Cifrari a blocchi:
Data Encryption Standard

Barbara Masucci

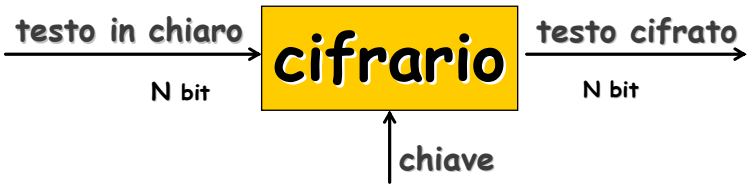
Dipartimento di Informatica ed Applicazioni
Università di Salerno

masucci@dia.unisa.it
http://www.dia.unisa.it/professori/masucci

Cifrari simmetrici

- Crittosistemi a chiave privata/segreta
- Alice e Bob conoscono la stessa chiave K
- Cifrari a blocchi
  - Messaggi divisi in blocchi e poi cifrati
- Stream cipher
  - Messaggi cifrati carattere per carattere

Cifrari a blocchi



- Il testo in chiaro è diviso in blocchi di lunghezza fissa
- Viene cifrato un blocco alla volta
  - Data Encryption Standard (DES)
  - DES triplo
  - Blowfish
  - RC2, RC5, RC6
  - Advanced Encryption Standard (AES)

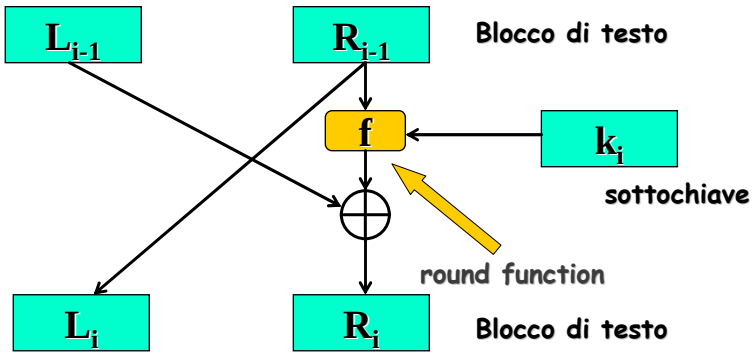
Cifrari di Feistel

- Molti dei cifrari a blocchi in uso si basano sulla proposta di Feistel del 1973
- Operazioni utilizzate:
  - Permutazioni
  - Sostituzioni
- Principi utilizzati, proposti da Shannon nel 1949 per complicare l'analisi statistica
  - Diffusione: ogni cifra del testo cifrato è prodotta da più cifre del testo in chiaro
  - Confusione: le relazioni statistiche tra testo cifrato e valore della chiave sono complicate

Cifrari di Feistel: Caratteristiche

- Dimensioni del blocco
  - Blocchi grandi migliorano la sicurezza ma riducono la velocità
- Dimensioni della chiave
  - Chiavi grandi migliorano la sicurezza ma riducono la velocità
- Numero di round
  - Tutti i round hanno la stessa struttura
- Algoritmo di schedulazione della chiave
  - A partire dalla chiave iniziale vengono prodotte tante sottochiavi quanti sono i round

Cifrari di Feistel: struttura di un round



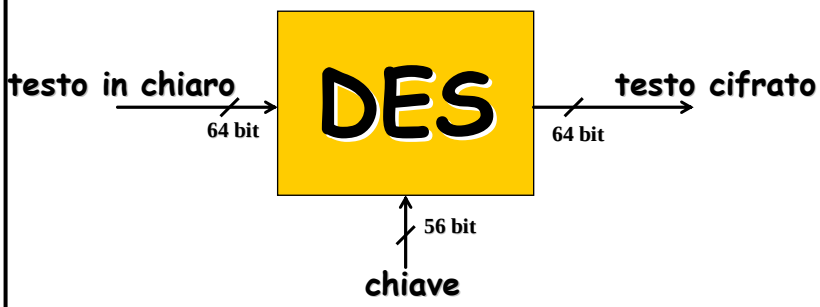
Cifrari di Feistel

- Cifratura:
  - Basta implementare un solo round
  - Lo stesso codice può essere usato per ogni round
- Decifratura
  - Usa lo stesso algoritmo per la cifratura
  - Usa le sottochiavi in ordine inverso
- Esempi di cifrari di Feistel
  - DES
  - Blowfish

Data Encryption Standard (DES)

- 15 maggio 1973: richiesta pubblica per uno standard della NBS, oggi NIST
- 27 agosto 1974: seconda richiesta
- 1975: Lucifer, sviluppato da IBM nel '71, viene modificato dalla NSA (chiave da 128 a 56 bit)
- 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)

