Cifrari simmetrici - II

Prof. Francesco Bergadano

Dipartimento di Informatica
Università di Torino

Cifrari simmetrici ‘moderni’

- Basati sull’uso del calcolatore
- Combinano permutazioni e sostituzioni
- Prevedono numerose ‘fasi’ (round)

Cifrari simmetrici ‘moderni’

- Macchine a rotori
- Feistel cipher
- DES (Data Encryption Standard)
- Nuovi cifrari e AES (Advanced Encryption Standard)

Macchine a rotori

- Ognuno dei K rotori individua una sostituzione monoalfabetica
- Ogni rotore ‘girando’ porta ad una diversa sostituzione, ripetendosi dopo N volte
- Otteniamo così N^K sostituzioni monoalfabetiche
- Per ogni carattere del testo cambia la sostituzione monoalfabetica utilizzata

Cifrari simmetrici - II

Prof. Francesco Bergadano

Dipartimento di Informatica
Università di Torino

Cifrari simmetrici ‘moderni’

- Basati sull’uso del calcolatore
- Combinano permutazioni e sostituzioni
- Prevedono numerose ‘fasi’ (round)

Cifrari simmetrici ‘moderni’

- Macchine a rotori
- Feistel cipher
- DES (Data Encryption Standard)
- Nuovi cifrari e AES (Advanced Encryption Standard)

Macchine a rotori

- Ognuno dei K rotori individua una sostituzione monoalfabetica
- Ogni rotore ‘girando’ porta ad una diversa sostituzione, ripetendosi dopo N volte
- Otteniamo così N^K sostituzioni monoalfabetiche
- Per ogni carattere del testo cambia la sostituzione monoalfabetica utilizzata

Cifrari simmetrici - II

Prof. Francesco Bergadano

Dipartimento di Informatica
Università di Torino

Cifrari simmetrici ‘moderni’

- Basati sull’uso del calcolatore
- Combinano permutazioni e sostituzioni
- Prevedono numerose ‘fasi’ (round)

Cifrari simmetrici ‘moderni’

- Macchine a rotori
- Feistel cipher
- DES (Data Encryption Standard)
- Nuovi cifrari e AES (Advanced Encryption Standard)

Macchine a rotori

- Ognuno dei K rotori individua una sostituzione monoalfabetica
- Ogni rotore ‘girando’ porta ad una diversa sostituzione, ripetendosi dopo N volte
- Otteniamo così N^K sostituzioni monoalfabetiche
- Per ogni carattere del testo cambia la sostituzione monoalfabetica utilizzata

Cifrari simmetrici - II

Prof. Francesco Bergadano

Dipartimento di Informatica
Università di Torino

Cifrari simmetrici ‘moderni’

- Basati sull’uso del calcolatore
- Combinano permutazioni e sostituzioni
- Prevedono numerose ‘fasi’ (round)

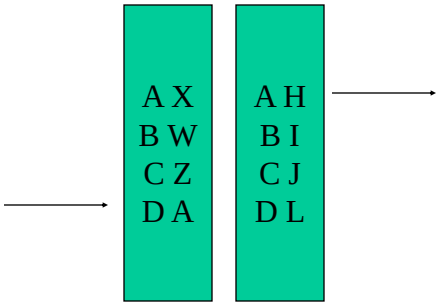
Cifrari simmetrici ‘moderni’

- Macchine a rotori
- Feistel cipher
- DES (Data Encryption Standard)
- Nuovi cifrari e AES (Advanced Encryption Standard)

Macchine a rotori

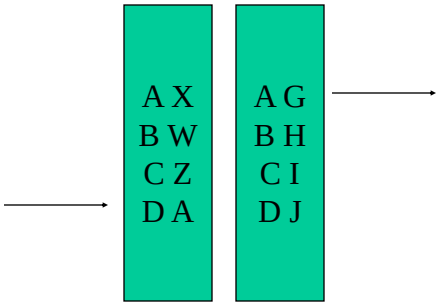
- Ognuno dei K rotori individua una sostituzione monoalfabetica
- Ogni rotore ‘girando’ porta ad una diversa sostituzione, ripetendosi dopo N volte
- Otteniamo così N^K sostituzioni monoalfabetiche
- Per ogni carattere del testo cambia la sostituzione monoalfabetica utilizzata

Macchine a rotori



D è cifrato con H

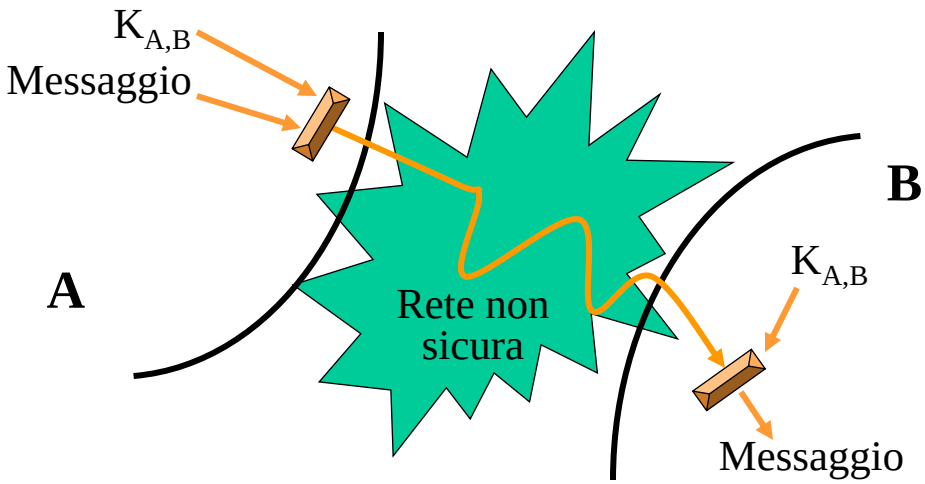
Macchine a rotori



D è cifrato con G

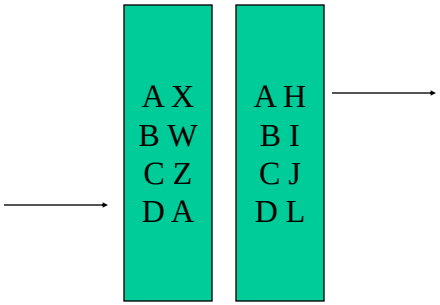
Data Encryption Standard

- Pubblicato nel 1977
- Cifrario simmetrico più usato fino al 2002
- Sostituito da AES
- Basato su concetto di “diffusione” e “confusione”



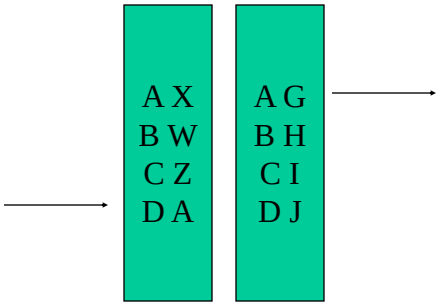
DES è un cifrario simmetrico

Macchine a rotori



D è cifrato con H

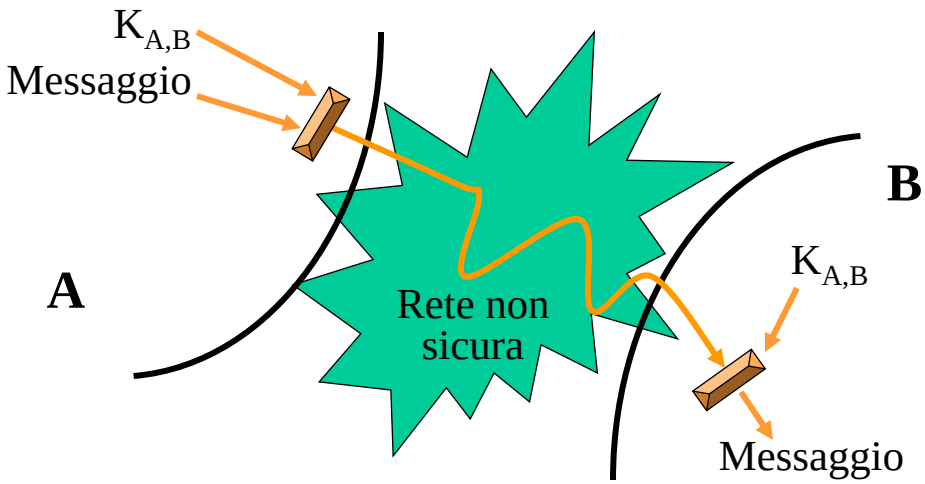
Macchine a rotori



D è cifrato con G

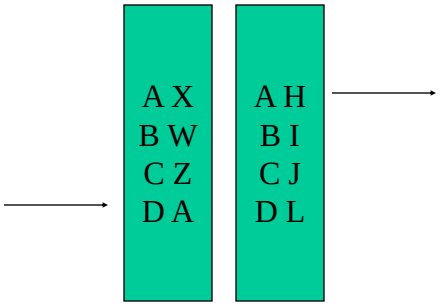
Data Encryption Standard

- Pubblicato nel 1977
- Cifrario simmetrico più usato fino al 2002
- Sostituito da AES
- Basato su concetto di “diffusione” e “confusione”



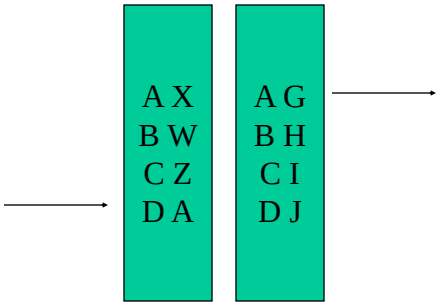
DES è un cifrario simmetrico

Macchine a rotori



D è cifrato con H

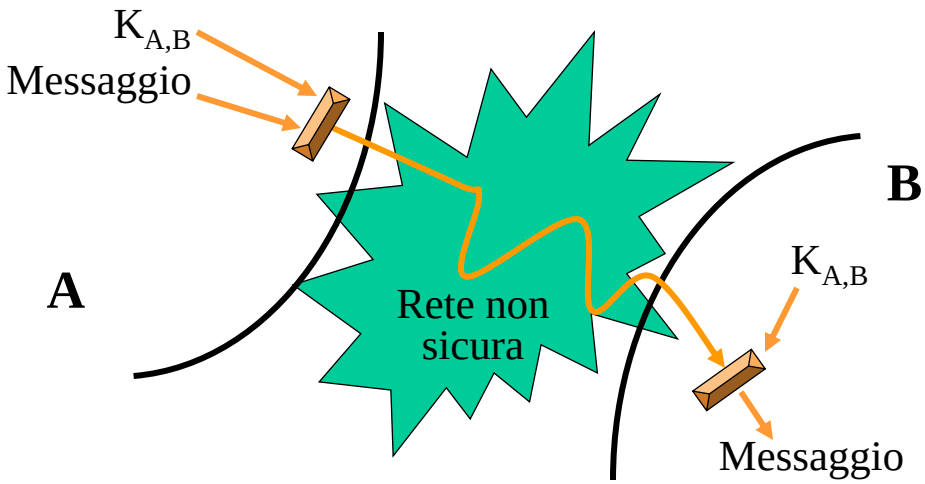
Macchine a rotori



D è cifrato con G

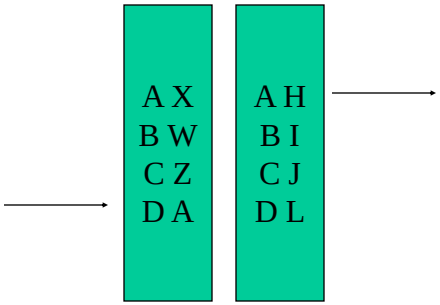
Data Encryption Standard

- Pubblicato nel 1977
- Cifrario simmetrico più usato fino al 2002
- Sostituito da AES
- Basato su concetto di “diffusione” e “confusione”



