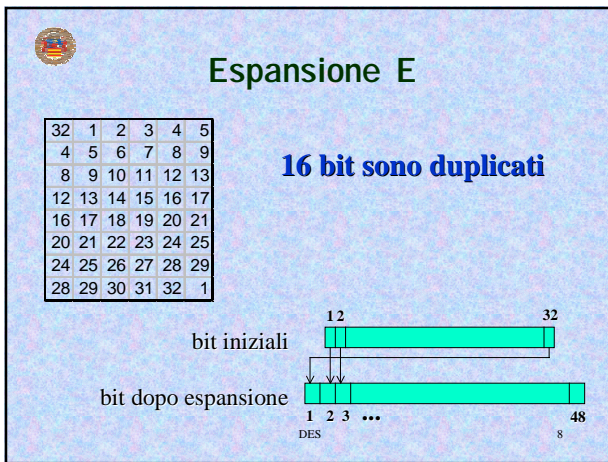
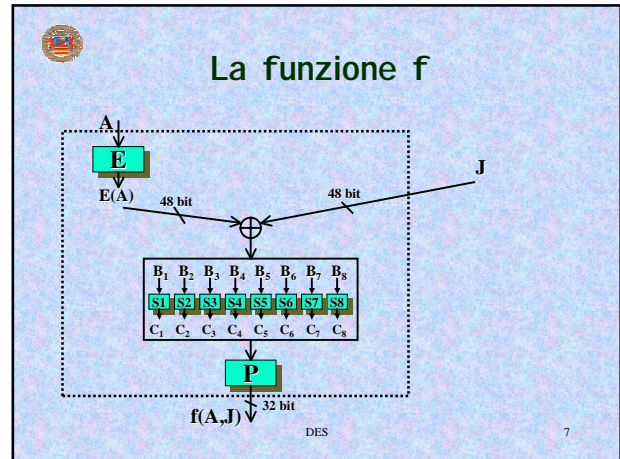
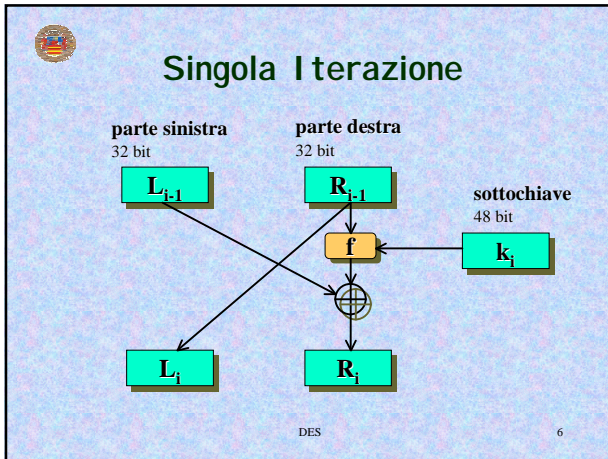
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