Data Encryption Standard

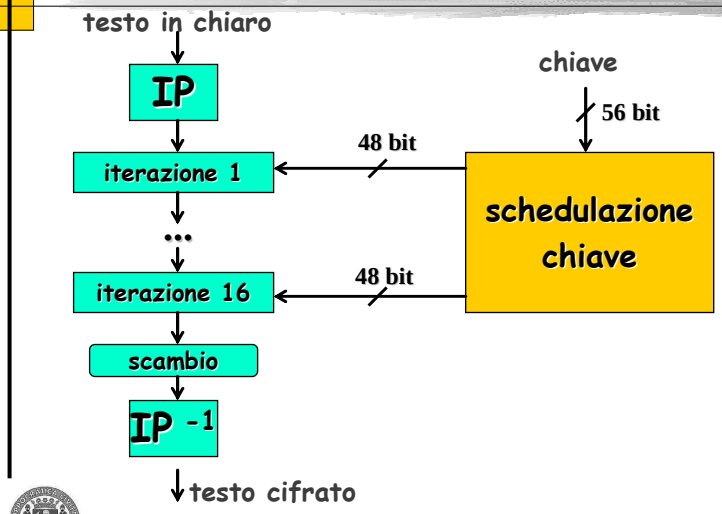


Lunghezza della Chiave

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

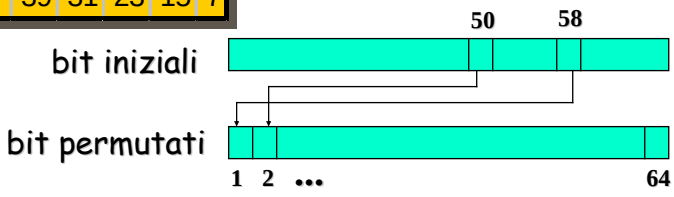
è lo xor dei precedenti 7 bit

Struttura del DES



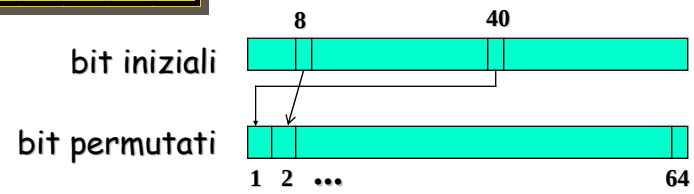
Permutazione Iniziale IP

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

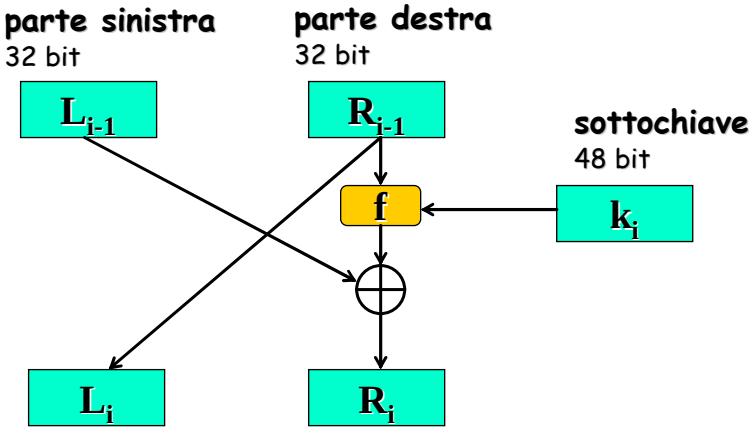


Permutazione Inversa IP^{-1}

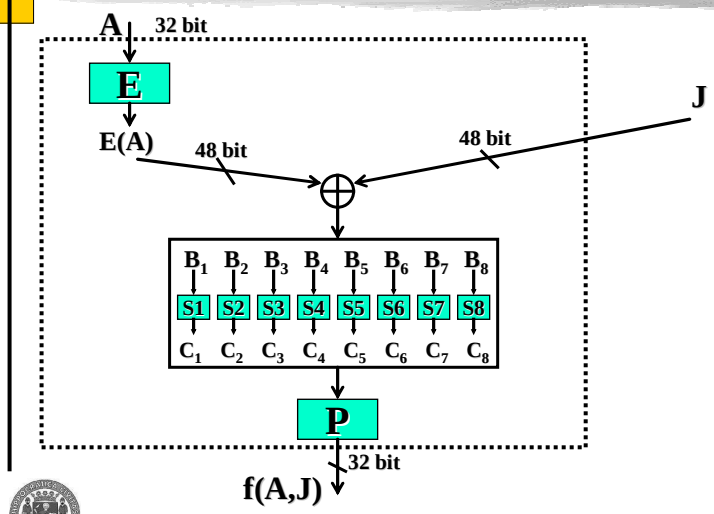
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25



Singola Iterazione



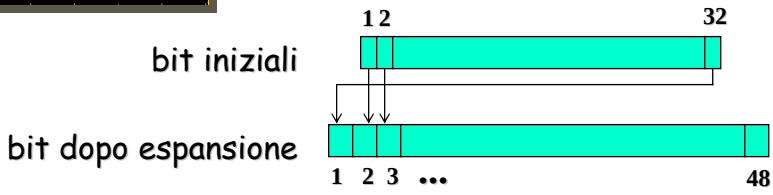
La funzione f



Espansione 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

16 bit sono duplicati



S-box

	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

6 bit in input specificano un elemento della tabella la cui conversione binaria dà i 4 bit output

Funzionamento delle S-box

input **101110**

primo ed ultimo bit

10

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	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

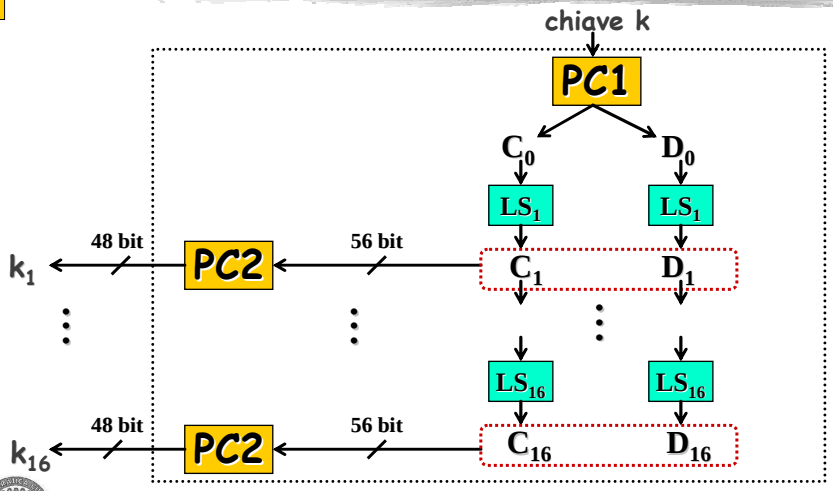
output **11** in binario = **1011**

Proprietà delle S-box

[NBS, 1976]

- Ogni riga è una permutazione degli interi 0,..,15
- Nessuna S-box è una funzione lineare dei suoi input
- Cambiando un solo bit di input ad una S-box variano almeno due bit nell'output
- Per ogni S-box S e per ogni input x a 6 bit: $S(x)$ e $S(x \oplus 001100)$ differiscono in almeno due bit
- Per ogni S-box, per ogni input x e per ogni bit d,g, $S(x) \neq S(x \oplus 11dg00)$
- Per ogni S-box, il numero degli input per i quali il bit di output è 0 è circa uguale al numero degli input per i quali tale bit è 1