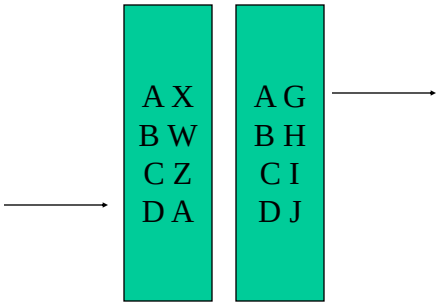
DES è un cifrario simmetrico

Macchine a rotori



D è cifrato con H

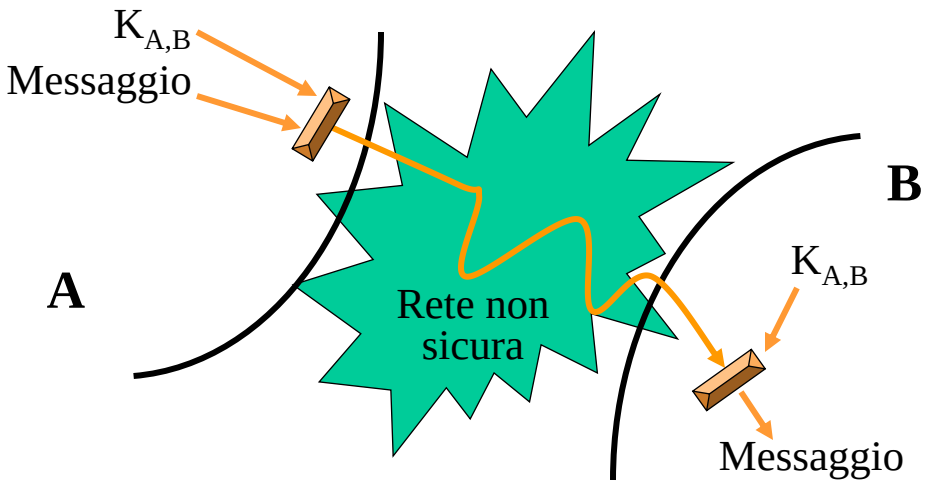
Macchine a rotori



D è cifrato con G

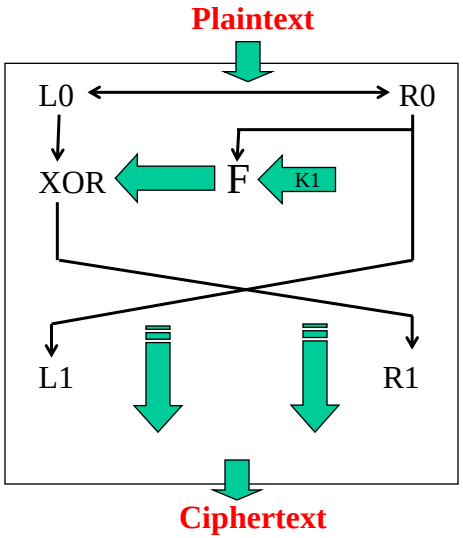
Data Encryption Standard

- Pubblicato nel 1977
- Cifrario simmetrico più usato fino al 2002
- Sostituito da AES
- Basato su concetto di “diffusione” e “confusione”

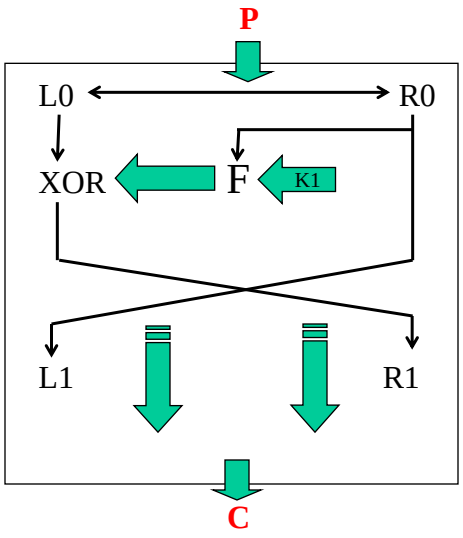


DES è un cifrario simmetrico

Feistel Cipher



Feistel Cipher - esercizio



C = E(P)
P = D(C)

Definire E, D

Dimostrare che
P = D(E(P))

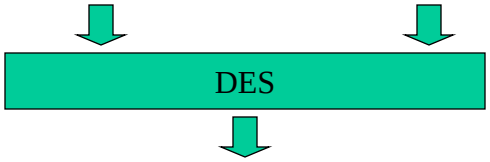
Caratteristiche di DES

- Chiavi di 56 bit
- 16 passi (‘rounds’)
- Efficiente
- Unici attacchi noti di tipo ‘forza bruta’

Schema Generale del DES

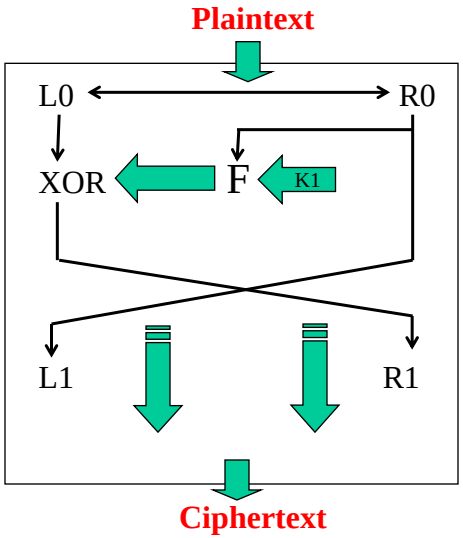
Testo in chiaro di 64 bit (**Plaintext** o Cleartext)

Chiave DES di 56 bit (solitamente estesa a 64 bit con bit di parità)

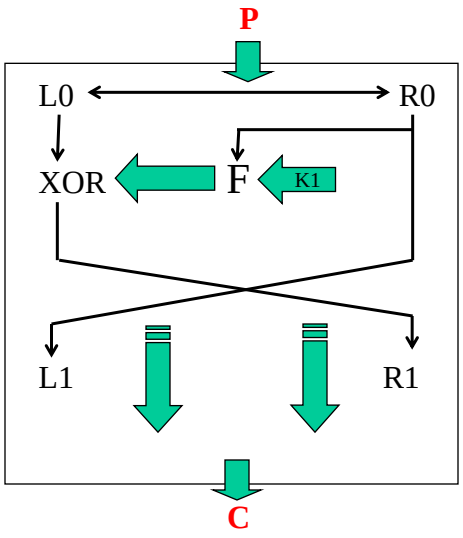


Testo cifrato di 64 bit (**Ciphertext**)

Feistel Cipher



Feistel Cipher - esercizio



C = E(P)
P = D(C)

Definire E, D

Dimostrare che
P = D(E(P))

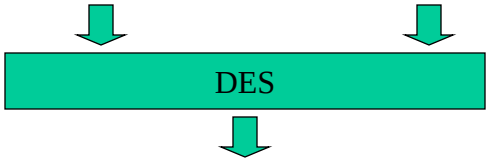
Caratteristiche di DES

- Chiavi di 56 bit
- 16 passi (‘rounds’)
- Efficiente
- Unici attacchi noti di tipo ‘forza bruta’

Schema Generale del DES

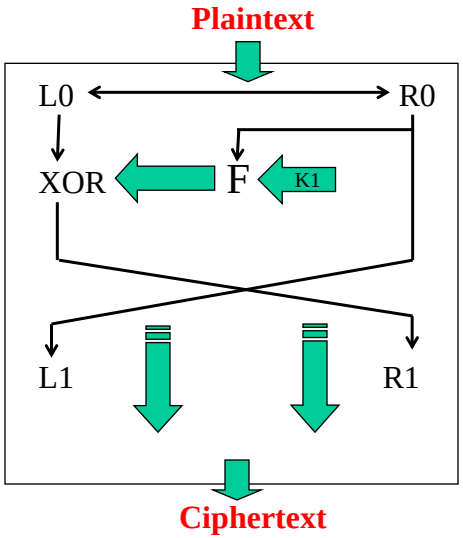
Testo in chiaro di 64 bit (**Plaintext** o Cleartext)

Chiave DES di 56 bit (solitamente estesa a 64 bit con bit di parità)

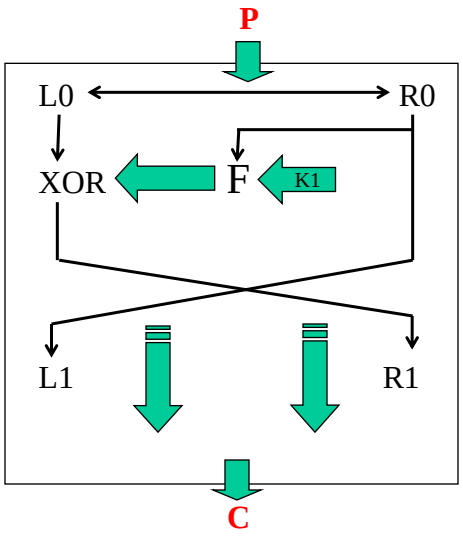


Testo cifrato di 64 bit (**Ciphertext**)

Feistel Cipher



Feistel Cipher - esercizio



C = E(P)
P = D(C)

Definire E, D

Dimostrare che
P = D(E(P))

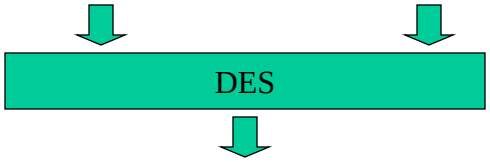
Caratteristiche di DES

- Chiavi di 56 bit
- 16 passi (‘rounds’)
- Efficiente
- Unici attacchi noti di tipo ‘forza bruta’

Schema Generale del DES

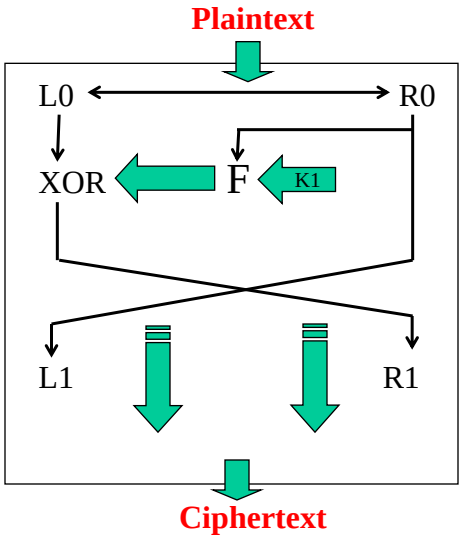
Testo in chiaro di 64 bit (**Plaintext** o Cleartext)

Chiave DES di 56 bit (solitamente estesa a 64 bit con bit di parità)

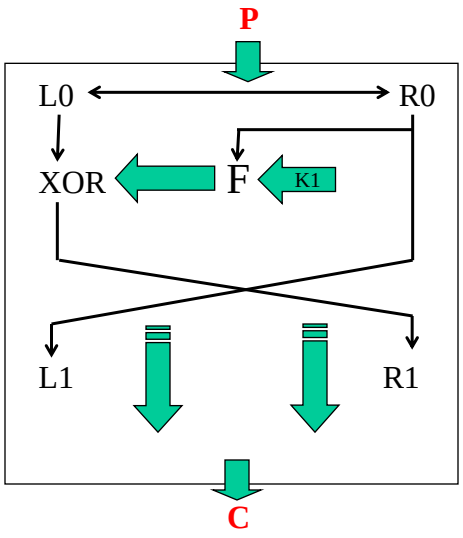


Testo cifrato di 64 bit (**Ciphertext**)

Feistel Cipher



Feistel Cipher - esercizio



C = E(P)
P = D(C)

Definire E, D

Dimostrare che
P = D(E(P))

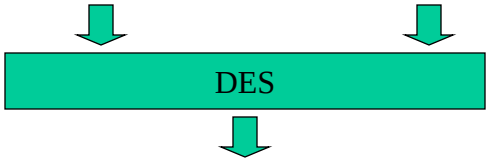
Caratteristiche di DES

- Chiavi di 56 bit
- 16 passi (‘rounds’)
- Efficiente
- Unici attacchi noti di tipo ‘forza bruta’

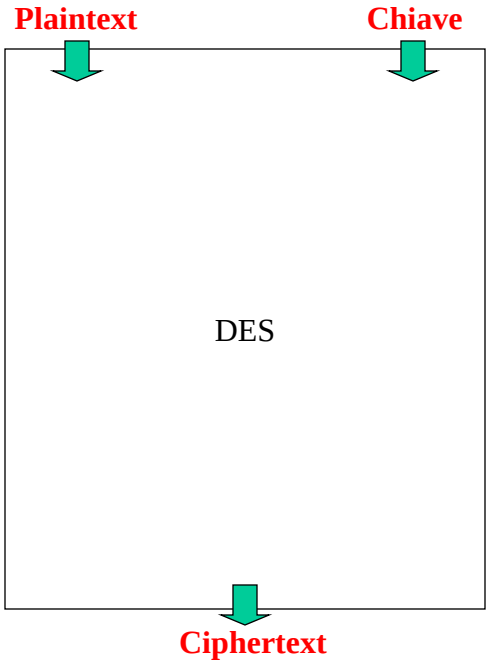
Schema Generale del DES

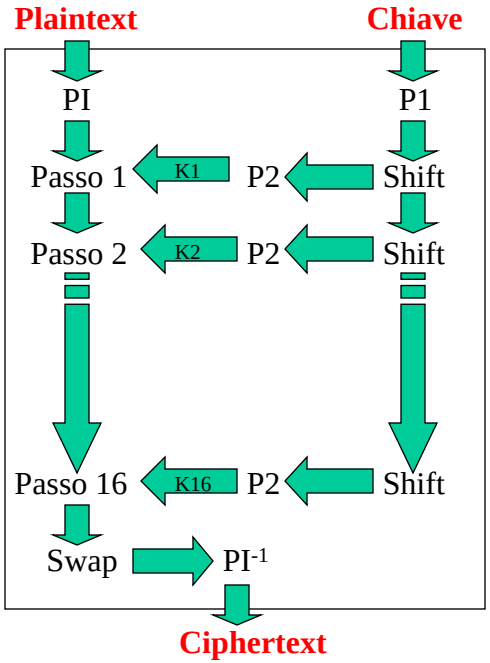
Testo in chiaro di 64 bit (**Plaintext** o Cleartext)

