Alternative al DES: cifratura multipla

Idea: concatenare più copie del DES, con chiavi diverse

Date due arbitrarie chiavi k_1 e k_2

$$C_{DES}(C_{DES}(m, k_1), k_2) \neq C_{DES}(m, k_3)$$

per qualsiasi messaggio m e qualsiasi chiave k_3

Due chiavi di 56 bit → una chiave di ~~112~~ **57** bit

Attacchi "meet in the middle"

$c = C_{DES}(C_{DES}(m, k_1), k_2)$ $\quad D_{DES}(c, k_2) = C_{DES}(m, k_1)$

Data una coppia <m,c>

1. per ogni k_1, si calcola e si salva $C_{DES}(m, k_1)$ in una tabella
2. per ogni k_2, si calcola $D_{DES}(c, k_2)$ e si cerca nella tabella

Costo: $O(2^b + 2^b)$ op. = $O(2^{b+1})$ op., b = bit della chiave

doppia enumerazione delle di chiavi → 2^{57}

Triple Data Encryption Algorithm (TDEA)

3TDEA

$$c = C_{DES}(D_{DES}(C_{DES}(m, k_1), k_2), k_3)$$

2TDEA

$$c = C_{DES}(D_{DES}(C_{DES}(m, k_1), k_2), k_1)$$

- Sicurezza pari a una chiave di 112 bit
- Certificati dal NIST fino al 2005
- Dal 2001, il nuovo standard per la cifratura simmetrica è l'AES (cifrario Rijndael)

Triple Data Encryption Algorithm (3TDEA)

$$c = C_{DES}(D_{DES}(C_{DES}(m, k_1), k_2), k_3)$$

Tre chiavi di 56 bit → ma sicurezza pari a una chiave di 112 bit

Attacchi "meet in the middle"

$D_{DES}(c, k_3) = D_{DES}(C_{DES}(m, k_1), k_2)$

$C_{DES}(D_{DES}(c, k_3), k_2) = C_{DES}(m, k_1)$

Data una coppia <m,c>

1. per ogni k_1, si calcola e si salva $C_{DES}(m, k_1)$ in una tabella
2. per ogni **coppia** di chiavi k_2, k_3, si calcola $C_{DES}(D_{DES}(c, k_3), k_2)$ e si cerca nella tabella

Costo: $O(2^b + 2^b \cdot 2^b)$ op = $O(2^{2b})$ op, b = bit della chiave

enumerazione delle coppie di chiavi → 2^{112}

Triple Data Encryption Algorithm (2TDEA)

$$c = C_{DES}(D_{DES}(C_{DES}(m, k_1), k_2), k_1)$$

Due chiavi di 56 bit → una chiave di 112 bit

Attacchi "meet in the middle"

$D_{DES}(c, k_1) = D_{DES}(C_{DES}(m, k_1), k_2)$

$C_{DES}(D_{DES}(c, k_1), k_2) = C_{DES}(m, k_1)$

Hanno lo stesso costo di un attacco esauriente sulle chiavi

Advanced Encryption Standard (AES)

AES è lo standard per le comunicazioni sicure dal 2001

Cifrario a blocchi di 128 bit, con chiavi di 128, 192 o 256 bit

	chiave (bit)	dim. blocco (bit)	Numero di fasi
AES (128)	128	128	10
AES (192)	192	128	12
AES (256)	256	128	14

Ogni fase opera su un blocco di 128 bit, logicamente organizzato come matrice bidimensionale B di 16 byte

B

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

AES(128): gestore delle chiavi

La chiave iniziale è caricata, per colonne, in una matrice W di byte 4 x 4
La matrice è ampliata aggiungendo 40 colonne, generate ricorsivamente a partire dalle prime 4: W[0], W[1], W[2], W[3]

W[0] W[1] W[2] W[3]