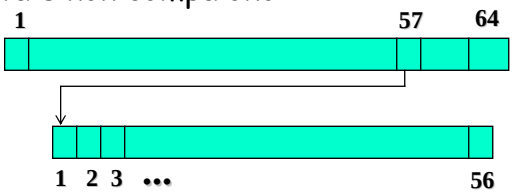
Schedulazione delle chiavi



Permutazione 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

i bit in posizione 8, 16, 24, 32, 40, 48, 56, 64
sono di parità e non compaiono



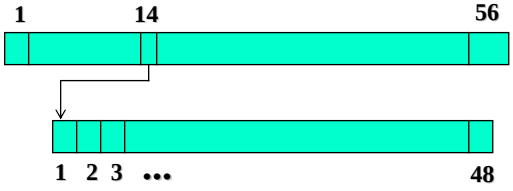
Barbara Masucci - DIA – Università di Salerno

20

Compressione-permutazione 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	26	41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32

8 bit soppressi in posizione
9, 18, 22, 25, 35, 38, 43 e 54



Barbara Masucci - DIA – Università di Salerno

21

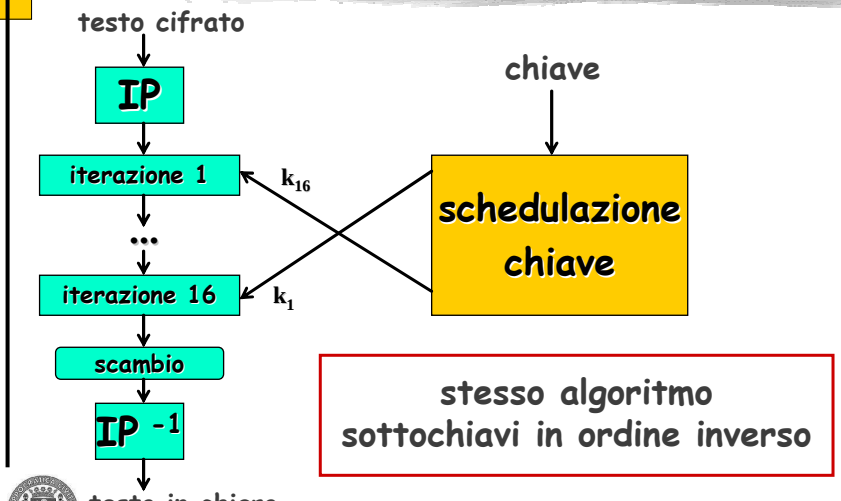
Schedulazione shift a sinistra

iterazione	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
shift	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Totale shift nelle 16 iterazioni = 28 posizioni

Decifratura DES

Decifratura DES



stesso algoritmo
sottochiavi in ordine inverso

Prestazioni Hardware

Hardware: chip della Digital, 1 Gbit/secondo

Processore	Frequenza del clock (Mhz)	Parola macchina (in bits)	Numero di blocchi DES (per second)
8088	4.7	8	370
68000	7.6	16	900
80286	6.0	16	1.100
68020	16.0	32	3.500
68030	16.0	32	3.900
80286	25.0	16	5.000
68030	50.0	32	10.00
68040	25.0	32	16.000
68040	40.0	32	23.000
80486	66.0	32	43.000
Sun ELC			26.000
HyperSparc			32.000
RS6000-350			53.000
Sparc 10-52			84.000
DEC Alpha 4000-610			154.000
HP 9000-887	125		196.000

Prestazioni Software

Pentium II 400, FreeBSD, OpenSSL

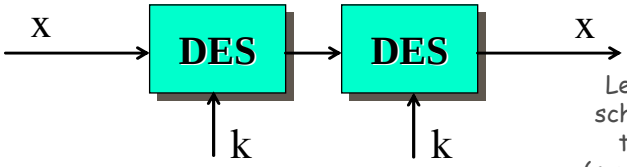
	MB/s
DES	9

Celeron 850, Windows 2000, Crypto++

	MB/s
DES	12,871

Chiavi deboli

k è una chiave debole se per ogni x



Le sottochiavi schedulate sono tutte uguali (sempre la stessa, usata 16 volte)

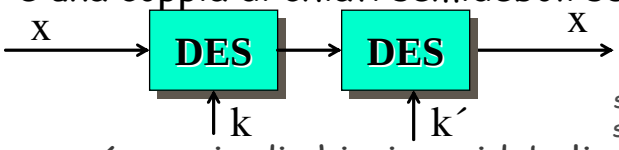
Ci sono 4 chiavi deboli

Rappresentazione esadecimale

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

Chiavi semideboli

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

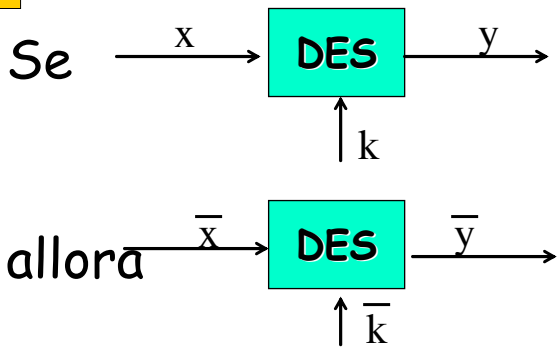


Le sottochiavi schedulate sono solo due, ognuna usata 8 volte

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 OE01 0E01	0^{28}	$\{10\}^{14}$
1^{28}	$\{01\}^{14}$	E0FE E0FE F1FE F1FE	FEE0 FEE0 FEF1 FEF1	1^{28}	$\{10\}^{14}$