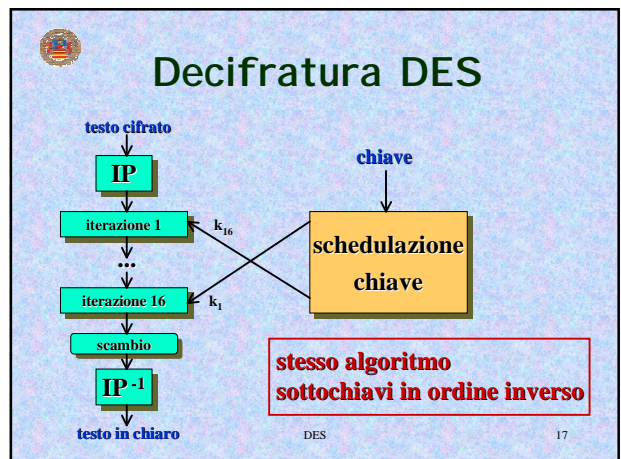
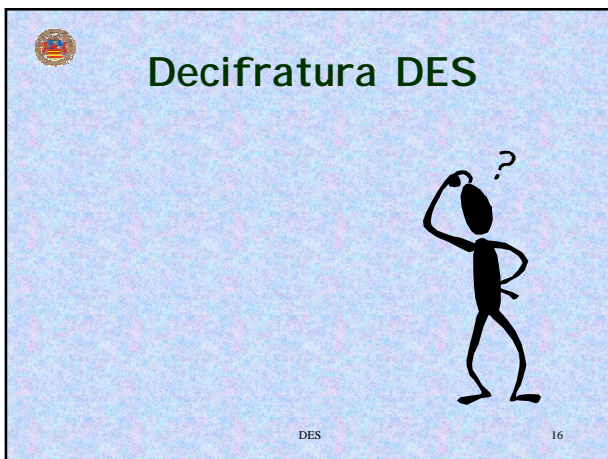
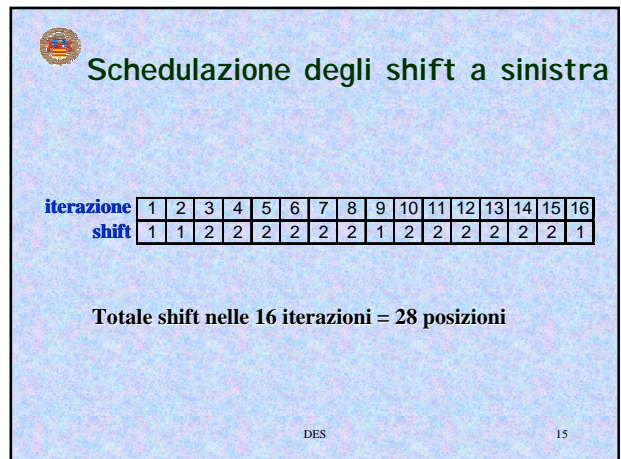
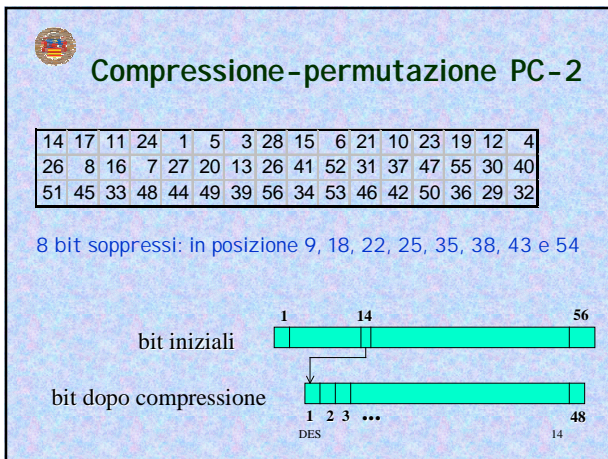
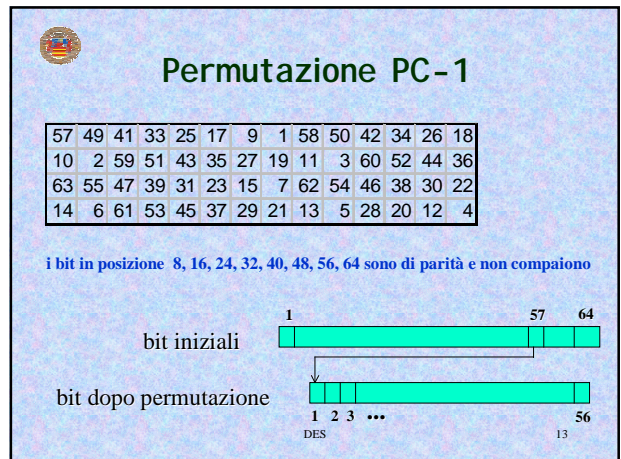
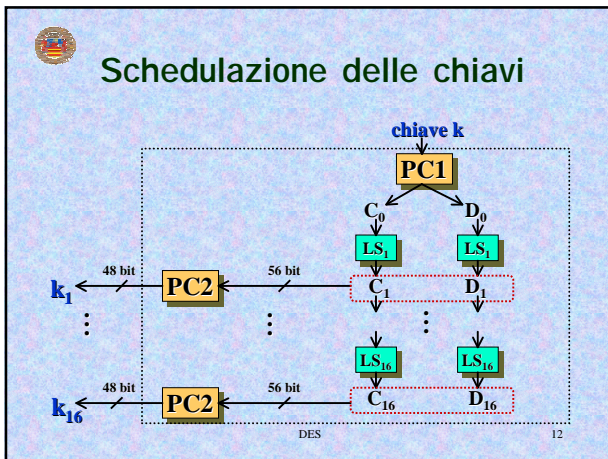
DES 4