W

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

➔

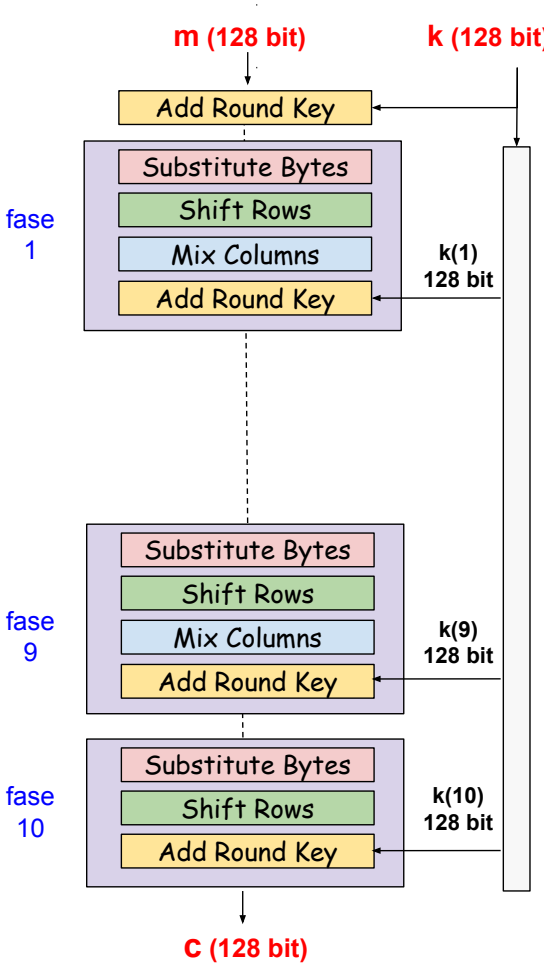
W[0]	W[1]	W[2]	…	W[42]	W[43]

W[i] = W[i-4] ⊕ W[i-1] , se i non è un multiplo di 4
W[i] = W[i-4] ⊕ **T**(W[i-1]), se i è un multiplo di 4 **T** trasformazione non lineare (S-box)

La chiave k(i) per la i-esima fase è data dalle 4 colonne

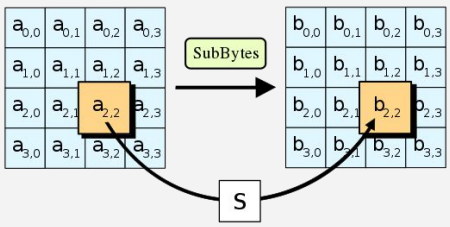
W[4i], W[4i+1], W[4i+2], W[4i+3]

AES (128)

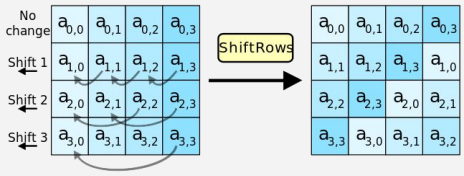


Gestore delle chiavi
Espansioni e trasformazioni non lineari (S-box)

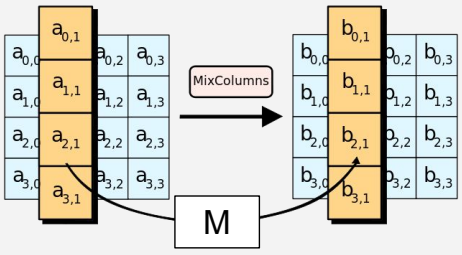
Trasformazioni di fase



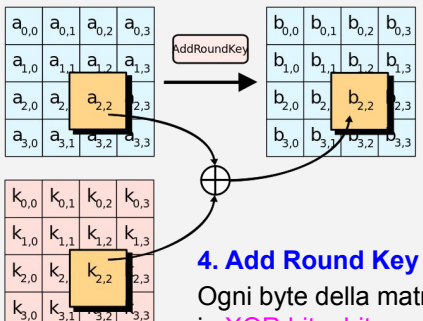
1. Substitution byte
ogni byte del blocco B è trasformato mediante una **S-box**: una look-up table che contiene una permutazione di tutti i 256 interi a 8 bit