Proprietà del complemento



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

con un attacco chosen plaintext si esaminano 2^{55} chiavi invece che 2^{56}

Ricerca esaustiva

- Numero chiavi DES = $2^{56} \approx 7{,}2056 \cdot 10^{16}$ = 72 milioni di miliardi di combinazioni distinte
- Considerando un computer che svolge:
  - 1 cifratura DES al microsecondo, ci vogliono circa 1142 anni per provare la metà dello spazio delle chiavi $2^{55} \approx 3{,}6 \cdot 10^{16}$ chiavi
  - 1 milione di cifrature DES al microsecondo, ci vogliono solo circa 10 ore

Ricerca esaustiva

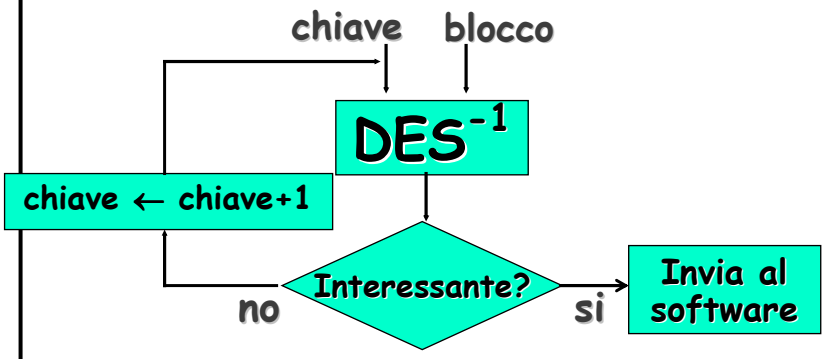
Con macchine parallele è possibile diminuire il tempo richiesto dalla ricerca esaustiva

- 1977: ipotesi di macchina in grado di rompere il DES in un giorno
  - costo: 20 milioni di dollari
  - 10^6 chip, in grado di testare 10^6 chiavi al secondo
- 1993: ipotesi di macchina in grado di rompere il DES in tre ore e mezza
  - Costo: 1 milione di dollari
  - 10 macchine in parallelo, ciascuna con 5760 chip

DES challenges

- Proposte da RSA Data Security
  - 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

Deep Crack: Unità di ricerca



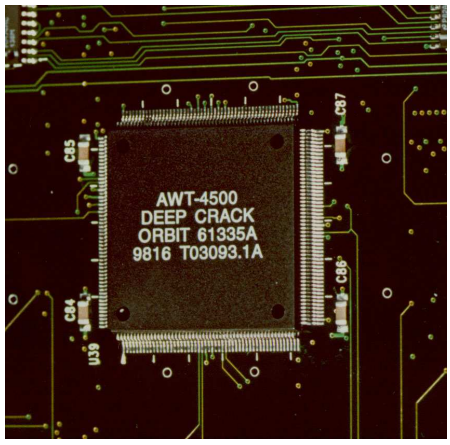
Deep Crack: Unità di ricerca

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

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

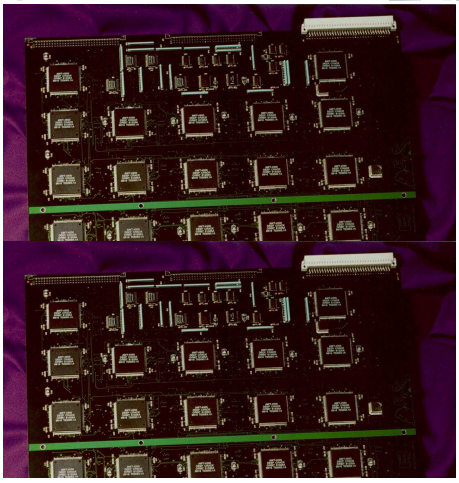
Chip

- 24 unità di ricerca
- Prova 24 · 2.500.000 = 60.000.000 chiavi al sec.
- Prova tutte le chiavi in 13.900 giorni (≈38 anni)



Board

- 64 processori
- 32 per faccia
- 40 cm X 40 cm
- Prova 64·60.000.000 = 3.840.000.000 chiavi al sec.
- Prova tutte le chiavi in ≈218 giorni



Chassis

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

EFF DES Cracker

1998: ricavata la chiave in sole 56 ore
costo: $ 250000

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

Attacchi sofisticati al DES

Crittoanalisi differenziale

- Biham e Shamir, 1990
- Già noto a Coppersmith quando fu progettato?
- Recupera la chiave a partire da 2^{47} coppie (plaintext, ciphertext) di testi scelti

Crittoanalisi lineare

- Matsui, 1993
- Recupera la chiave a partire da 2^{43} coppie (plaintext, ciphertext) di testi noti
- Implementato nel 1993: 10 giorni su 12 macchine

Modalità operative del DES

Come cifrare testi più lunghi di 64 bit?

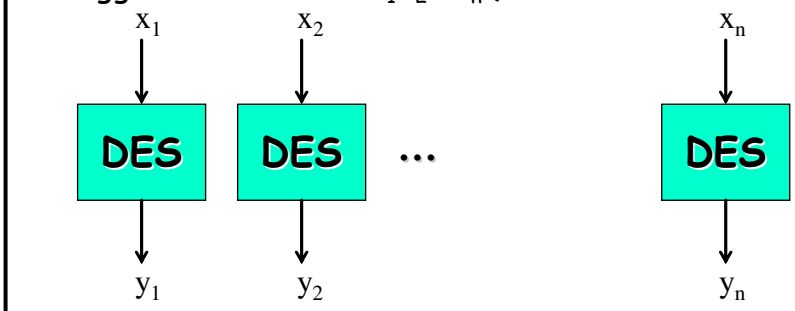
- Electronic codebook chaining (ECB)
- Cipher block chaining (CBC)
- Cipher feedback (CFB)
- Output feedback (OFB)
- Counter (CTR)

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

NIST SP 800-38A, Recommendation for block cipher modes of operation, National Institute of Standards and Technology, 2001

Electronic codebook chaining (ECB)