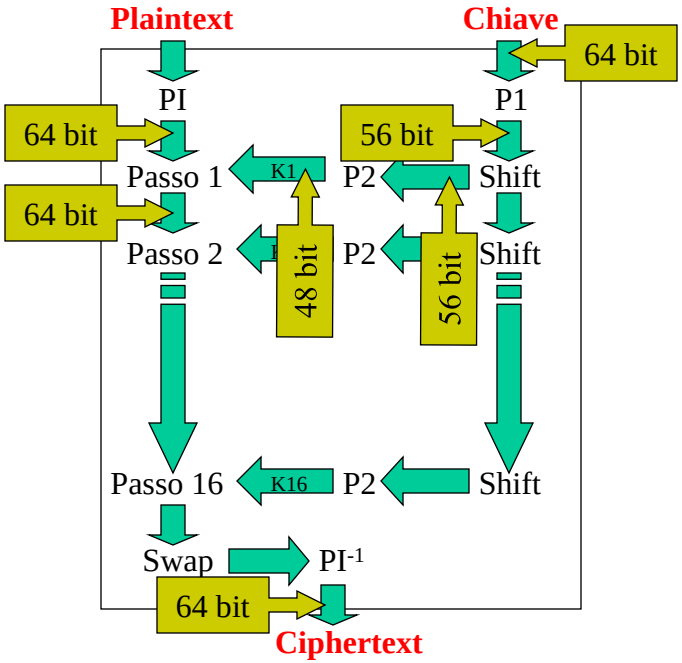
Chiave DES di 56 bit (solitamente estesa a 64 bit con bit di parità)



Testo cifrato di 64 bit (**Ciphertext**)



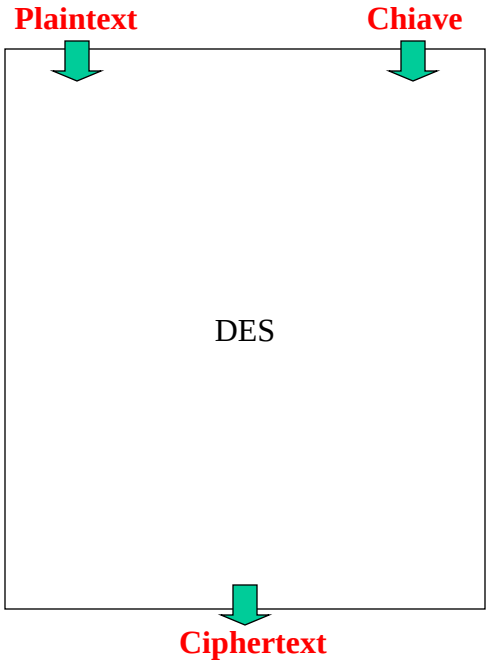


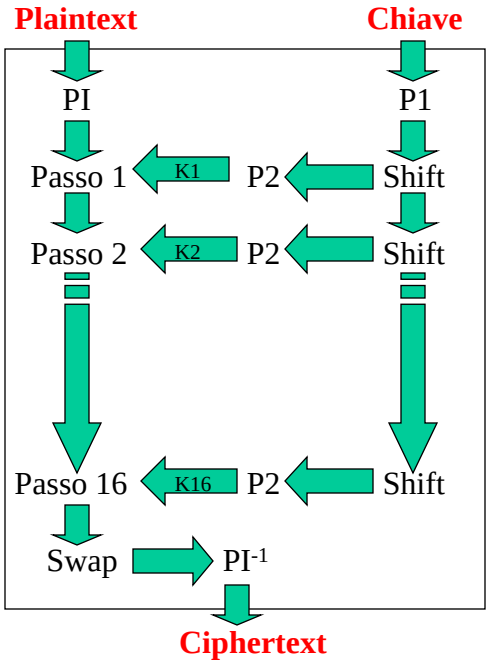


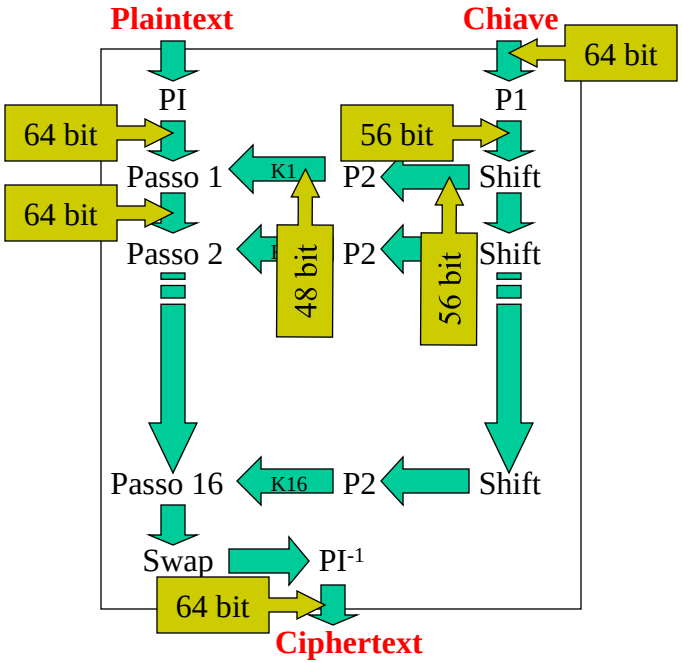
Data Encryption Standard

<K1, K2, …, K16> = key schedule

(si può calcolare a partire dalla chiave simmetrica originaria K)



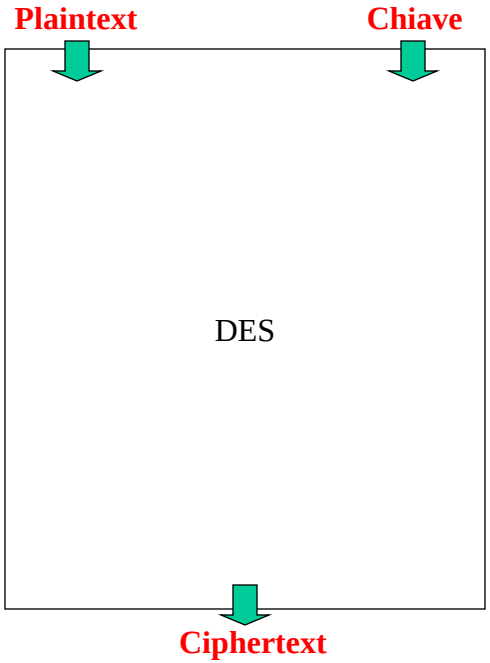


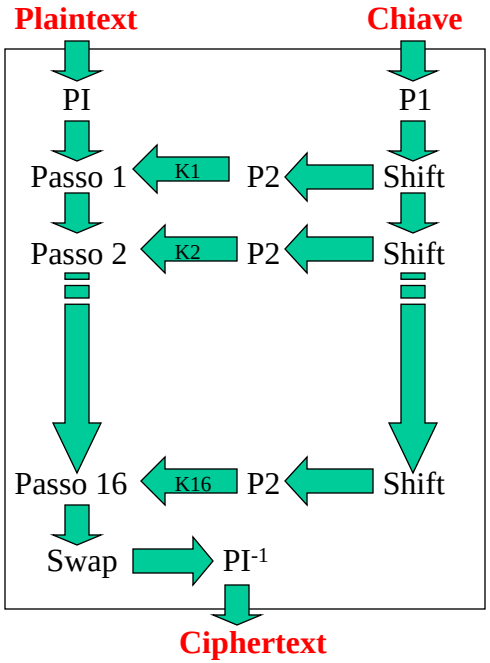


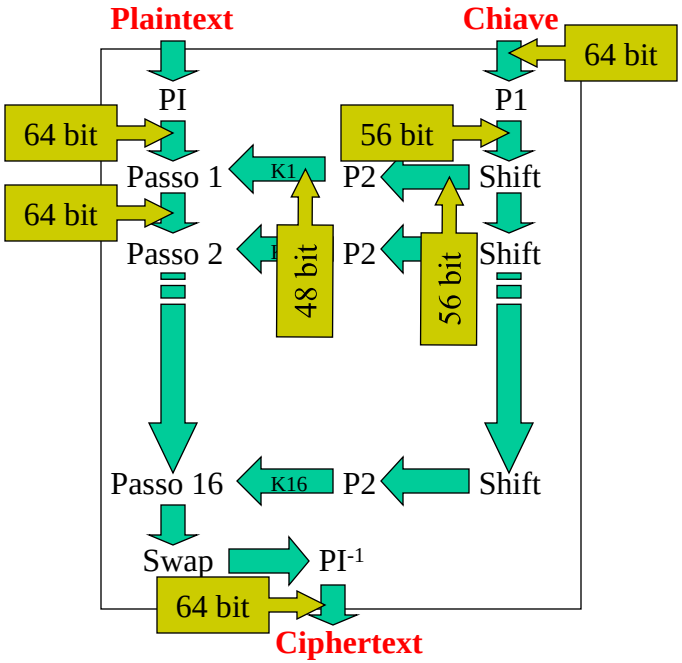
Data Encryption Standard

<K1, K2, …, K16> = key schedule

(si può calcolare a partire dalla chiave simmetrica originaria K)



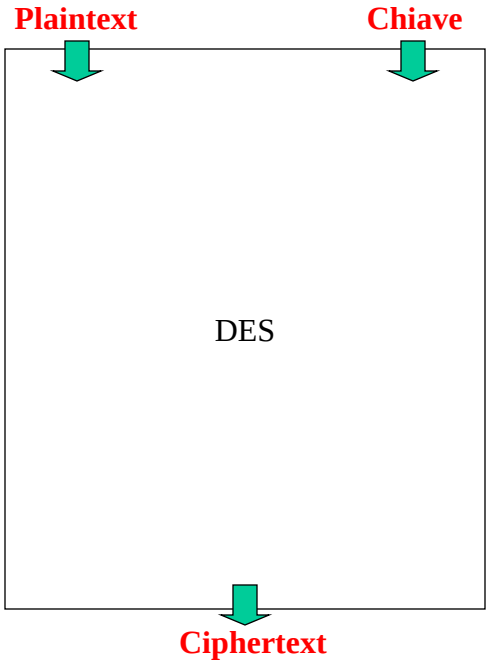


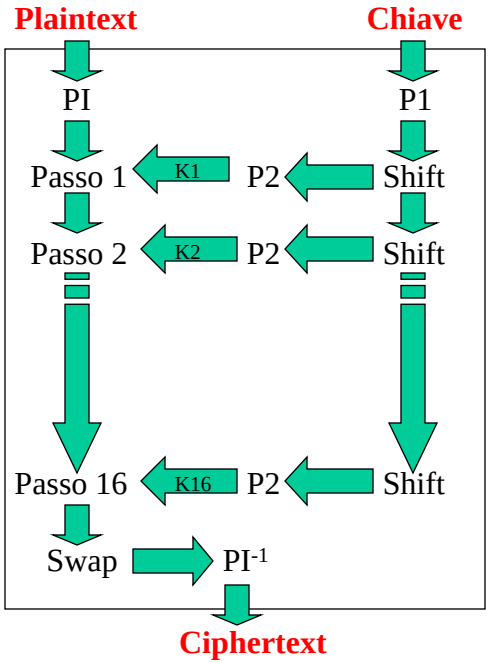


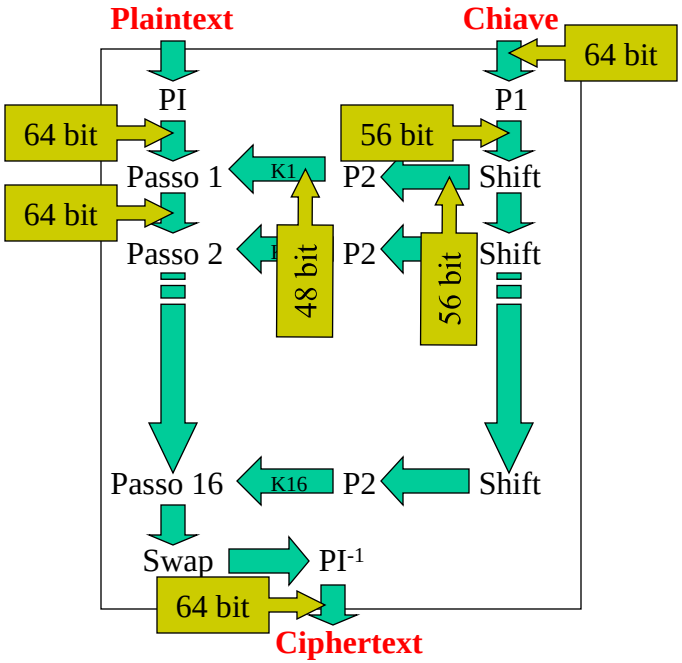
Data Encryption Standard

<K1, K2, …, K16> = key schedule

(si può calcolare a partire dalla chiave simmetrica originaria K)