2. Shift Rows
I byte di ogni riga vengono shiftati verso sinistra di 0, 1, 2 e 3 posizioni, rispettivamente ➜ i 4 byte di ogni colonna si disperdono su 4 colonne diverse



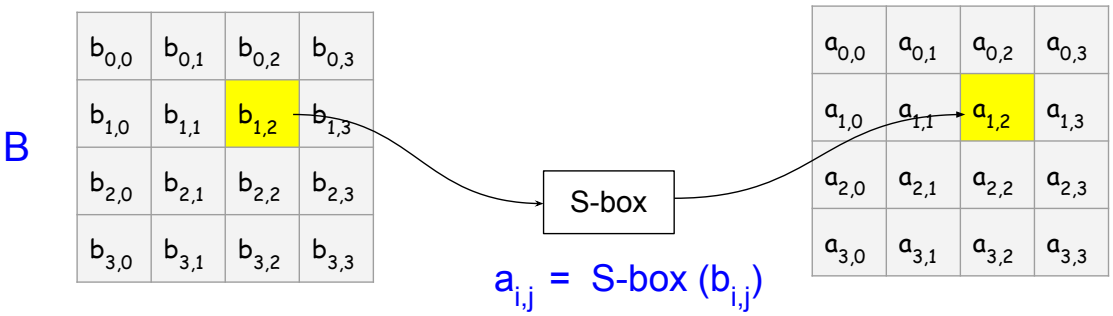
3. Mix Columns
$a_{i,j}$ si trasforma linearmente in un nuovo byte $b_{i,j}$ che dipende da tutti i byte della colonna j



4. Add Round Key
Ogni byte della matrice è posto in XOR bit a bit, con un byte della chiave locale di fase

Substitution byte

Ogni byte del blocco B è trasformato mediante una S-box



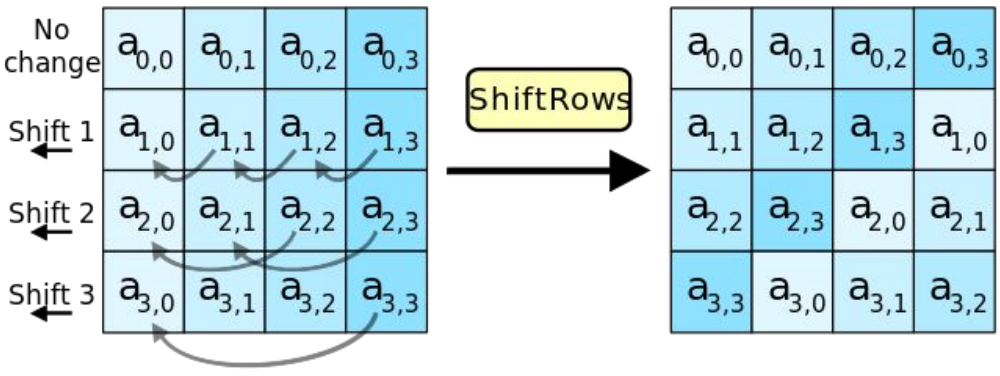
$a_{i,j} = S\text{-box}(b_{i,j})$

La S-box è una matrice di 16 x 16 byte, che contiene una permutazione di tutti i 256 interi a 8 bit (da 0 a 255)

Costruzione algebrica

ogni byte $b_{i,j}$ viene prima sostituito con il suo inverso moltiplicativo in $GF(2^8)$ [→ non linearità], e poi moltiplicato per una matrice di 8 x 8 bit e sommato con un vettore colonna

Shift Rows



I byte di ogni riga vengono shiftati ciclicamente verso sinistra di 0, 1, 2 e 3 posizioni, rispettivamente

In questo modo i 4 byte di ogni colonna si disperdono su 4 colonne diverse

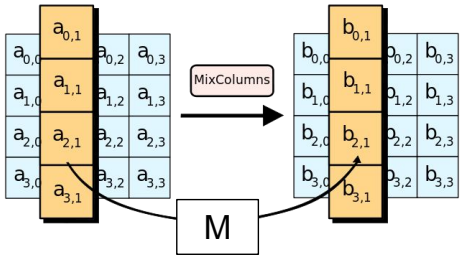
Mix Columns

Ogni colonna del blocco, trattata come un vettore di 4 elementi, viene moltiplicata per un matrice M prefissata di 4 x 4 byte