### Permutazione Inversa 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 5





### Prestazioni

Hardware: chip della Digital, 1 Gbit/secondo

Frequenza	Dimensione del chip (mm <sup>2</sup> )	Potenza (mW)	Numero di porte I/O
1000	4.7	8	270
2000	7.5	15	500
3000	9.0	25	1.000
4000	16.0	32	1.500
5000	22.0	32	2.000
6000	22.0	16	2.000
7000	22.0	32	2.000
8000	22.0	32	2.000
9000	22.0	32	2.000
10000	22.0	32	2.000
11000	22.0	32	2.000
12000	22.0	32	2.000
13000	22.0	32	2.000
14000	22.0	32	2.000
15000	22.0	32	2.000
16000	22.0	32	2.000
17000	22.0	32	2.000
18000	22.0	32	2.000
19000	22.0	32	2.000
20000	22.0	32	2.000
21000	22.0	32	2.000
22000	22.0	32	2.000
23000	22.0	32	2.000
24000	22.0	32	2.000
25000	22.0	32	2.000
26000	22.0	32	2.000
27000	22.0	32	2.000
28000	22.0	32	2.000
29000	22.0	32	2.000
30000	22.0	32	2.000
31000	22.0	32	2.000
32000	22.0	32	2.000
33000	22.0	32	2.000
34000	22.0	32	2.000
35000	22.0	32	2.000
36000	22.0	32	2.000
37000	22.0	32	2.000
38000	22.0	32	2.000
39000	22.0	32	2.000
40000	22.0	32	2.000
41000	22.0	32	2.000
42000	22.0	32	2.000
43000	22.0	32	2.000
44000	22.0	32	2.000
45000	22.0	32	2.000
46000	22.0	32	2.000
47000	22.0	32	2.000
48000	22.0	32	2.000
49000	22.0	32	2.000
50000	22.0	32	2.000
51000	22.0	32	2.000
52000	22.0	32	2.000
53000	22.0	32	2.000
54000	22.0	32	2.000
55000	22.0	32	2.000
56000	22.0	32	2.000
57000	22.0	32	2.000
58000	22.0	32	2.000
59000	22.0	32	2.000
60000	22.0	32	2.000
61000	22.0	32	2.000
62000	22.0	32	2.000
63000	22.0	32	2.000
64000	22.0	32	2.000
65000	22.0	32	2.000
66000	22.0	32	2.000
67000	22.0	32	2.000
68000	22.0	32	2.000
69000	22.0	32	2.000
70000	22.0	32	2.000
71000	22.0	32	2.000
72000	22.0	32	2.000
73000	22.0	32	2.000
74000	22.0	32	2.000
75000	22.0	32	2.000
76000	22.0	32	2.000
77000	22.0	32	2.000
78000	22.0	32	2.000
79000	22.0	32	2.000
80000	22.0	32	2.000
81000	22.0	32	2.000
82000	22.0	32	2.000
83000	22.0	32	2.000
84000	22.0	32	2.000
85000	22.0	32	2.000
86000	22.0	32	2.000
87000	22.0	32	2.000
88000	22.0	32	2.000
89000	22.0	32	2.000
90000	22.0	32	2.000
91000	22.0	32	2.000
92000	22.0	32	2.000
93000	22.0	32	2.000
94000	22.0	32	2.000
95000	22.0	32	2.000
96000	22.0	32	2.000
97000	22.0	32	2.000
98000	22.0	32	2.000
99000	22.0	32	2.000
100000	22.0	32	2.000

DES 18

### Proprietà del complemento

Se  $x \xrightarrow{k} y$  allora  $\bar{x} \xrightarrow{\bar{k}} \bar{y}$

$\bar{\cdot}$  è il complemento bit per bit

DES 19

### Chiavi deboli

$k$  è una chiave debole se per ogni  $x$

$x \xrightarrow{k} y \xrightarrow{k} x$

Ci sono 4 chiavi deboli

chiave debole	$C_0$	$D_0$
0101 0101 0101 0101	$0^{28}$	$0^{28}$
FEFE FEFE FEFE FEFE	$1^{28}$	$1^{28}$
1F1F 1F1F OE0E OE0E	$0^{28}$	$1^{28}$
E0E0 E0E0 F1F1 F1F1	$1^{28}$	$0^{28}$

DES 20

### Chiavi semideboli

$k, k'$  è una coppia di chiavi semideboli se per ogni  $x$

$x \xrightarrow{k} y \xrightarrow{k'} x$

Ci sono 6 coppie di chiavi semideboli

$C_0$	$D_0$	$k$	$k'$	$C_0$	$D_0$
$\{01\}^{14}$	$\{01\}^{14}$	01FE 01FE 01FE 01FE	FE01 FE01 FE01 FE01	$\{10\}^{14}$	$\{10\}^{14}$
$\{01\}^{14}$	$\{10\}^{14}$	1FE0 1FE0 0EF1 0EF1	E01F E01F F10E F10E	$\{10\}^{14}$	$\{01\}^{14}$
$\{01\}^{14}$	$0^{28}$	01E0 01E0 01F1 01F1	E001 E001 F101 F101	$\{10\}^{14}$	$0^{28}$
$\{01\}^{14}$	$1^{28}$	1FFE 1FFE 0EFE 0EFE	FE1F FE1F FE0E FE0E	$\{10\}^{14}$	$1^{28}$
$0^{28}$	$\{01\}^{14}$	011F 011F 010E 010E	1F01 1F01 0E01 0E01	$0^{28}$	$\{10\}^{14}$
$1^{28}$	$\{01\}^{14}$	E0FE E0FE F1FE F1FE	FEE0 FEE0 FEF1 FEF1	$1^{28}$	$\{10\}^{14}$

DES 21

### Crittoanalisi differenziale

- Eli Biham e Adi Shamir [1990]
- Già conosciuto da Coppersmith quando fu progettato !?

numero round	chosen plaintext	known plaintext
8	$2^{14}$	$2^{38}$
9	$2^{24}$	$2^{44}$
10	$2^{24}$	$2^{43}$
11	$2^{31}$	$2^{47}$
12	$2^{31}$	$2^{47}$
13	$2^{39}$	$2^{52}$
14	$2^{39}$	$2^{51}$
15	$2^{47}$	$2^{56}$
16	$2^{47}$	$2^{55}$

numero messaggi in chiaro

DES 22

### Crittoanalisi differenziale e lineare

Attacco *known-plaintext* oppure *chosen-plaintext*

Metodo di attacco	known plaintext	chosen plaintext	complessità spazio	complessità tempo
precomputazione esaustiva	-	1	$2^{56}$	1
ricerca esaustiva	1	-	trascurabile	$2^{55}$
crittoanalisi lineare	$2^{43}$ (85%)	-	messaggi	$2^{43}$
	$2^{38}$ (10%)	-	messaggi	$2^{50}$
crittoanalisi differenziale	-	$2^{47}$	messaggi	$2^{47}$
	$2^{55}$	-	messaggi	$2^{55}$

percentuale di successo

DES 23

### Ricerca esaustiva

- Numero chiavi DES =  $2^{56} \approx 7,2056 \cdot 10^{16}$
- Un computer a 500 Mhz che testa una chiave per ciclo di clock impiega  
 $144.115.188$  secondi  $\approx 834$  giorni  $\approx 2$  anni e 3 mesi  
 per provare  $2^{55} \approx 3,6 \cdot 10^{16}$  chiavi

