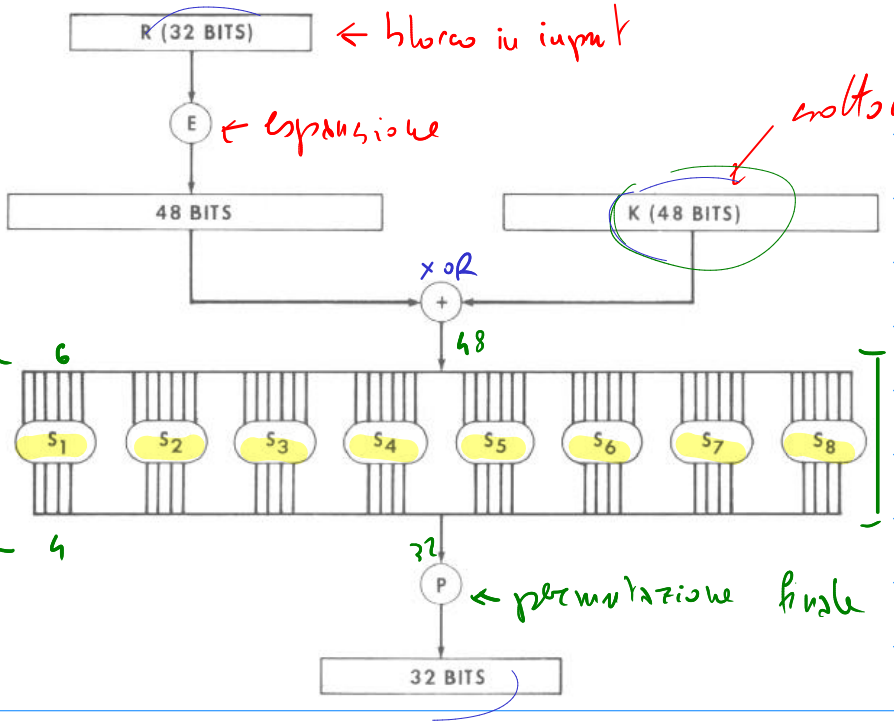


← blocco in input

← espansione

sottochiave derivata da K (esattamente mediante una semplice stream cipher).

operazione non lineare di selezione bits

← permutazione finale

DOVE È L'INFAMITÀ IN K_i?

Questi sono i criteri da rispettare.

→ resistenza alla crittoanalisi differenziale.

CONFUSIONE

In ogni ciclo abbiamo in input un blocco di 32 bit in output un nuovo blocco che dovrebbe essere statisticamente non correlato col blocco in input.

Cosa possiamo dire della differenza di 2 blocchi?

→ possiamo agire su se le differenze in ogni ciclo non dipendono dalla chiave (tutto è lineare) ↓
il nostro sistema è "praticamente" uno stream cipher.

→ possiamo anche agire se le differenze dipendono in modo "controllato" dai singoli bit della chiave.

crittoanalisi lineare

1977 2001

DES → AES

limitazioni di DES
- crittoanalisi lineare 2^{56}
- chiave piccola (56 bit) problema reale
- blocco piccolo (64 bit)

$2^{12}/2^6 = 2^6$

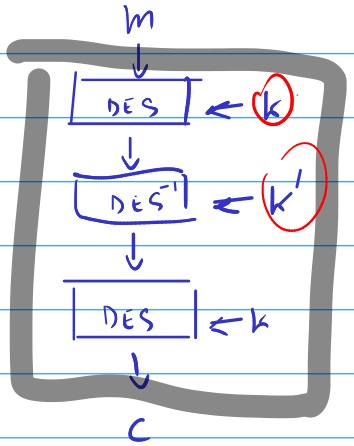
2048/64

4096/64

DES obsoleto.