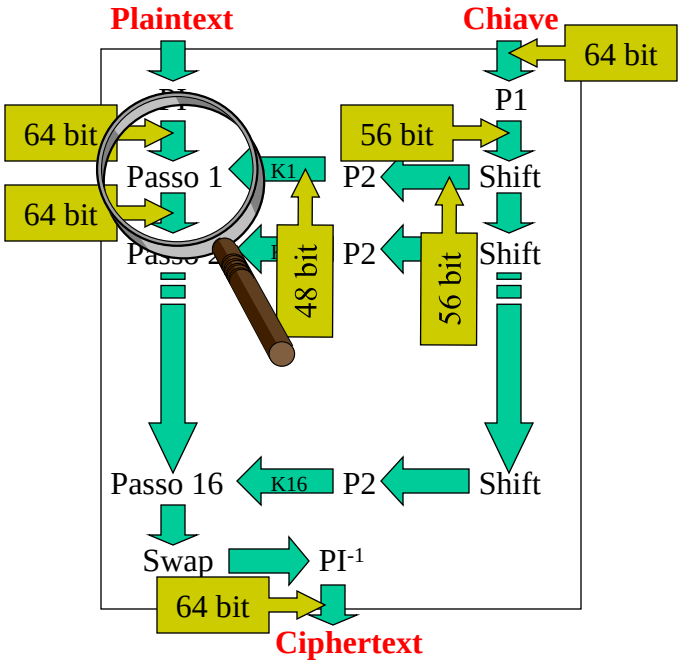


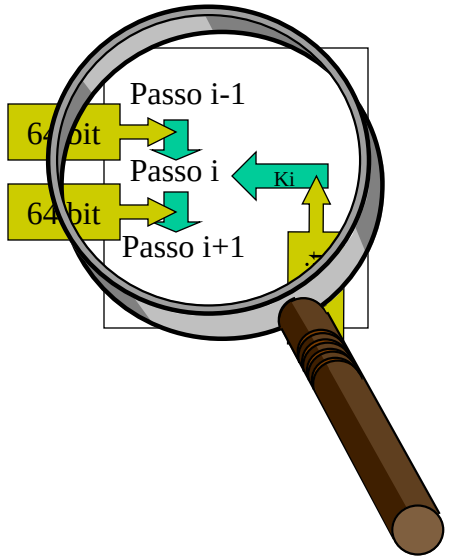


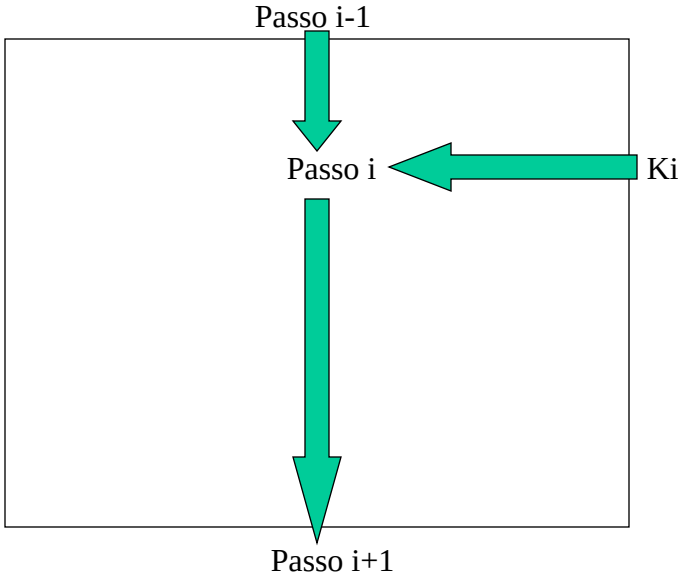
Data Encryption Standard

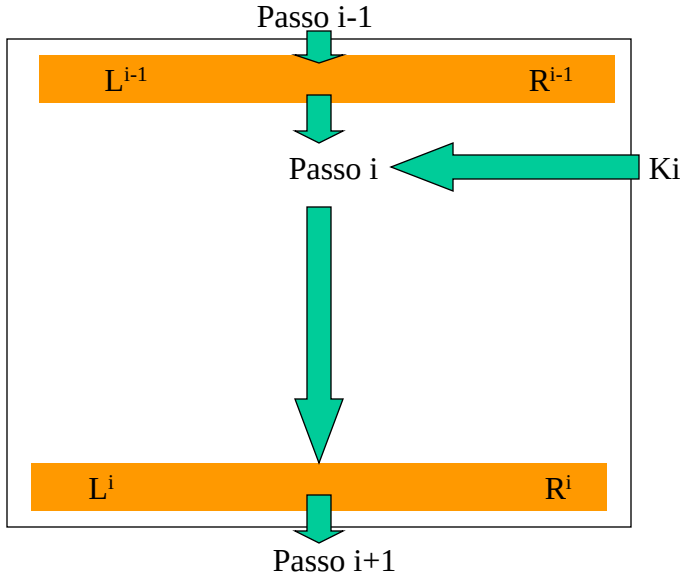
<K1, K2, …, K16> = key schedule

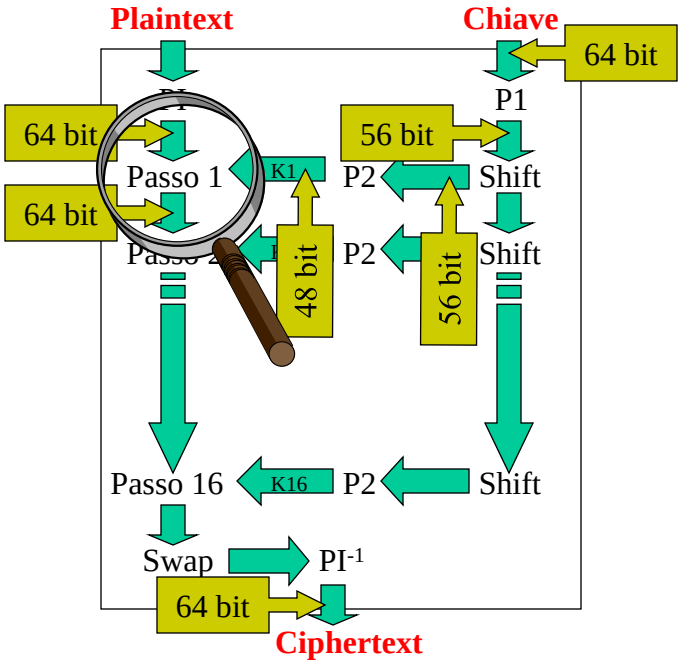
(si può calcolare a partire dalla chiave simmetrica originaria K)

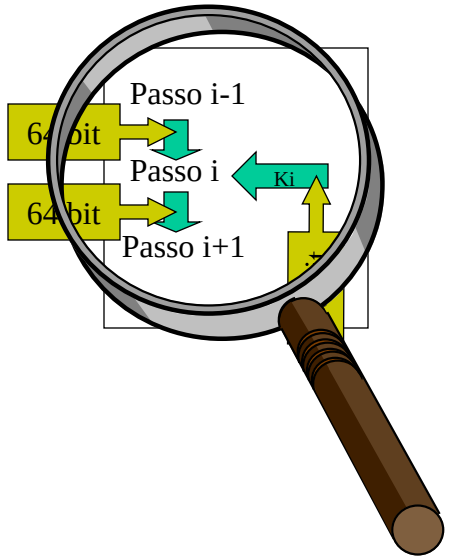

Plaintext
Chiave
64 bit
P1
64 bit
56 bit
Passo 1
K1
P2
Shift
64 bit
48 bit
P2
56 bit
Shift
Passo 16
K16
P2
Shift
Swap
PI-1
64 bit
Ciphertext

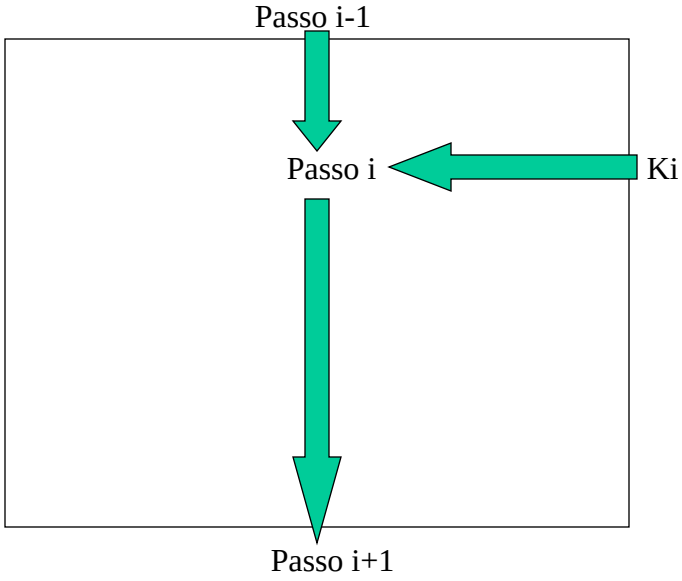

Passo i-1
Passo i
Ki
Passo i+1

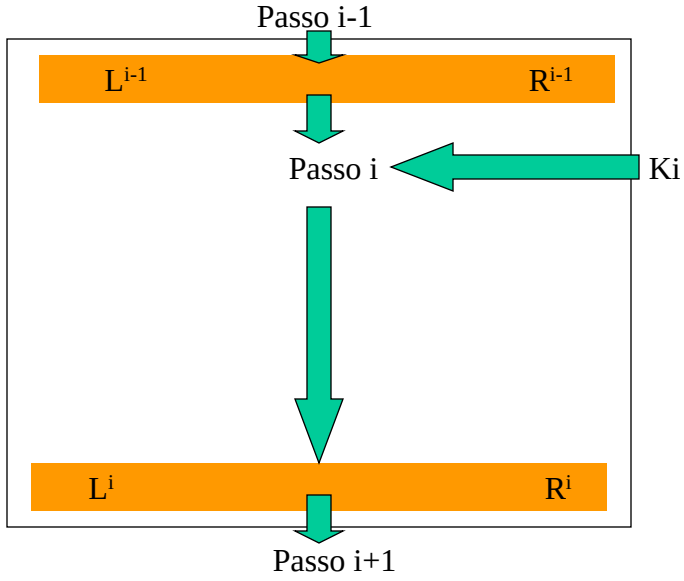

Passo i-1
Passo i
Ki
Passo i+1

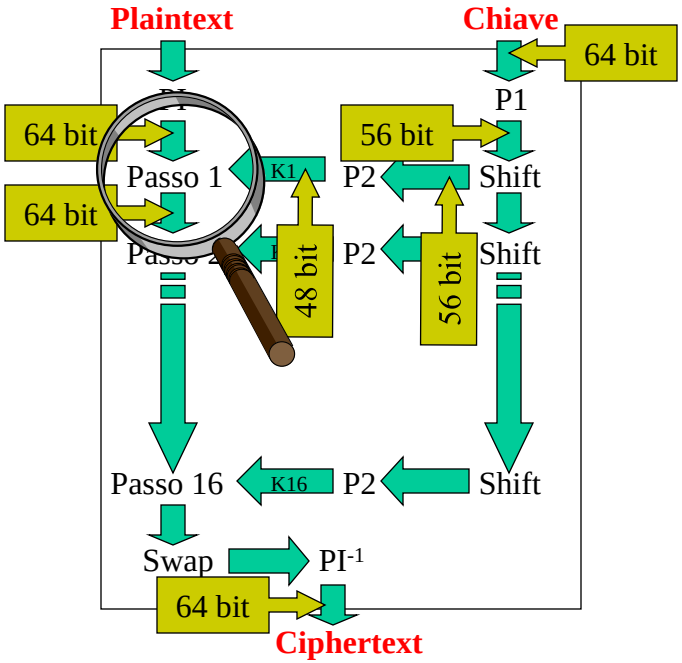

Passo i-1
Li-1
Ri-1
Passo i
Ki
Li
Ri
Passo i+1

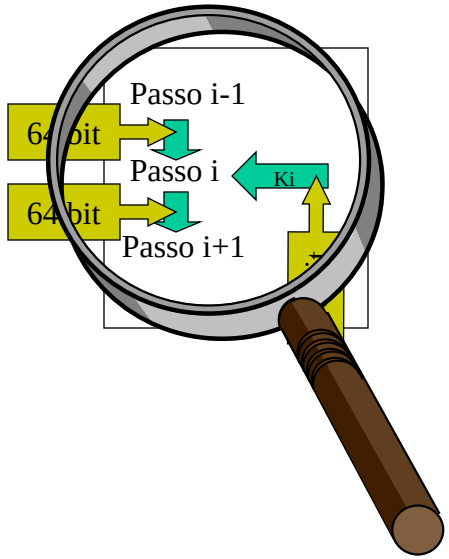

Plaintext
Chiave
64 bit
P1
64 bit
56 bit
Passo 1
K1
P2
Shift
64 bit
48 bit
P2
56 bit
Shift
Passo 16
K16
P2
Shift
Swap
PI-1
64 bit
Ciphertext