DES 24

### DES challenges

- 10.000 dollari al primo che rompe la *challenge* se rotta entro il 25% del miglior tempo precedente
- Giugno 1997:** 39 giorni, testato 24% delle  $2^{56}$  chiavi, **DESCHALL**
  - Rocke Verser scrisse e distribuì un client di ricerca,
  - 70.000 computer,
  - trovata da Michael K. Sanders (Pentium 90 MHz, 16M)
  - messaggio: Strong cryptography makes the world a safer place
- Luglio 1998:** 56 ore, **Deep Crack**, EFF, 250.000 dollari
- Gennaio 1999:** 22 ore 15 minuti testando 245 miliardi di chiavi al secondo, Distributed.Net 100.000 computer e EFF

DES 25

### Deep Crack: Unità di ricerca

DES 26

### Deep Crack: Unità di ricerca

- Clock di 40Mhz
- Una decifratura in 16 cicli di clock
- Numero chiavi provate al secondo

$$\frac{40.000.000}{16} = 2.500.000$$

DES 27

### Chip

- 24 unità di ricerca
- Prova  $24 \cdot 2.500.000 = 60.000.000$  chiavi al sec.
- Prova tutte le chiavi in 13.900 giorni ( $\approx 38$  anni)

DES 28


### Board

- 64 chip
- 32 per faccia
- 40 cm X 40 cm
- Prova  $64 \cdot 60.000.000 = 3.840.000.000$  chiavi al sec.
- Prova tutte le chiavi in  $\approx 218$  giorni

DES 29

### Chassis

- ❑ 12 schede
- ❑ Prova 12 · 3.840.000.000 = 46.080.000.000 chiavi al sec.
- ❑ Prova tutte le chiavi in ≈18 giorni



DES 30

### EFF DES Cracker




DES 31

### Prestazioni

Device	Quanti nella prossima device	Chiavi/sec	Num. medio Giorni per ricerca
Unità di ricerca	24	2.500.000	166.800
Chip	64	60.000.000	6.950
Board	12	3.840.000.000	109
Chassis	2	46.080.000.000	9,05
EFF DES Cracker		92.160.000.000	4,524

DES 32

### Modalità operative del DES

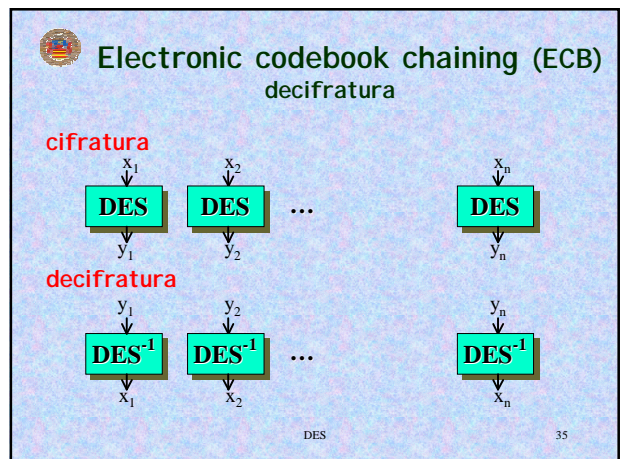
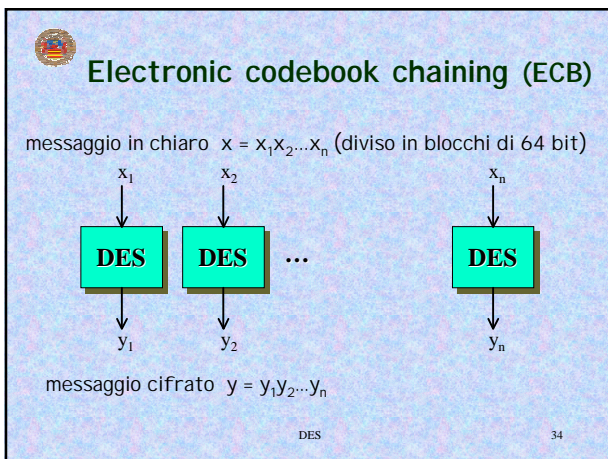


Come cifrare testi più lunghi di 64 bit?