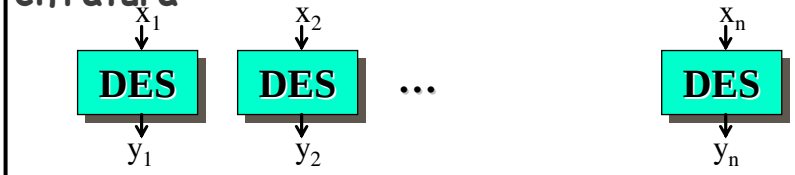
messaggio in chiaro $x = x_1x_2...x_n$ (diviso in n blocchi di 64 bit)



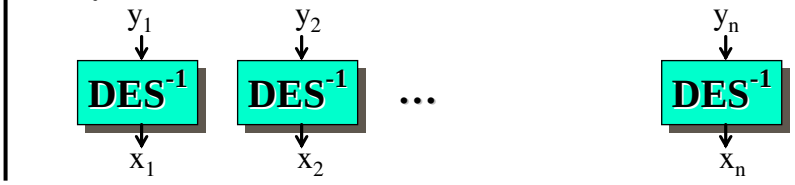
messaggio cifrato $y = y_1y_2...y_n$

Electronic codebook chaining (ECB)

cifratura



decifratura



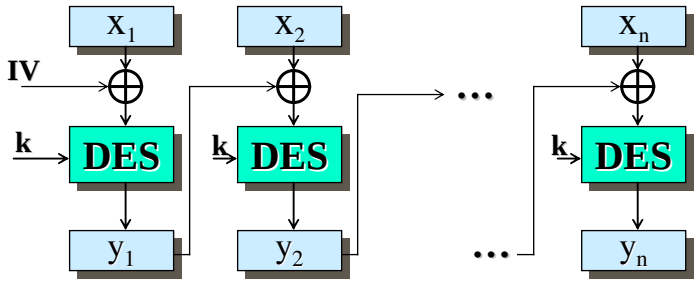
Electronic codebook chaining (ECB)

- 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

Cipher Block Chaining (CBC)

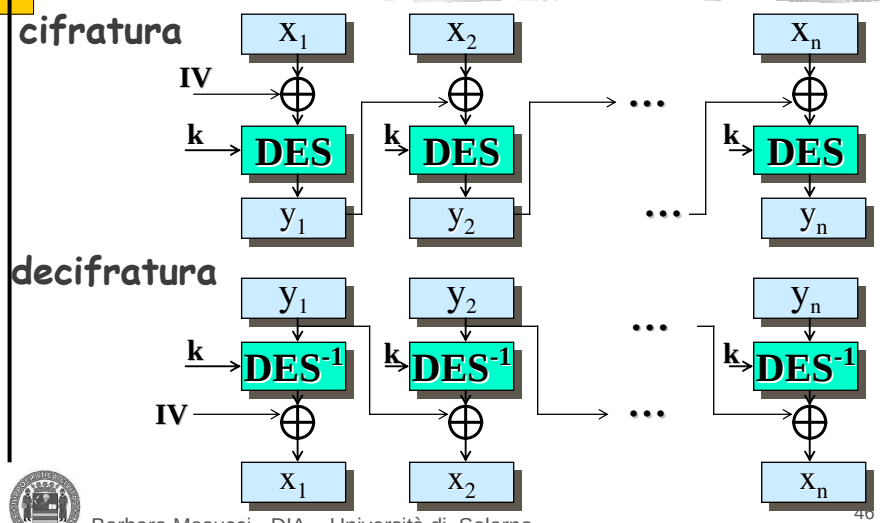
messaggio in chiaro $x=x_1x_2…x_n$ (diviso in n blocchi di 64 bit)



messaggio cifrato $y = y_1y_2…y_n$

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

Cipher Block Chaining (CBC)



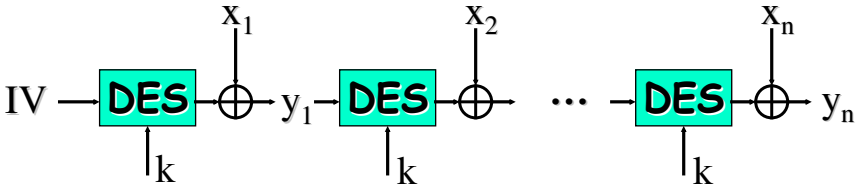
Cipher Block Chaining (CBC)

- Meno veloce dell'ECB
- Propagazione errori

- C'è dipendenza tra i blocchi
- Non possibili attacchi di sostituzione

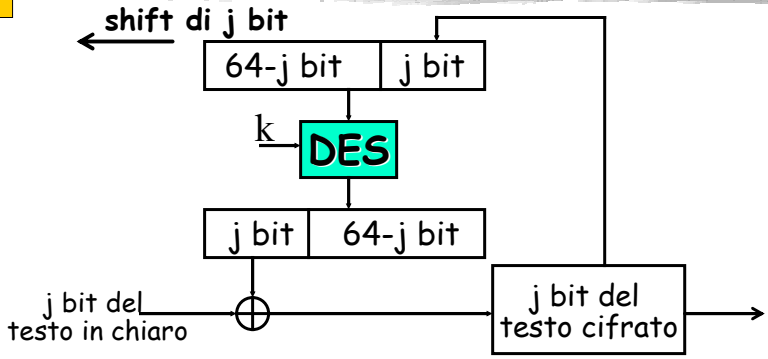
Cipher feedback (CFB)

messaggio in chiaro $x=x_1x_2...x_n$
(diviso in n blocchi di 64 bit)