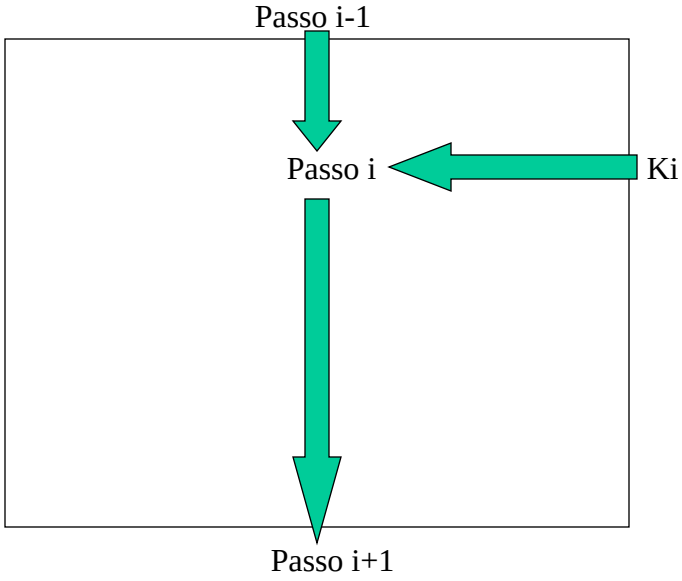

Passo i-1
Passo i
Ki
Passo i+1

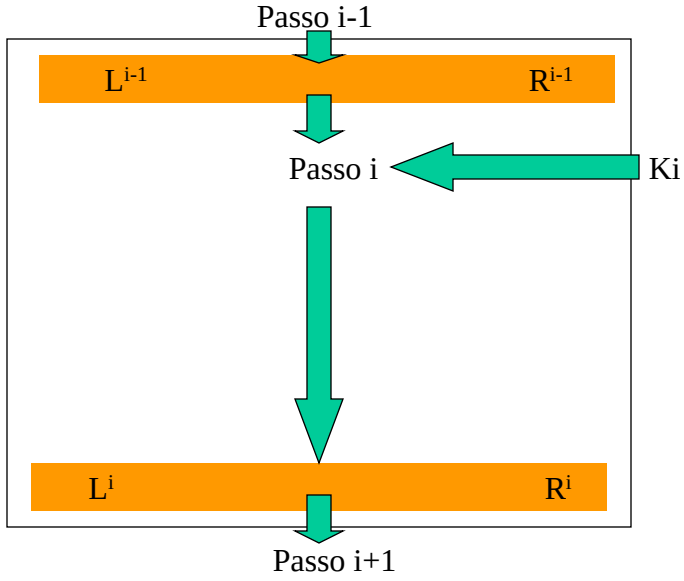

Passo i-1
Passo i
Ki
Passo i+1

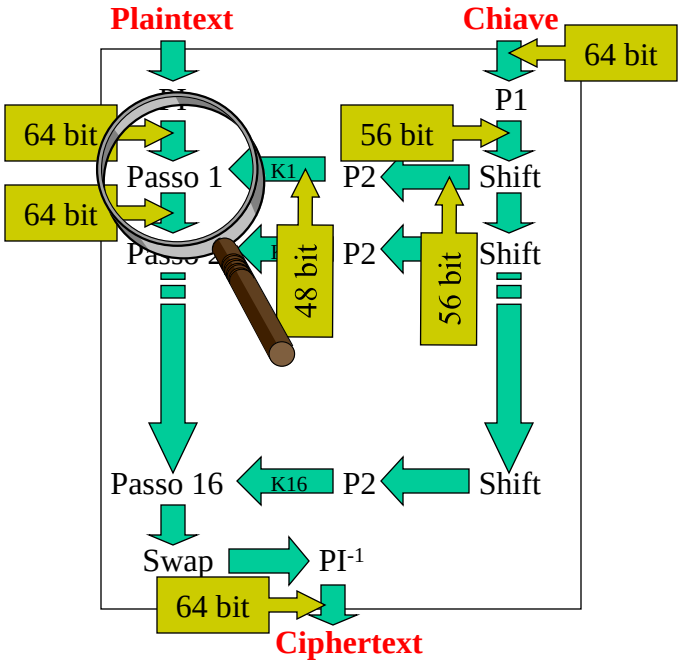

Passo i-1
Li-1
Ri-1
Passo i
Ki
Li
Ri
Passo i+1

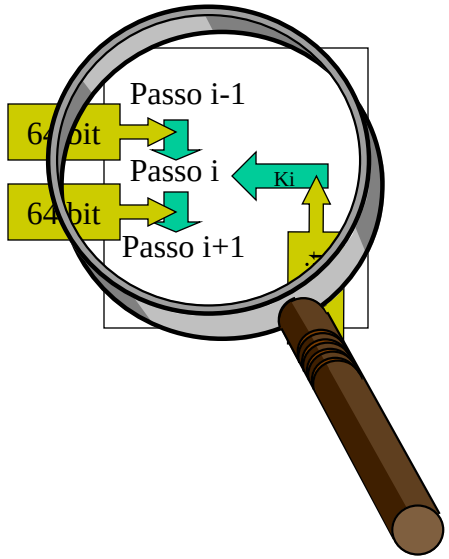

Plaintext
Chiave
64 bit
P1
64 bit
56 bit
Passo 1
K1
P2
Shift
64 bit
48 bit
P2
56 bit
Shift
Passo 16
K16
P2
Shift
Swap
PI-1
64 bit
Ciphertext

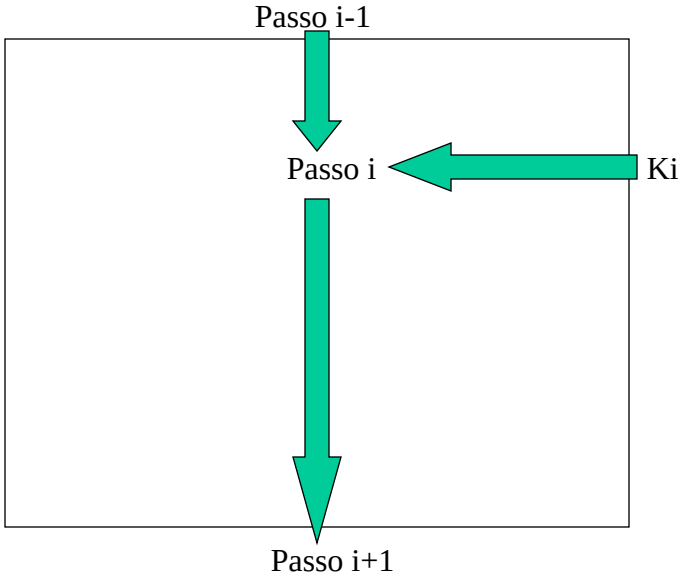

Passo i-1
Passo i
Ki
Passo i+1

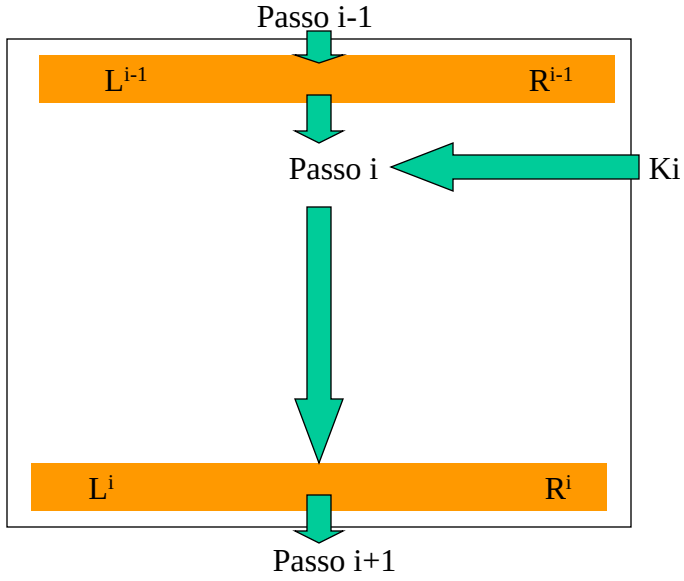

Passo i-1
Passo i
Ki
Passo i+1

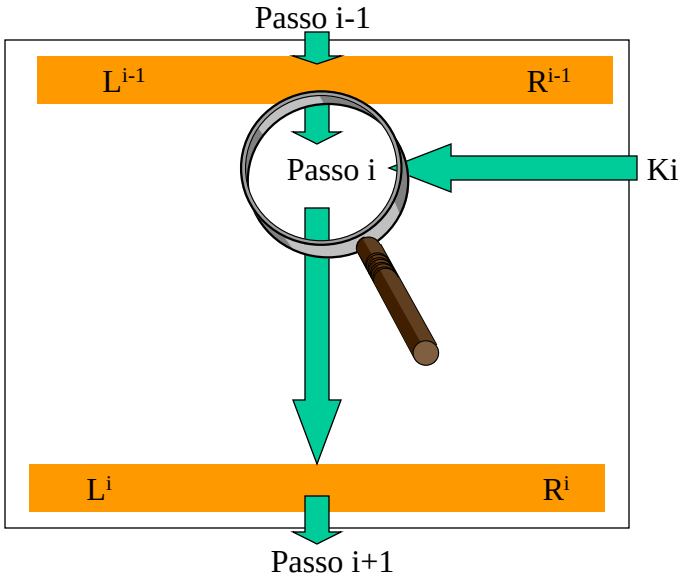

Passo i-1
Li-1
Ri-1
Passo i
Ki
Li
Ri
Passo i+1

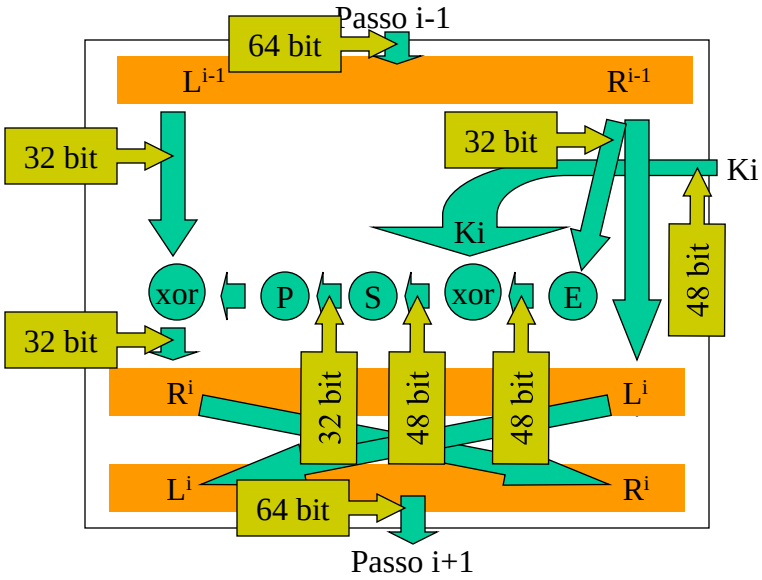

Plaintext
Chiave
64 bit
P1
64 bit
56 bit
Passo 1
K1
P2
Shift
64 bit
48 bit
P2
56 bit
Shift
Passo 16
K16
P2
Shift
Swap
PI-1
64 bit
Ciphertext