↓

3DES

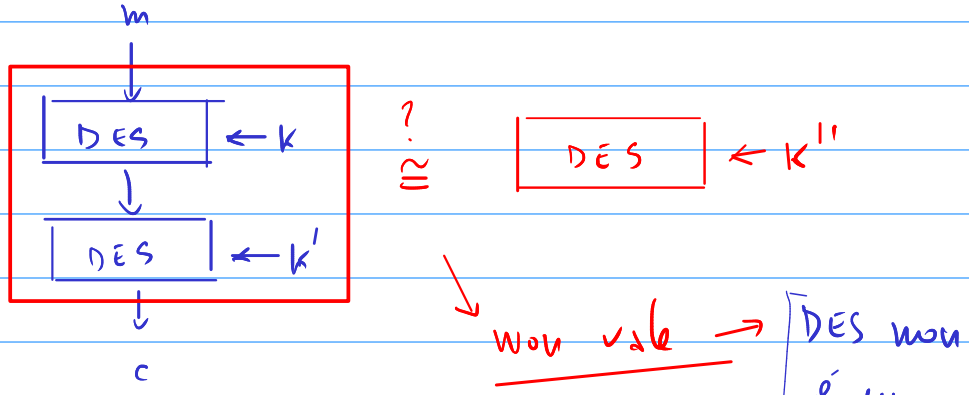


i bit segreti sono $56 \times 2 = 112$

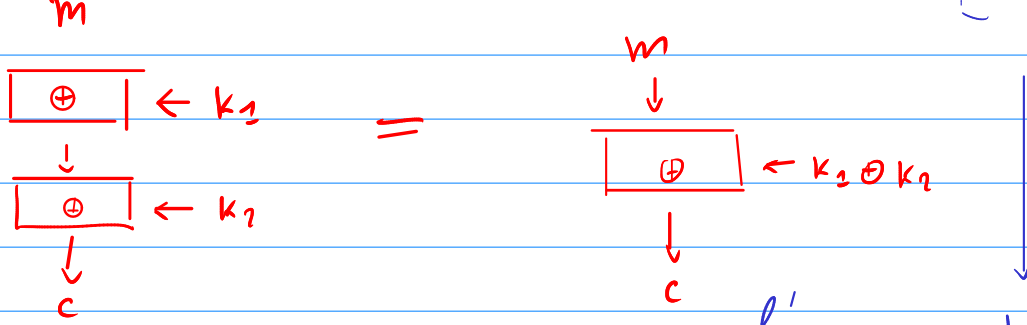
2 OSSERVAZIONI

1) Siamo sicuri che

$DES(DES(m,k),k') \neq DES(m,k'')$?



non vale → DES non è un gruppo



l'operazione di composizione di 2 codifiche con DES non è una codifica

con DES.

In termini algebrici. Sia $G_k : \begin{cases} \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64} \\ m \to DES(k, m) \end{cases}$

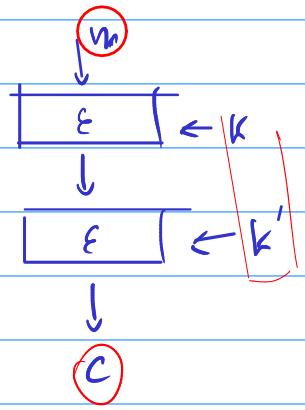
$\Rightarrow \{ G_k \mid k \in \mathbb{Z}_2^{56} \}$ non è chiuso rispetto la composizione di funzioni

$\Rightarrow$ NON È UN GRUPPO.

$$\langle \{ G_k \mid k \in \mathbb{Z}_2^{56} \} \rangle \neq \{ G_k \mid k \in \mathbb{Z}_2^{56} \}.$$

2) perché 3DES e non 2DES??

perché 2DES sarebbe vulnerabile ad attacchi di tipo meet in the middle.



vogliamo fare un attacco known plaintext.

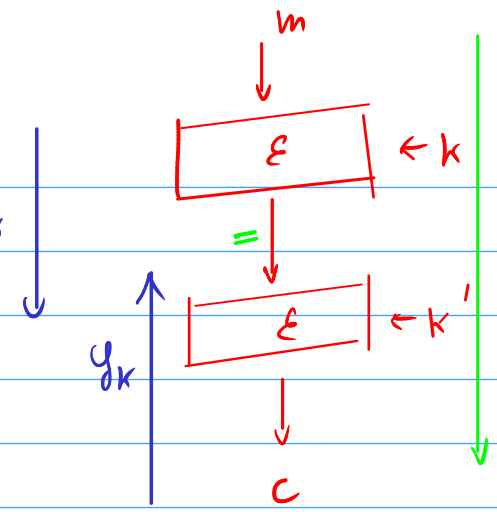
conosciamo m e c vogliamo trovare k e k'

$\forall (k, k')$ calcolo $E(k'(E(k, m))) \stackrel{?}{=} c$ — sì → ok, no → ricerco.

se $|k| = |k| \cong 2^{56}$ → # tentativi $\approx 2^{112}$

2^{56} $\forall k$ calcolo $E(k, m) = x_k$

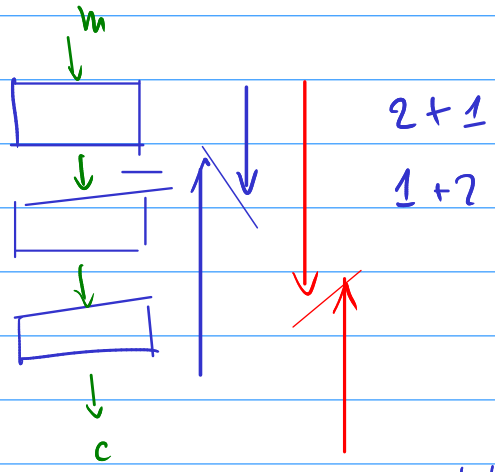
2^{56} $\forall k'$ calcolo $D(k', c) = y_{k'}$



Testo se $x_k = y_{k'}$ { sì → ok ; no → ricerco

operazioni $2^{56} + 2^{56} = 2^{57}$!!

Con 3DES si evita il meet in the middle.



questo è anche il motivo per cui per 3DES è inutile usare 3 chiavi diverse.

3) perché E/D/E e non E/E/E?

perché così se $k = k'$ vai avanti DES normale.

ph: noi sappiamo che se un blocco è di 64 bit e usiamo OTP con 64 bit => abbiamo un cifrario perfetto. In 3DES, blocco 64 bit, chiave

≈ 112 bit. E' perfetto? Se no, cosa c'è che non funziona?