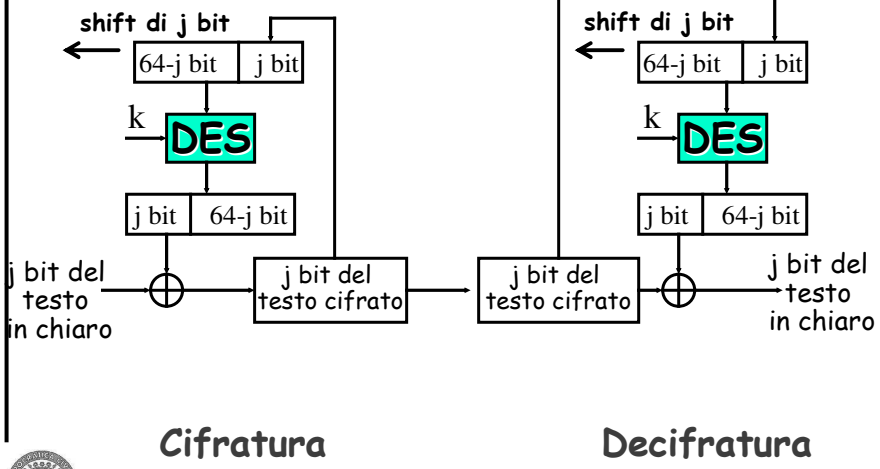
messaggio cifrato $y = y_1y_2...y_n$

j-bit CFB



Si inizia cifrando IV

j-bit CFB



Cifratura Decifratura

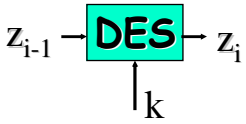
j-bit CFB

- 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

Output feedback (OFB)

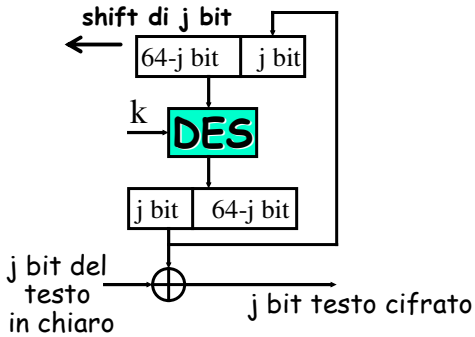
messaggio in chiaro $x=x_1x_2...x_n$
(diviso in n blocchi di 64 bit)

sequenza $z=z_0z_1...z_n$ indipendente dal messaggio, z_0=IV



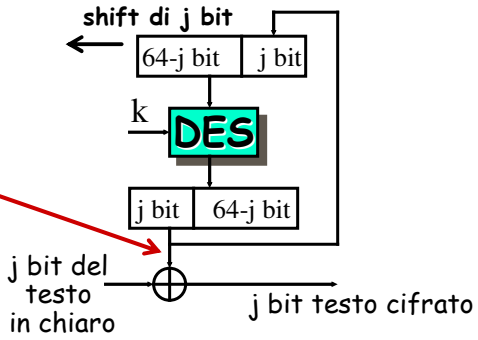
messaggio cifrato $y = y_1y_2...y_n$ $\quad y_i=x_i \oplus z_i$

j-bit OFB



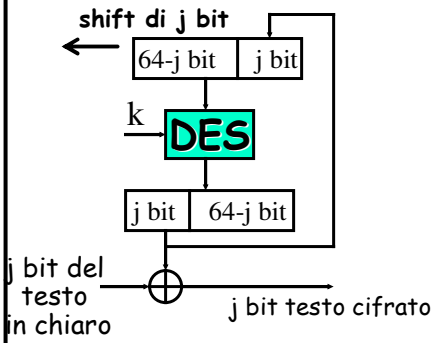
Si inizia cifrando IV

j-bit OFB

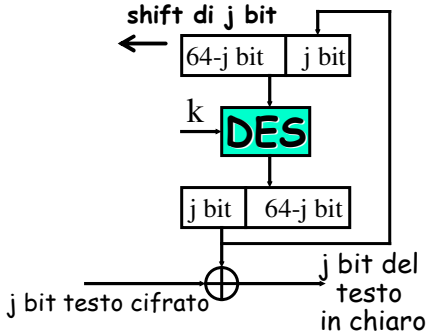


I valori input allo xor possono essere precomputati

j-bit OFB



Cifratura



Decifratura

j-bit CFB

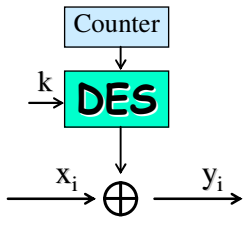
- XOR veloci da realizzare 
- Non c'è dipendenza tra i blocchi 
  - Cambiando un bit nel testo in chiaro, cambia un solo bit nel cifrato

Counter

Impiega un contatore delle dimensioni del blocco in chiaro:

Vantaggi:

- Efficienza hardware e software
- Preelaborazione
- Accesso casuale
- Sicurezza dimostrabile
- Semplice



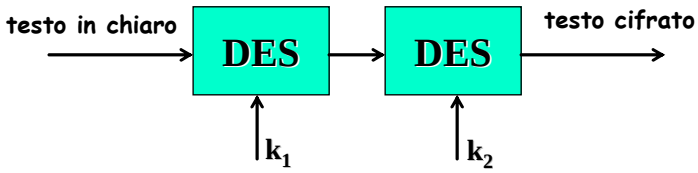
Bibliografia

- Cryptography: Theory and Practice by D. Stinson (1995)
  - cap. 3
- Cryptography and Network Security by W. Stallings (2003)
  - cap. 3
- Tesina di Sicurezza su reti
  - Data Encryption Standard

Cifratura multipla

- Debolezze del DES
  - chiave piccola (56 bit)
  - taglia dei blocchi piccola (64 bit)
- Come costruire un cifrario più sicuro a partire dal DES (senza modificarne la struttura)?
- Cifratura multipla
  - Cifrare il messaggio varie volte con chiavi differenti, sperando che questo aumenti la sicurezza...