- Electronic codebook chaining (ECB)
- Cipher block chaining (CBC)
- Cipher feedback (CFB)
- Output feedback (OFB)

NBS FIPS PUB 46, DES modes of operation, National Bureau of Standards, 1977

DES 33



### Electronic codebook chaining (ECB)

- Se la lunghezza del messaggio non è multiplo di 64?  
Possibile soluzione: Padding con 100...00
- L'ECB è il metodo più veloce
- Eventuali errori non si propagano 😊
- Non c'è dipendenza tra i blocchi
  - Possibili attacchi di sostituzione
  - Ridondanza testo in chiaro 😞

DES 36

### Cipher Block Chaining (CBC)

messaggio in chiaro  $x = x_1 x_2 \dots x_n$  (diviso in n blocchi di 64 bit)

messaggio cifrato  $y = y_1 y_2 \dots y_n$

vettore di inizializzazione IV di solito pubblico.  
(potrebbe anche essere scelto a caso e tenuto nascosto)

DES 37

### Cipher Block Chaining (CBC) decifratura

cifratura

decifratura

DES 38

### Cipher Block Chaining (CBC)

- Meno veloce dell'ECB 😞
- Propagazione errori 😞
- C'è dipendenza tra i blocchi 😊

Non possibili attacchi di sostituzione

DES 39

### Cipher feedback (CFB)

messaggio in chiaro  $x = x_1 x_2 \dots x_n$  (diviso in n blocchi di 64 bit)

messaggio cifrato  $y = y_1 y_2 \dots y_n$

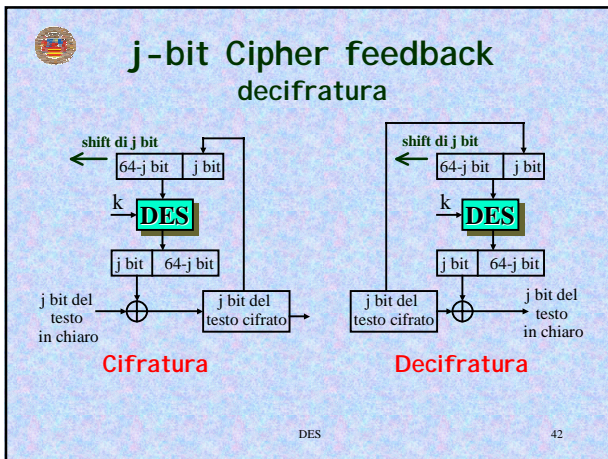
DES 40

### j-bit Cipher feedback

shift di j bit

Si inizia cifrando IV

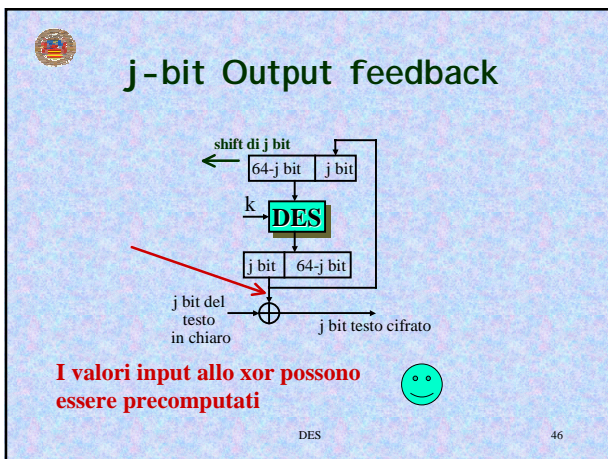
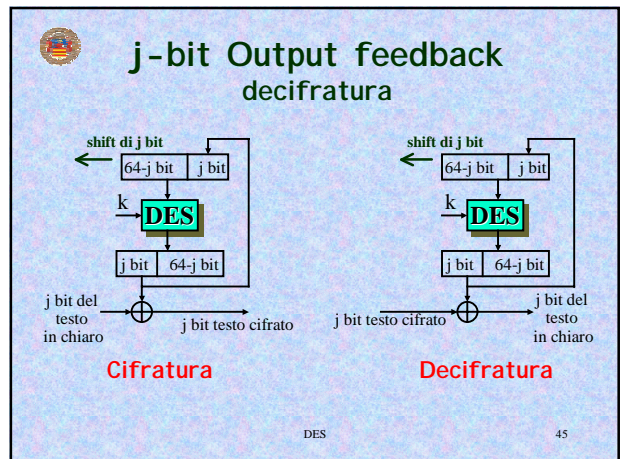
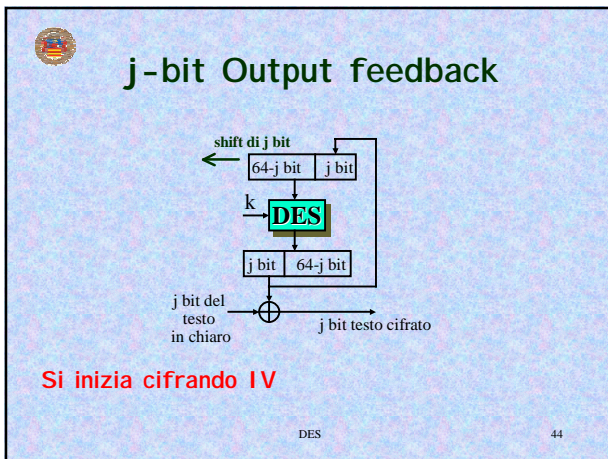
DES 41



### j-bit Cipher feedback

- ❑ j può essere scelto a piacimento, ad es. j=8
- ❑ Si possono utilizzare j bit cifrati senza aspettarne 64 😊
- ❑ Più lento al decrescere di j 😞