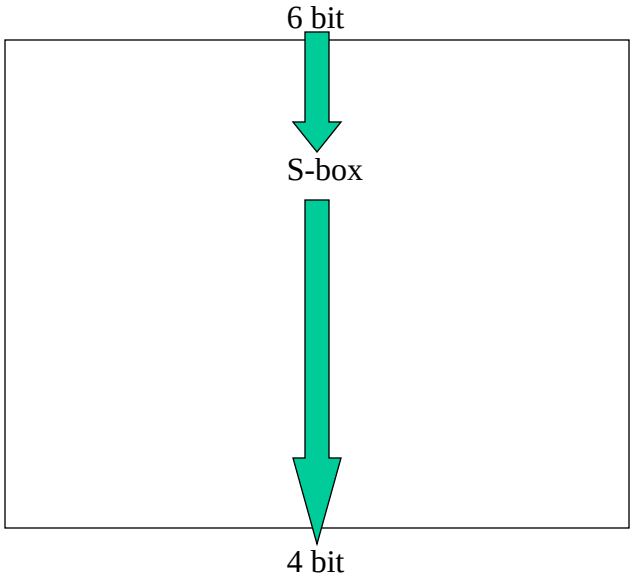

Passo i-1
Passo i
Ki
Passo i+1

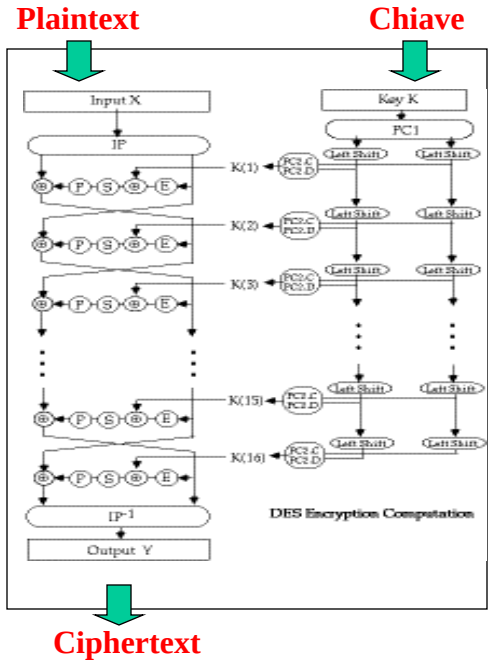

Passo i-1
Passo i
Ki
Passo i+1

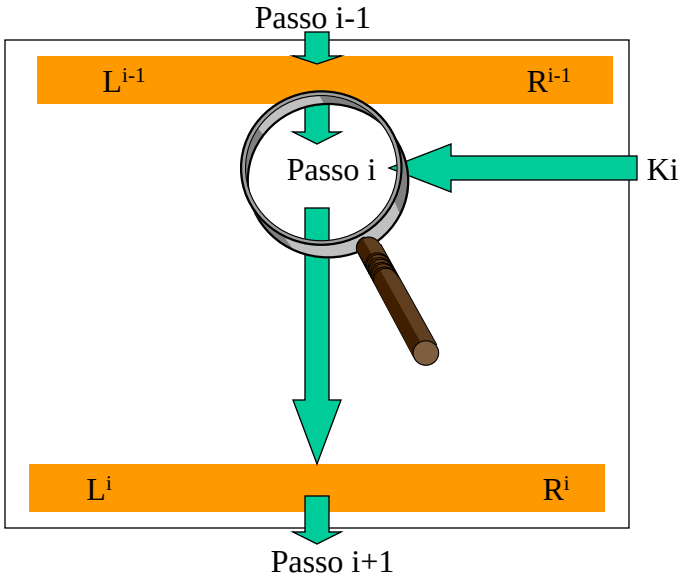

Passo i-1
Li-1
Ri-1
Passo i
Ki
Li
Ri
Passo i+1

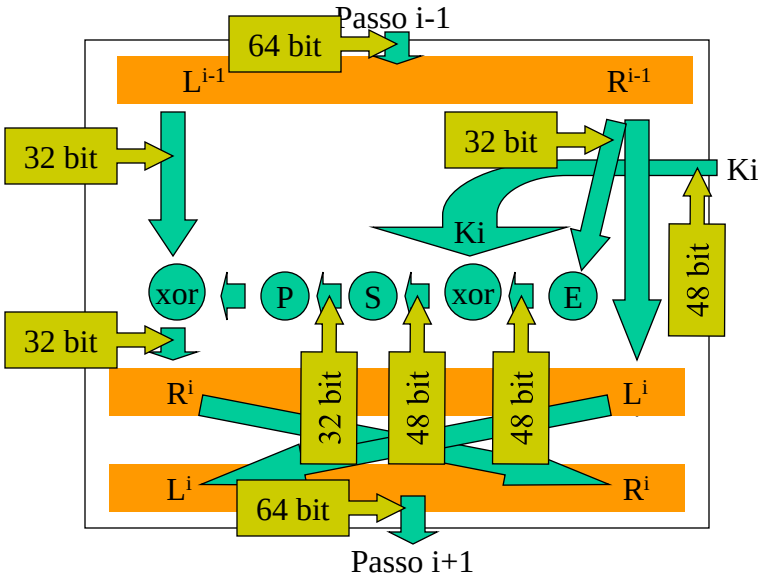

Passo i-1
L i-1
R i-1
Passo i
Ki
L i
R i
Passo i+1

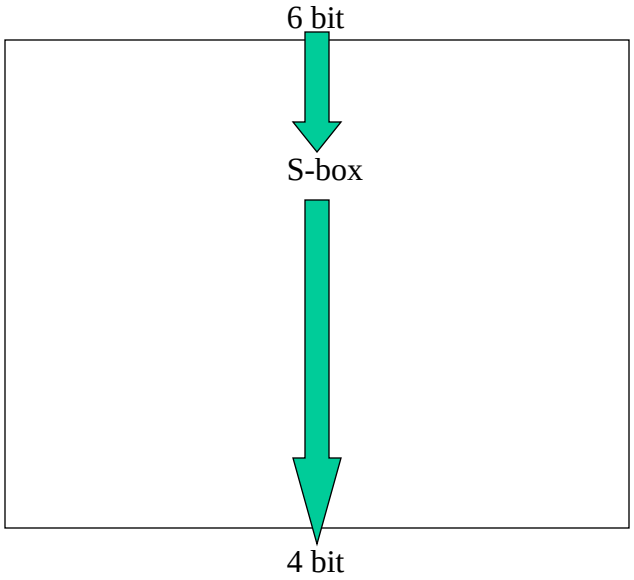

Passo i-1
64 bit
L i-1
R i-1
32 bit
32 bit
Ki
Ki
xor
P
S
xor
E
48 bit
32 bit
R i
L i
32 bit
48 bit
48 bit
L i
R i
64 bit
Passo i+1

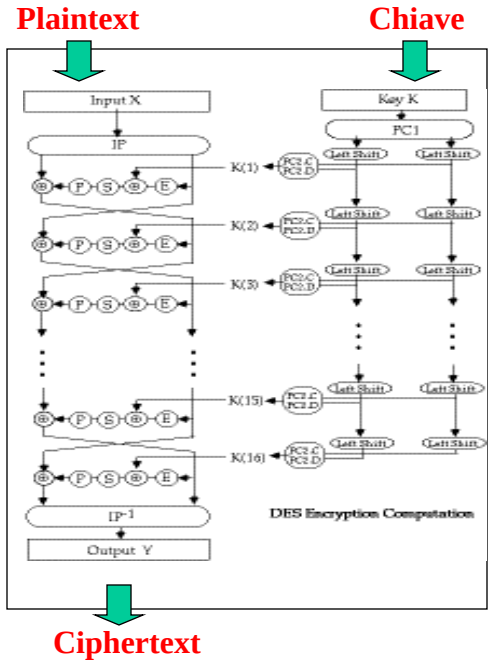

6 bit
S-box
4 bit

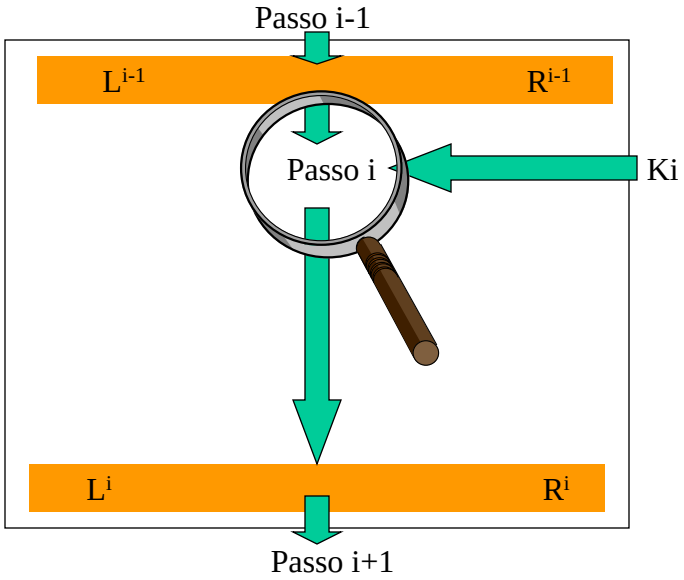

Plaintext
Chiave
Input X
Key K
PC1
IP
K(1)
K(2)
K(3)
K(15)
K(16)
IP-1
Output Y
DES Encryption Computation
Ciphertext

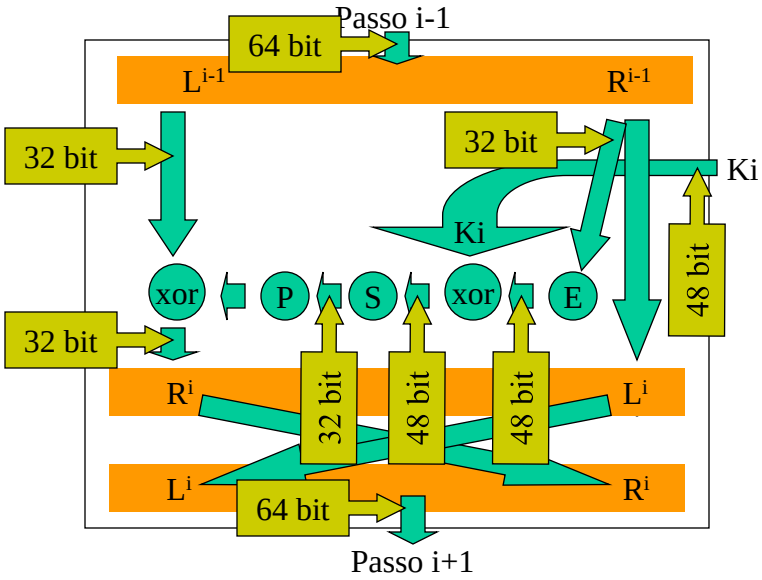

Passo i-1
L i-1
R i-1
Passo i
Ki
L i
R i
Passo i+1

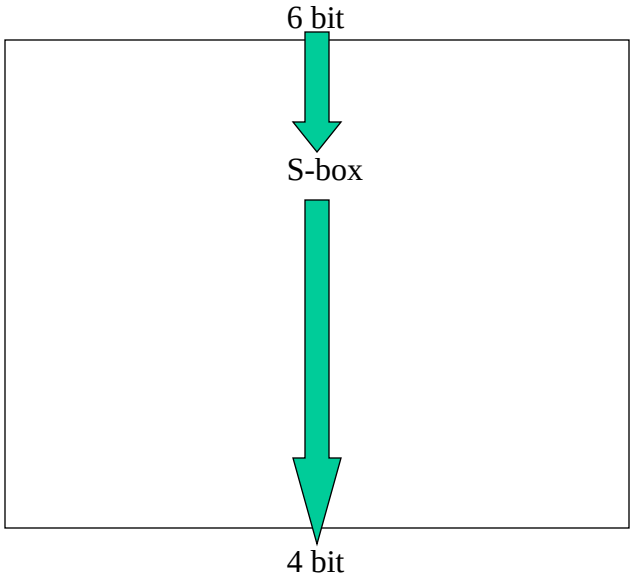

Passo i-1
64 bit
L i-1
R i-1
32 bit
32 bit
Ki
Ki
xor
P
S
xor
E
48 bit
32 bit
R i
L i
32 bit
48 bit
48 bit
L i
R i
64 bit
Passo i+1

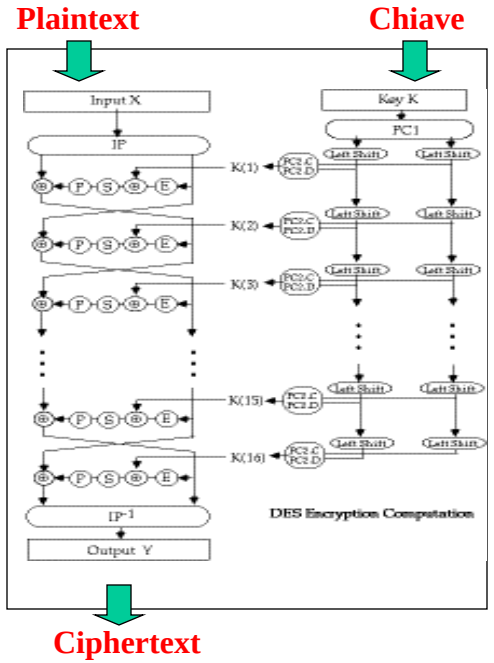

6 bit
S-box
4 bit

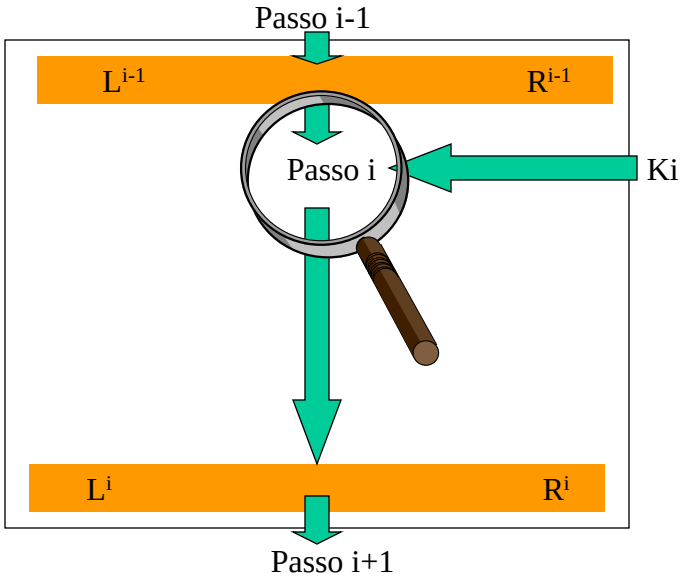

Plaintext
Chiave
Input X
Key K
PC1
IP
K(1)
K(2)
K(3)
K(15)
K(16)
IP-1
Output Y
DES Encryption Computation
Ciphertext