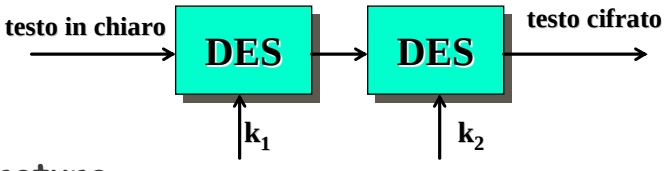
DES Doppio



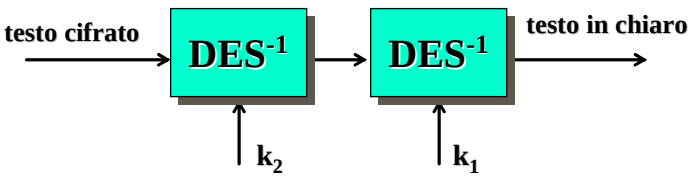
- lunghezza blocco = 64 bit
- chiave (k_1, k_2) lunga 56+56 = 112 bit

DES Doppio

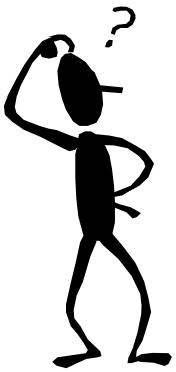
Cifratura



Decifratura



Sicurezza DES doppio



Quanto è "sicuro" il DES doppio?

DES ≡ DES doppio ?

Data una coppia (k_1, k_2), se esistesse k_3 tale che

$$DES_{k_3}(\cdot) = DES_{k_2}(DES_{k_1}(\cdot))$$

la doppia cifratura sarebbe equivalente

ad una cifratura singola

DES non forma un gruppo

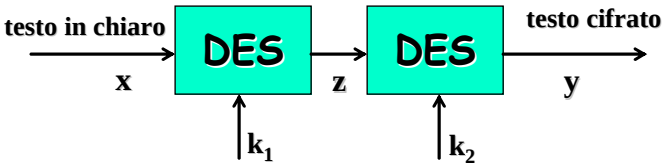
- Esistono $2^{64}! > 10^{347.380.000.000.000.000.000} > 10^{10^{20}}$ permutazioni
  - Corrispondenti ai 2^{64} input possibili
- Ci sono $2^{56} << 10^{10^{20}}$ permutazioni definite da DES
  - A ciascuna chiave, DES fa corrispondere una permutazione
- Se DES viene applicato due volte con chiavi diverse può produrre una delle permutazioni non definite da DES

L'insieme delle 2^{56} permutazioni definite dalle 2^{56} chiavi DES non è chiuso per composizione

(dimostrato solo nel 1992)

DES Doppio

attacco *meet in the middle*



- Data una coppia nota (x,y) eseguo tutte le cifrature per i 2^{56} valori possibili di k_1 in una tabella
- Eseguo le decifrature per i 2^{56} valori possibili di k_2 e cerco le corrispondenze nella tabella

DES Doppio:
attacco meet in the middle

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

chiave	testo cifrato
k_1	$DES_{k_1}(x)$
…	…

DES Doppio:
attacco *meet in the middle*

- **Complessità spazio**: 2^{56} righe nella tabella
- **Complessità tempo**:
  - 2^{56} cifrature per x (costruzione tabella)
  - 2^{56} decifrature per y
  - 2^{56} ricerche in tabella
    - O(1) se tabella hash
    - 56 se array ordinato

DES Doppio:
attacco *meet in the middle*

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

DES Doppio:
attacco *meet in the middle*

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

$y = DES_{k_2}(DES_{k_1}(x))$?

DES Doppio:
attacco *meet in the middle*

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

$$y = DES_{k_2}(DES_{k_1}(x))?$$

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

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

DES Doppio:
attacco *meet in the middle*

Known Plaintext Attack

Input: $x, y = DES_{k_2}(DES_{k_1}(x))$

$x', y' = DES_{k_2}(DES_{k_1}(x'))$

Costruisci tabella

chiave	testo cifrato
k_1	$DES_{k_1}(x)$
…	…

for $k_2 \in \{0,1\}^{56}$

do $z = DES^{-1}_{k_2}(y)$

if per qualche k_1, (k_1, z) è nella tabella

e $y' = DES_{k_2}(DES_{k_1}(x'))$

then return la chiave è (k_1,k_2)

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

$$y = DES_{k_2}(DES_{k_1}(x))$$

$$y' = DES_{k_2}(DES_{k_1}(x'))\ ?$$

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

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

Prob. di indovinare la chiave corretta = $1- 2^{-16}= 0.99998474$

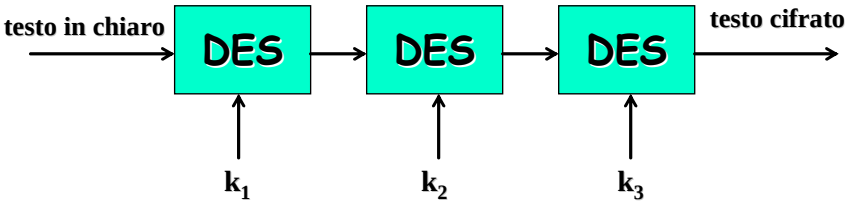
DES Doppio: attacco *meet in the middle*

Complessità *Known Plaintext Attack* $\approx 2^{56}$

Ricerca esaustiva su tutte le chiavi $\approx 2^{112}$

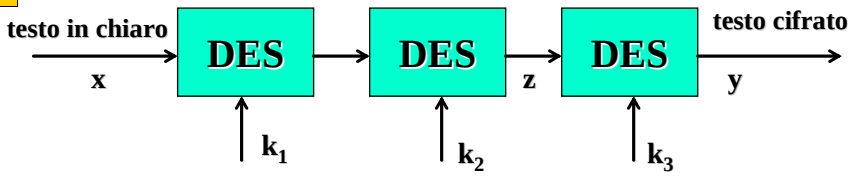
"Equivalente" ad un cifrario con una chiave di 56 bit, e non 112 bit