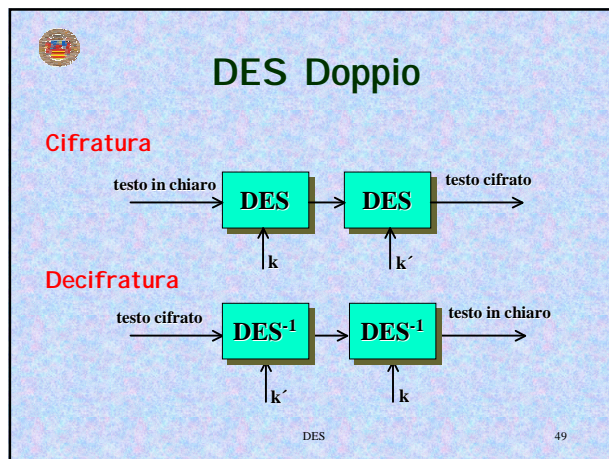
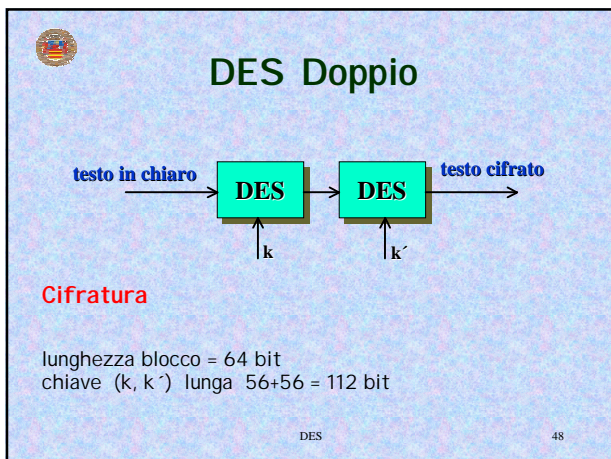
DES                      43



### j-bit Output feedback

Se la stessa chiave e lo stesso IV vengono usati per diversi OFB, la *keystream* è la stessa!  
 IV deve essere cambiato se si usa la stessa chiave

DES                      47



### Sicurezza DES doppio

Quanto è "sicuro"  
il DES doppio?

DES 50

### DES ≡ DES doppio ?

E' possibile che per ogni (k, k') esiste k'' tale che

$$DES_{k''}(\cdot) = DES_{k'}(DES_k(\cdot))$$

DES 51

### DES non forma un gruppo

- ❑ Ci sono  $(2^{64})! > 10^{347.380.000.000.000.000} > 10^{10^{20}}$  permutazioni per i  $2^{64}$  input
- ❑ Ci sono solo  $2^{56}$  permutazioni definite dal DES

L'insieme delle  $2^{56}$  permutazioni definite dalle  $2^{56}$  chiavi DES non è chiuso per composizione (dimostrato solo nel 1992)

[Gruppo generato da composizione di DES]  $> 10^{2499}$

DES 52

### DES Doppio: attacco *meet in the middle*

**Known Plaintext Attack**  
 Input:  $x, y = DES_{k'}(DES_k(x))$   
 Costruisci tabella  
 for  $k_2 \in (0,1)^{56}$   
   do  $z = DES_{k_2}^{-1}(y)$   
   if per qualche  $k_1, (k_1, z)$  è nella tabella  
   then return la chiave è  $(k_1, k_2)$

chiave	testo cifrato
k''	DES <sub>k''</sub> (x)
...	...

DES 53

### DES Doppio: attacco meet in the middle

**Known Plaintext Attack**

Input:  $x, y = \text{DES}_k(\text{DES}_k(x))$   
 Costruisci tabella

chiave	testo cifrato
$k^*$	$\text{DES}_{k^*}(x)$
...	...

**for**  $k_2 \in \{0,1\}^{56}$   
**do**  $z = \text{DES}_{k_2}^{-1}(y)$   
**if** per qualche  $k_1, (k_1, z)$  è nella tabella  
**then return** la chiave è  $(k_1, k_2)$


Complessità spazio:  $2^{56}$  righe nella tabella  
 Complessità tempo:  $2^{57}$  cifrature +  $2^{56}$  ricerche in tabella

O(1) se tabella hash  
 56 se array ordinato

DES 54

### DES Doppio: attacco meet in the middle


L'output  $(k_1, k_2)$  è sicuramente la chiave cercata?