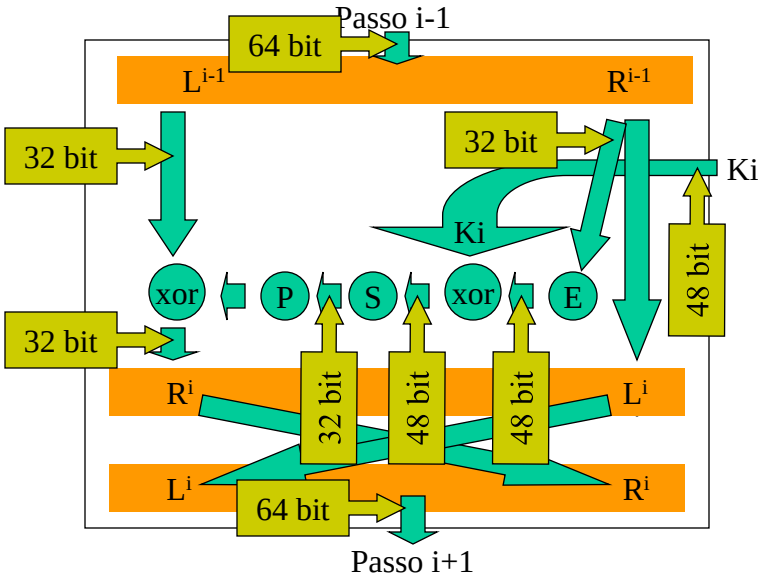

Passo i-1
L i-1
R i-1
Passo i
Ki
L i
R i
Passo i+1

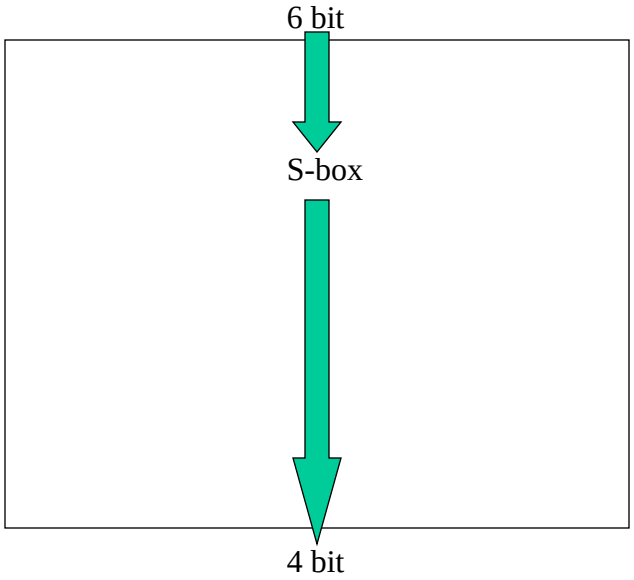

Passo i-1
64 bit
L i-1
R i-1
32 bit
32 bit
Ki
Ki
xor
P
S
xor
E
48 bit
32 bit
R i
L i
32 bit
48 bit
48 bit
L i
R i
64 bit
Passo i+1

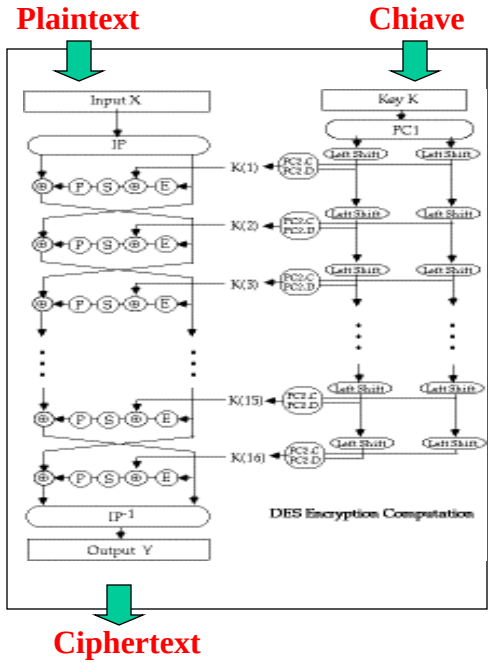

6 bit
S-box
4 bit


Plaintext
Chiave
Input X
Key K
PC1
IP
K(1)
K(2)
K(3)
K(15)
K(16)
IP-1
Output Y
DES Encryption Computation
Ciphertext


Passo i-1
L i-1
R i-1
Passo i
Ki
L i
R i
Passo i+1


Passo i-1
64 bit
L i-1
R i-1
32 bit
32 bit
Ki
Ki
xor
P
S
xor
E
48 bit
32 bit
R i
L i
32 bit
48 bit
48 bit
L i
R i
64 bit
Passo i+1


6 bit
S-box
4 bit


Plaintext
Chiave
Input X
Key K
PC1
IP
K(1)
K(2)
K(3)
K(15)
K(16)
IP-1
Output Y
DES Encryption Computation
Ciphertext

«effetto valanga»

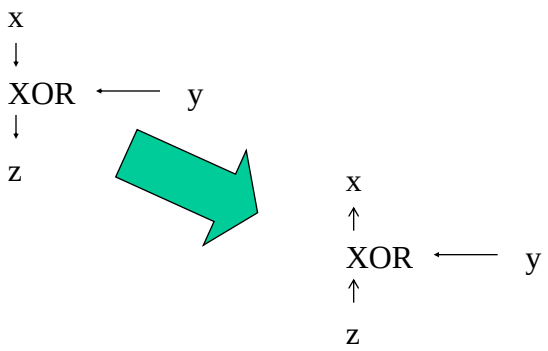
1 bit invertito nell'input provoca
un effetto su «molti» bit a valle

… in qualsiasi cifrario

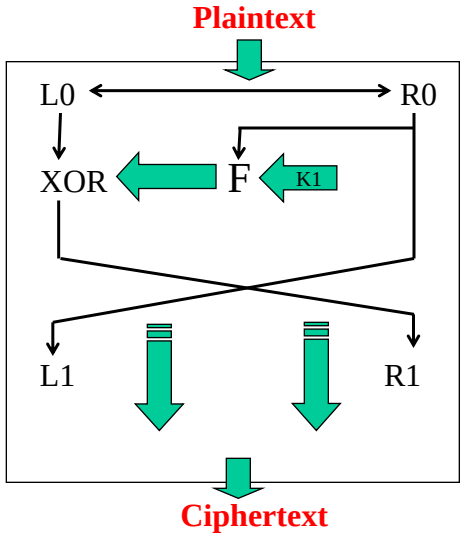
Sia E = encryption
e D = decryption

D(E(M)) = M

x XOR y = z
x XOR y XOR y = z XOR y
x XOR 0 = z XOR y
x = z XOR y



Feistel Cipher



Sia E = encryption

E(L0,R0) = L1,R1 =
R0, (L0 XOR F(k1,R0))

«effetto valanga»

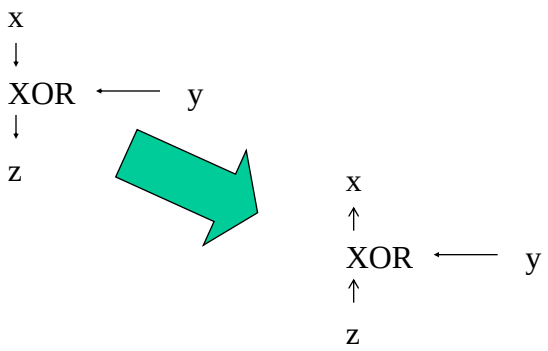
1 bit invertito nell'input provoca
un effetto su «molti» bit a valle

… in qualsiasi cifrario

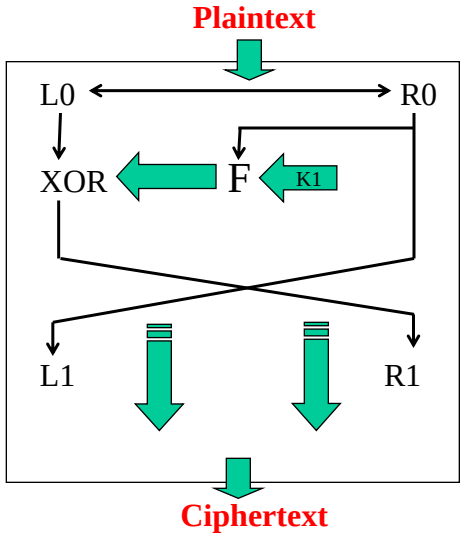
Sia E = encryption
e D = decryption

D(E(M)) = M

x XOR y = z
x XOR y XOR y = z XOR y
x XOR 0 = z XOR y
x = z XOR y



Feistel Cipher



Sia E = encryption

E(L0,R0) = L1,R1 =
R0, (L0 XOR F(k1,R0))

«effetto valanga»

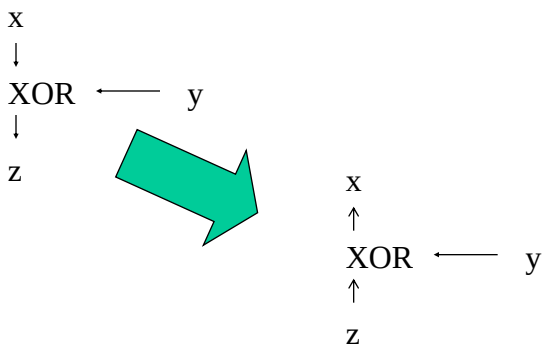
1 bit invertito nell'input provoca
un effetto su «molti» bit a valle

… in qualsiasi cifrario

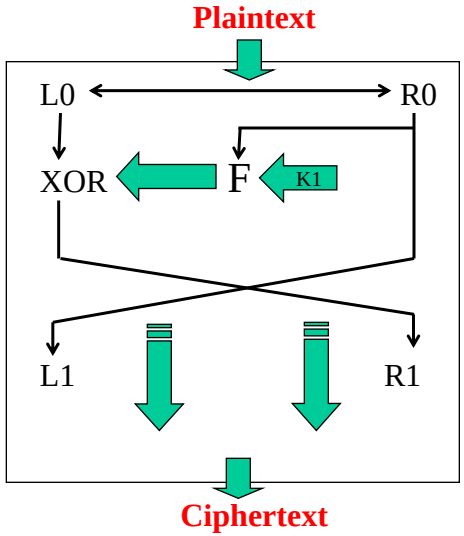
Sia E = encryption
e D = decryption

D(E(M)) = M

x XOR y = z
x XOR y XOR y = z XOR y
x XOR 0 = z XOR y
x = z XOR y



Feistel Cipher



Sia E = encryption

E(L0,R0) = L1,R1 =
R0, (L0 XOR F(k1,R0))

«effetto valanga»

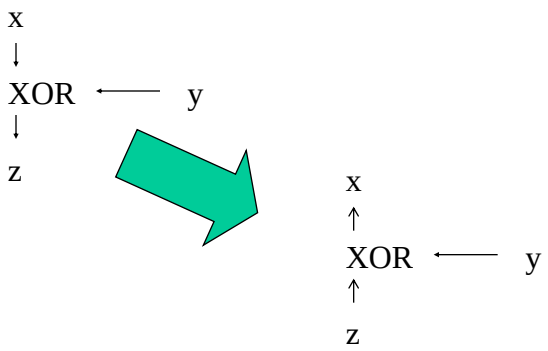
1 bit invertito nell'input provoca
un effetto su «molti» bit a valle

… in qualsiasi cifrario

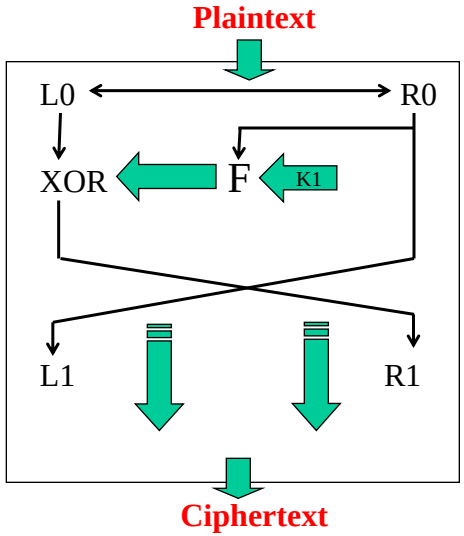
Sia E = encryption
e D = decryption

D(E(M)) = M

x XOR y = z
x XOR y XOR y = z XOR y
x XOR 0 = z XOR y
x = z XOR y



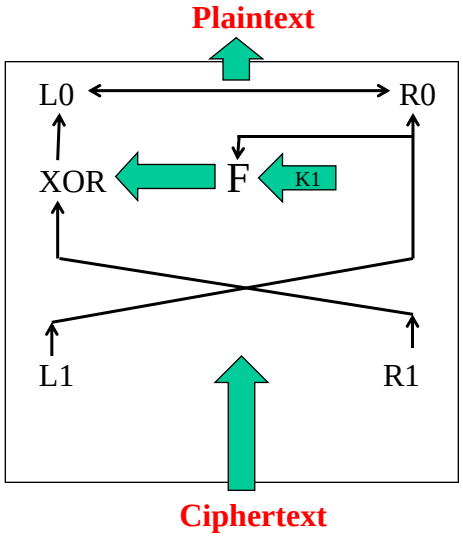
Feistel Cipher



Sia E = encryption

E(L0,R0) = L1,R1 =
R0, (L0 XOR F(k1,R0))

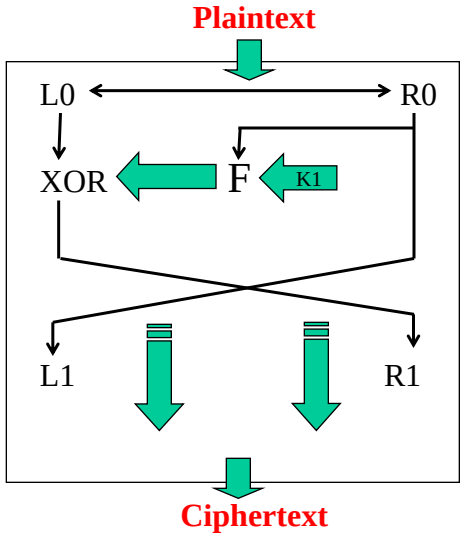
Feistel Cipher



Sia D = decryption

D(L1,R1) = L0,R0 =
(R1 XOR F(k1,L1)), L1

Feistel Cipher



Il sistema funziona:

D(E(L0,R0))=
= D(R0, (L0 XOR F(k1,R0))) =
= (L0 XOR F(k1,R0))
XOR F(k1,L1), R0 =
= L0 XOR F(k1,R0)
XOR F(k1,R0), R0 =
= L0, R0

DES Challenge

RSA security, nel 1997, offre **10.000 $** a chi avesse decifrato un testo ottenuto cifrando con DES una frase segreta («strong crypto makes the world a better place»).