DES Triplicato



- lunghezza blocco = 64 bit
- chiave (k_1,k_2,k_3) lunga 56 + 56 + 56 = 168 bit

DES Triplicato: *attacco meet in the middle*



Known Plaintext Attack
Input: x, y = $DES_{k_3}(DES_{k_2}(DES_{k_1}(x)))$
Costruisci tabella
for $k_3 \in \{0,1\}^{56}$
  do $z = DES^{-1}_{k_3}(y)$
    if per qualche k_1,k_2, (k_1k_2, z) è nella tabella
      then return la chiave è (k_1,k_2,k_3)

chiave	testo cifrato
(k_1,k_2)	$DES_{k1}(DES_{k2}(x))$
…	…

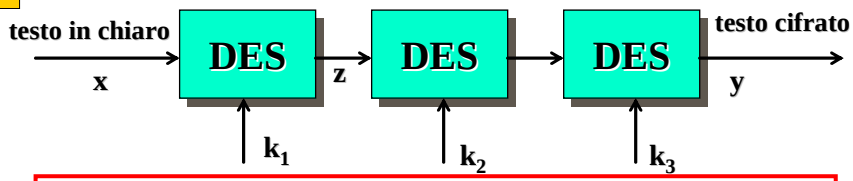
DES Triplicato: attacco *meet in the middle*

Known Plaintext Attack
Input: x, y = $DES_{k_3}(DES_{k_2}(DES_{k_1}(x)))$
Costruisci tabella
for $k_3 \in \{0,1\}^{56}$
  do $z = DES^{-1}_{k_3}(y)$
    if per qualche k_1,k_2, (k_1k_2, z) è nella tabella
      then return la chiave è (k_1,k_2,k_3)

chiave	testo cifrato
(k_1,k_2)	$DES_{k1}(DES_{k2}(x))$
…	…

Complessità spazio: 2^{112} righe nella tabella
Complessità tempo:
- 2^{112} cifrature per x (costruzione tabella)
- 2^{56} decifrature per y
- 2^{56} ricerche in tabella

DES Triplicato: attacco *meet in the middle*



Known Plaintext Attack
Input: x, y = $DES_{k_3}(DES_{k_2}(DES_{k_1}(x)))$
Costruisci tabella
for $k_3,k_2 \in \{0,1\}^{56} \times \{0,1\}^{56}$
  do $z = DES^{-1}_{k_2}(DES^{-1}_{k_3}(y))$
    if per qualche k_1, (k_1, z) è nella tabella
      then return la chiave è (k_1,k_2,k_3)

chiave	testo cifrato
k_1	$DES_{k1}(x)$
…	…

DES Triplicato: attacco *meet in the middle*

Known Plaintext Attack
Input: x, y = $DES_{k_3}(DES_{k_2}(DES_{k_1}(x)))$
Costruisci tabella
for $k_3,k_2 \in \{0,1\}^{56} \times \{0,1\}^{56}$
do $z = DES^{-1}_{k_2}(DES^{-1}_{k_3}(y))$
if per qualche k_1, (k_1, z) è nella tabella
then return la chiave è (k_1,k_2,k_3)

chiave	testo cifrato
k_1	$DES_{k1}(x)$
…	…

Complessità spazio: 2^{56} righe nella tabella

Complessità tempo:

- 2^{56} cifrature per x (costruzione tabella)
- 2^{112} decifrature per y
- 2^{112} ricerche in tabella

DES Triplicato: attacco *meet in the middle*

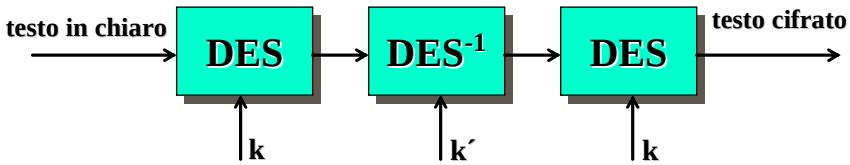
- Complessità *Known Plaintext Attack* ≈ 2^{112}
- Ricerca esaustiva su tutte le chiavi ≈ 2^{168}

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

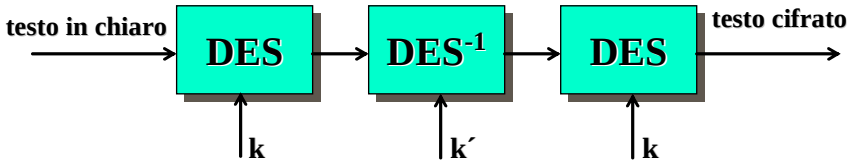
DES Triplo



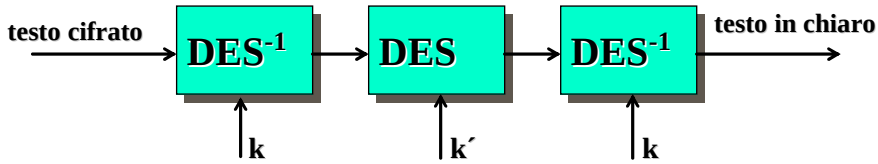
- lunghezza blocco = 64 bit
- chiave (k, k´) lunga 56+56 = 112 bit
- spesso chiamato $EDE_{k,k'}$ (acronimo per Encrypt Decrypt Encrypt)
- adottato negli standard X9.17 e ISO 8732

Decifratura DES Triplo

Cifratura

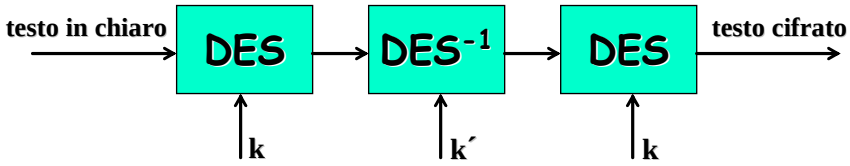


Decifratura



Compatibilità DES Triplo e DES

Se k = k´ il DES triplo



è equivalente al semplice DES

Prestazioni

Pentium II 400, FreeBSD, OpenSSL

	Key length	MB/s
DES - CBC	56	9
3DES - CBC	168	3

Celeron 850, Windows 2000, Crypto++

	Key length	MB/s
DES - CBC	56	12,871
3DES - CBC	168	4,748

Bibliografia

- Cryptography and Network Security by W. Stallings (2003)
  - cap. 6
- Tesina di Sicurezza su reti
  - Data Encryption Standard