DES 55

### DES Doppio: attacco meet in the middle

Dato  $x$ , qual'è il numero medio di chiavi  $(k_1, k_2)$  tali che  
 $y = \text{DES}_{k_2}(\text{DES}_{k_1}(x))$



DES 56

### DES Doppio: attacco meet in the middle

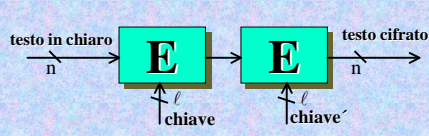
Dato  $x, y$ , qual'è il numero medio di chiavi  $(k_1, k_2)$  tali che  
 $y = \text{DES}_{k_2}(\text{DES}_{k_1}(x))$

Fissato  $x$ , ci sono  $2^{112}$  chiavi e  $2^{64}$  testi cifrati  $y$

$$\frac{\# \text{chiavi}}{\#y \text{ per fissato } x} = \frac{2^{112}}{2^{64}} = 2^{48}$$

DES 57

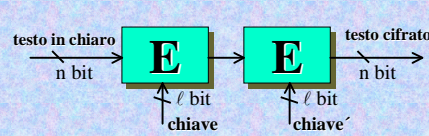
### Doppia cifratura



Cifrario a blocchi casuale: dati  $n$  ed  $l$ , scegli a caso  $2^l$  permutazioni tra le  $(2^n)!$  possibili su  $2^n$  elementi, ed associale con le  $2^l$  chiavi

DES 58

### Doppia cifratura



Dato  $x$ , y il numero medio di chiavi  $(k_1, k_2)$  tali che  
 $y = E_{k_2}(E_{k_1}(x))$   
 è

$$2^{2l-n}$$

DES 59

### DES Doppio: attacco meet in the middle

**Known Plaintext Attack**

Input:  $x, y = \text{DES}_k(\text{DES}_k(x))$   
 $x', y' = \text{DES}_k(\text{DES}_k(x'))$

chiave	testo cifrato
$k'$	$\text{DES}_{k'}(x)$
...	...

Costruisci tabella  
**for**  $k_2 \in \{0,1\}^{56}$   
**do**  $z = \text{DES}_{k_2}^{-1}(y)$   
**if** per qualche  $k_1$ ,  $(k_1, z)$  è nella tabella  
e  $y' = \text{DES}_{k_2}(\text{DES}_{k_1}(x'))$   
**then return** la chiave è  $(k_1, k_2)$

DES 60

### DES Doppio: attacco meet in the middle

Dato  $x, y, x', y'$  qual è il numero medio di chiavi  $(k_1, k_2)$  tali che

$$y = \text{DES}_{k_2}(\text{DES}_{k_1}(x))$$

$$y' = \text{DES}_{k_2}(\text{DES}_{k_1}(x'))$$

Fissati  $x, x'$ , ci sono  $2^{112}$  chiavi e  $2^{128}$  testi cifrati  $y, y'$

$$\frac{\# \text{chiavi}}{\# y, y' \text{ per fissati } x, x'} = \frac{2^{112}}{2^{128}} = 2^{-16}$$

DES 61

### Cascata con L-stadi di un cifrario

Dati  $x_1, y_1, \dots, x_t, y_t$  il numero medio di chiavi  $(k_1, k_2, \dots, k_L)$  tali che

$$y_i = E_{k_L}(\dots E_{k_2}(E_{k_1}(x_i)))$$

è  $2^{L \cdot tn}$

DES 62

### DES Doppio: attacco meet in the middle

- Tradeoff tempo-memoria
- Indovino i primi  $s$  bit di  $k$ ,  $0 \leq s \leq 56$
- $2^s$  tabelle di  $2^{56-s}$  righe

Complessità spazio:  $2^{56-s}$  righe nella tabella

Complessità tempo:  $\underbrace{2^s}_{2^{56-s}} \cdot 2^{56-s}$  cifrature +  $\underbrace{2^s}_{2^{56-s}} \cdot 2^{56-s}$  ricerche in tabella

**SPAZIO \* TEMPO  $\approx 2^{112}$**

DES 63

### DES Doppio: attacco meet in the middle

**Known Plaintext Attack**

Input:  $x, y = \text{DES}_k(\text{DES}_k(x))$   
 $x', y' = \text{DES}_k(\text{DES}_k(x'))$

chiave	testo cifrato
$k' = uv$	$\text{DES}_{k'}(x)$
...	...

**for**  $u \in \{0,1\}^s$   
Costruisci tabella per  $v \in \{0,1\}^{56-s}$   
**for**  $k_2 \in \{0,1\}^{56}$   
**do**  $z = \text{DES}_{k_2}^{-1}(y)$   
**if** per qualche  $k_1$ ,  $(k_1, z)$  è nella tabella  
e  $y' = \text{DES}_{k_2}(\text{DES}_{k_1}(x'))$   
**then return** la chiave è  $(k_1, k_2)$

Complessità spazio:  $2^{56-s}$  righe nella tabella

Complessità tempo:  $2^s \cdot 2^{56-s}$  cifrature +  $2^s \cdot 2^{56-s}$  ricerche in tabella

**SPAZIO \* TEMPO  $\approx 2^{112}$**

DES 64

### DES Triplicato

**Cifratura**

- lunghezza blocco = 64 bit
- chiave  $(k, k', k'')$  lunga  $56 + 56 + 56 = 168$  bit

DES 65

### DES Triplicato: attacco meet in the middle

**Known Plaintext Attack**  
 Input:  $x, y = \text{DES}_{k''} \cdot (\text{DES}_{k'} \cdot (\text{DES}_k((x)))$   
 Costruisci tabella

chiave	testo cifrato
$(k'', k')$	$\text{DES}_{k''} \cdot (\text{DES}_{k'}(x))$
...	...