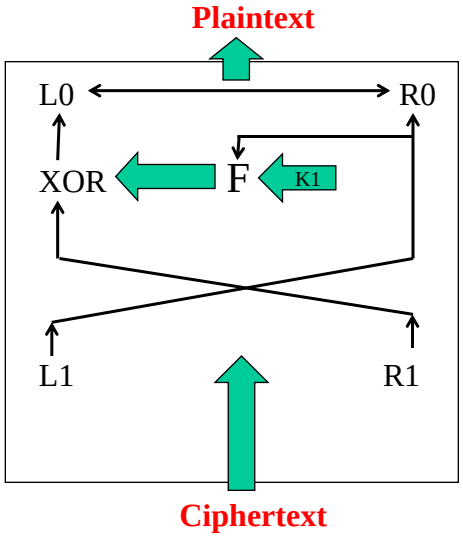
Rocke Verser vince dopo **5 mesi** avendo pubblicato su Internet un programma capace di distribuire le possibili chiavi e di far fare una ricerca esaustiva sui calcolatori di privati (10.000 $ divisi 60%/40% con l'utilizzatore che aveva trovato la chiave).

Secoda sfida DES (1998) vinta in **39 gg**. Nel 1998 la Electronic Frontier Foundation sviluppa un HW DES Cracker, che viola DES in **5 giorni**.

AES

- Necessità di chiavi più lunghe (128 bit)
- Riferimento a macchine a 64 bit
- Robustezza rispetto ad attacchi lineari e differenziali

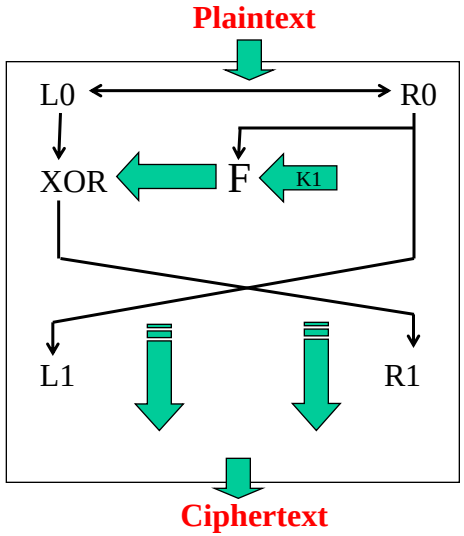
Feistel Cipher



Sia D = decryption

D(L1,R1) = L0,R0 =
(R1 XOR F(k1,L1)), L1

Feistel Cipher



Il sistema funziona:

D(E(L0,R0))=
= D(R0, (L0 XOR F(k1,R0))) =
= (L0 XOR F(k1,R0))
XOR F(k1,L1), R0 =
= L0 XOR F(k1,R0)
XOR F(k1,R0), R0 =
= L0, R0

DES Challenge

RSA security, nel 1997, offre **10.000 $** a chi avesse decifrato un testo ottenuto cifrando con DES una frase segreta («strong crypto makes the world a better place»).

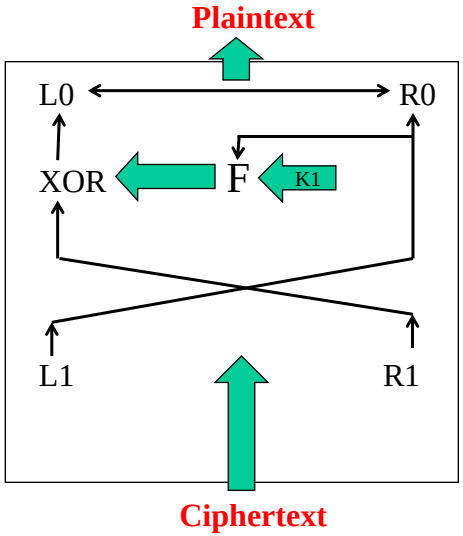
Rocke Verser vince dopo **5 mesi** avendo pubblicato su Internet un programma capace di distribuire le possibili chiavi e di far fare una ricerca esaustiva sui calcolatori di privati (10.000 $ divisi 60%/40% con l'utilizzatore che aveva trovato la chiave).

Secoda sfida DES (1998) vinta in **39 gg**. Nel 1998 la Electronic Frontier Foundation sviluppa un HW DES Cracker, che viola DES in **5 giorni**.

AES

- Necessità di chiavi più lunghe (128 bit)
- Riferimento a macchine a 64 bit
- Robustezza rispetto ad attacchi lineari e differenziali

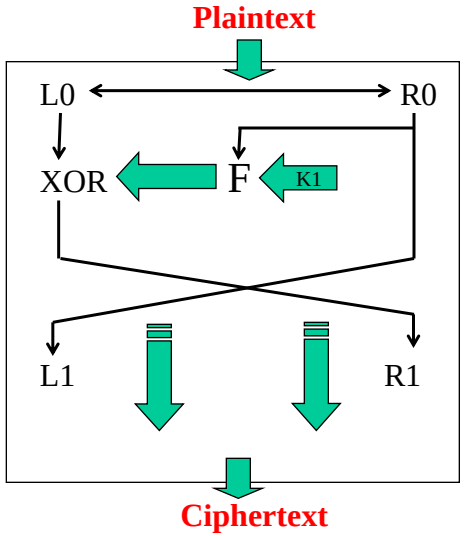
Feistel Cipher



Sia D = decryption

D(L1,R1) = L0,R0 =
(R1 XOR F(k1,L1)), L1

Feistel Cipher



Il sistema funziona:

D(E(L0,R0))=
= D(R0, (L0 XOR F(k1,R0))) =
= (L0 XOR F(k1,R0))
XOR F(k1,L1), R0 =
= L0 XOR F(k1,R0)
XOR F(k1,R0), R0 =
= L0, R0

DES Challenge

RSA security, nel 1997, offre **10.000 $** a chi avesse decifrato un testo ottenuto cifrando con DES una frase segreta («strong crypto makes the world a better place»).

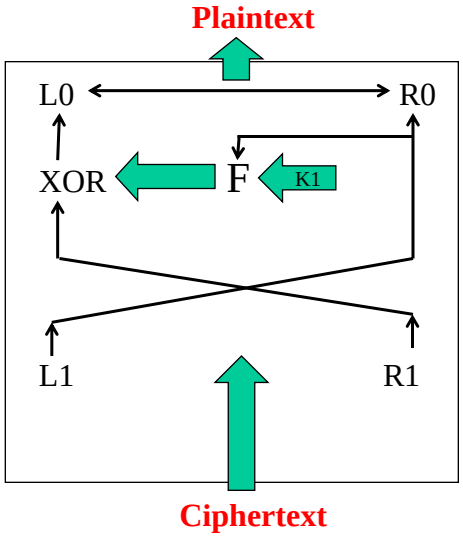
Rocke Verser vince dopo **5 mesi** avendo pubblicato su Internet un programma capace di distribuire le possibili chiavi e di far fare una ricerca esaustiva sui calcolatori di privati (10.000 $ divisi 60%/40% con l'utilizzatore che aveva trovato la chiave).

Secoda sfida DES (1998) vinta in **39 gg**. Nel 1998 la Electronic Frontier Foundation sviluppa un HW DES Cracker, che viola DES in **5 giorni**.

AES

- Necessità di chiavi più lunghe (128 bit)
- Riferimento a macchine a 64 bit
- Robustezza rispetto ad attacchi lineari e differenziali

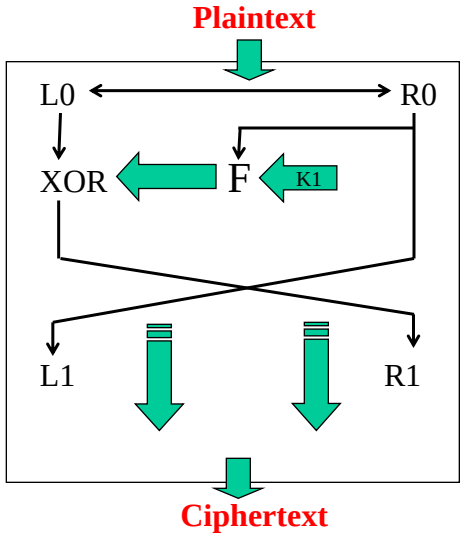
Feistel Cipher



Sia D = decryption

D(L1,R1) = L0,R0 =
(R1 XOR F(k1,L1)), L1

Feistel Cipher



Il sistema funziona:

D(E(L0,R0))=
= D(R0, (L0 XOR F(k1,R0))) =
= (L0 XOR F(k1,R0))
XOR F(k1,L1), R0 =
= L0 XOR F(k1,R0)
XOR F(k1,R0), R0 =
= L0, R0

DES Challenge

RSA security, nel 1997, offre **10.000 $** a chi avesse decifrato un testo ottenuto cifrando con DES una frase segreta («strong crypto makes the world a better place»).

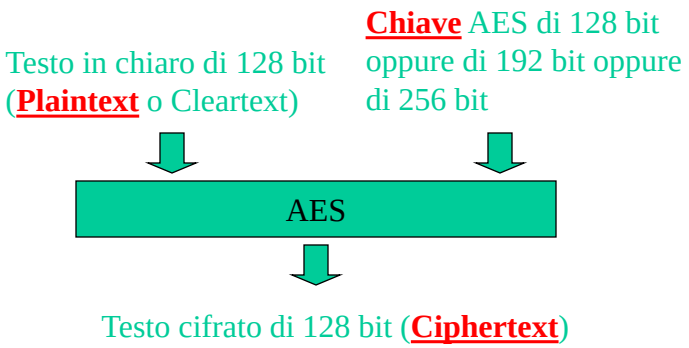
Rocke Verser vince dopo **5 mesi** avendo pubblicato su Internet un programma capace di distribuire le possibili chiavi e di far fare una ricerca esaustiva sui calcolatori di privati (10.000 $ divisi 60%/40% con l'utilizzatore che aveva trovato la chiave).

Secoda sfida DES (1998) vinta in **39 gg**. Nel 1998 la Electronic Frontier Foundation sviluppa un HW DES Cracker, che viola DES in **5 giorni**.

AES

- Necessità di chiavi più lunghe (128 bit)
- Riferimento a macchine a 64 bit
- Robustezza rispetto ad attacchi lineari e differenziali

Schema Generale di AES

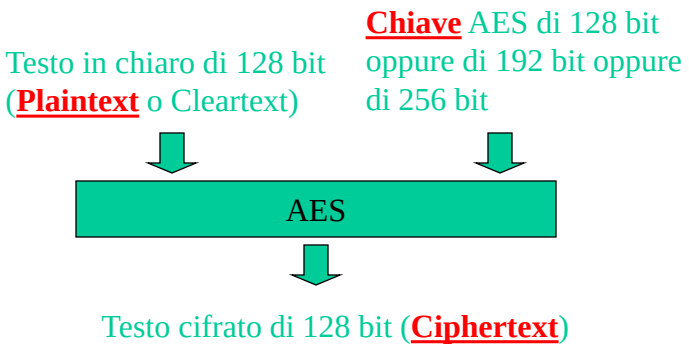


Caratteristiche di AES

http://csrc.nist.gov/CryptoToolkit/aes/

- Chiavi di 128/192/256 bit, blocco di 128
- Da 10 a 14 passi (‘rounds’)
- Efficiente
- Unici attacchi noti di tipo ‘forza bruta’

Schema Generale di AES



Caratteristiche di AES

http://csrc.nist.gov/CryptoToolkit/aes/

- Chiavi di 128/192/256 bit, blocco di 128
- Da 10 a 14 passi (‘rounds’)
- Efficiente
- Unici attacchi noti di tipo ‘forza bruta’