**for**  $k_3 \in \{0,1\}^{56}$   
**do**  $z = \text{DES}^{-1}_{k_3}(y)$   
**if** per qualche  $k_1, k_2, (k_1, k_2, z)$  è nella tabella  
**then return** la chiave è  $(k_1, k_2, k_3)$

DES 66

### DES Triplicato: attacco meet in the middle

**Known Plaintext Attack**  
 Input:  $x, y = \text{DES}_{k''} \cdot (\text{DES}_{k'} \cdot (\text{DES}_k((x)))$   
 Costruisci tabella

chiave	testo cifrato
$(k'', k')$	$\text{DES}_{k''} \cdot (\text{DES}_{k'}(x))$
...	...

**for**  $k_3 \in \{0,1\}^{56}$   
**do**  $z = \text{DES}^{-1}_{k_3}(y)$   
**if** per qualche  $k_1, k_2, (k_1, k_2, z)$  è nella tabella  
**then return** la chiave è  $(k_1, k_2, k_3)$

Complessità spazio:  $2^{112}$  righe nella tabella  
 Complessità tempo:  $2^{112} + 2^{56}$  cifrature +  $2^{56}$  ricerche in tabella

DES 67

### DES Triplicato: attacco meet in the middle

**Known Plaintext Attack**  
 Input:  $x, y = \text{DES}_{k''} \cdot (\text{DES}_{k'} \cdot (\text{DES}_k((x)))$   
 Costruisci tabella

chiave	testo cifrato
$k''$	$\text{DES}_{k''}((x))$
...	...

**for**  $k_3, k_2 \in \{0,1\}^{56} \times \{0,1\}^{56}$   
**do**  $z = \text{DES}^{-1}_{k_2}(\text{DES}^{-1}_{k_3}(y))$   
**if** per qualche  $k_1, (k_1, z)$  è nella tabella  
**then return** la chiave è  $(k_1, k_2, k_3)$

DES 68

### DES Triplicato: attacco meet in the middle

**Known Plaintext Attack**  
 Input:  $x, y = \text{DES}_{k''} \cdot (\text{DES}_{k'} \cdot (\text{DES}_k((x)))$   
 Costruisci tabella

chiave	testo cifrato
$k''$	$\text{DES}_{k''}((x))$
...	...

**for**  $k_3, k_2 \in \{0,1\}^{56} \times \{0,1\}^{56}$   
**do**  $z = \text{DES}^{-1}_{k_2}(\text{DES}^{-1}_{k_3}(y))$   
**if** per qualche  $k_1, (k_1, z)$  è nella tabella  
**then return** la chiave è  $(k_1, k_2, k_3)$

Complessità spazio:  $2^{56}$  righe nella tabella  
 Complessità tempo:  $2^{56} + 2^{112}$  cifrature +  $2^{112}$  ricerche in tabella

DES 69

### DES Triplo: attacco meet in the middle

Complessità *Known Plaintext Attack*  $\approx 2^{112}$   
 Ricerca esaustiva su tutte le chiavi  $\approx 2^{112}$

DES 70

### DES Triplicato: attacco meet in the middle

Complessità *Known Plaintext Attack*  $\approx 2^{112}$

“Equivalente” ad un cifrario con una chiave di 112 bit, e non 168 bit

DES 71

### DES Triplo

**Cifratura**

- ❑ lunghezza blocco = 64 bit
- ❑ chiave (k, k') lunga 56+56 = 112 bit
- ❑ spesso chiamato EDE<sub>k,k'</sub> (acronimo per Encrypt Decrypt Encrypt)
- ❑ adottato negli standard X9.17 e ISO 8732

DES 72

### DES Triplo: attacco *meet in the middle*

**Known Plaintext Attack**  
 Input:  $x, y = \text{DES}_k(\text{DES}_{k'}^{-1}(\text{DES}_k(x)))$   
 Costruisci tabella

chiave	testo cifrato
$k'$	$\text{DES}_{k'}^{-1}(x)$
...	...

for  $k_1, k_2 \in \{0,1\}^{56} \times \{0,1\}^{56}$   
 do  $z = \text{DES}_{k_2}(\text{DES}_{k_1}^{-1}(y))$   
 if  $(k_1, z)$  è nella tabella  
 then return la chiave è  $(k_1, k_2)$

DES 73

### DES Triplo: attacco *meet in the middle*

**Known Plaintext Attack**  
 Input:  $x, y = \text{DES}_k(\text{DES}_{k'}^{-1}(\text{DES}_k(x)))$   
 Costruisci tabella

chiave	testo cifrato
$k'$	$\text{DES}_{k'}^{-1}(x)$
...	...

for  $k_1, k_2 \in \{0,1\}^{56} \times \{0,1\}^{56}$   
 do  $z = \text{DES}_{k_2}(\text{DES}_{k_1}^{-1}(y))$   
 if  $(k_1, z)$  è nella tabella  
 then return la chiave è  $(k_1, k_2)$

Complessità spazio:  $2^{56}$  righe nella tabella  
 Complessità tempo:  $2^{56} + 2^{112}$  cifrature +  $2^{112}$  ricerche in tabella

DES 74

### Compatibilità DES Triplo e DES

Se  $k = k'$  il DES triplo

è equivalente al semplice DES

DES 75

### Decifratura DES Triplo

**Cifratura**

**Decifratura**

DES 76