La moltiplicazione è eseguita mod 2^8, e la somma modulo 2 (operazioni del campo GF(2^8))

La matrice M è scelta in modo che ciascun byte della colonna venga mappato in un nuovo byte che è funzione di tutti i 4 byte presenti nella colonna

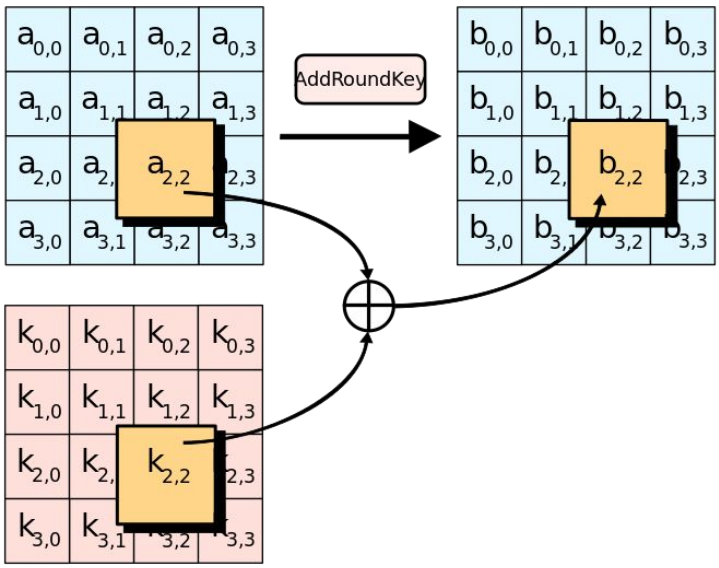
$a_{i,j}$ si trasforma in un valore $b_{i,j}$ che dipende da tutti i byte $a_{0,j}$, $a_{1,j}$, $a_{2,j}$, $a_{3,j}$ della colonna



Shift Rows e Mix Columns garantiscono **diffusione totale dopo solo due fasi:** ogni bit di output dipende da tutti i bit di input

Add Round Key

Ogni byte della matrice è posto in XOR (OR esclusivo) bit a bit, con un byte della chiave locale di fase



Sicurezza

Ad oggi nessuno attacco è stato in grado di compromettere AES anche nella sua versione più semplice con chiave di 128 bit

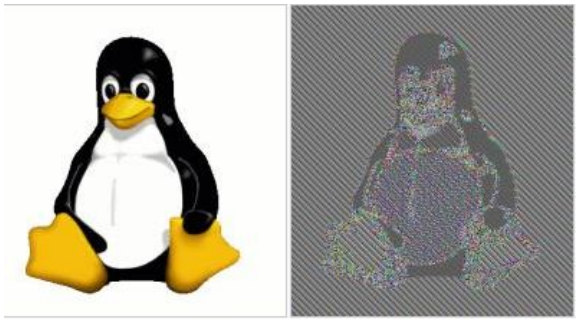
Tutti i bit della chiave sono bit di sicurezza

Esistono attacchi più efficienti di un attacco esauriente sulle chiavi per le versioni di AES con 6 fasi, ma nessun attacco è più efficiente se le fasi sono almeno 7

Si conoscono *attacchi side-channel* che non sfruttano le caratteristiche del cifrario ma le possibili debolezze della piattaforma su cui esso è implementato

Cifrari a blocchi

1. Come trattare i messaggi che hanno una lunghezza che non è un multiplo della dimensione del blocco? → PADDING
2. La cifratura a blocchi espone la comunicazione ad attacchi
   - ➢ blocchi uguali nel messaggio producono blocchi cifrati uguali (cifrati con la stessa chiave)
   - ➢ poca diffusione
   - ➢ periodicità nel crittogramma utile per la crittoanalisi



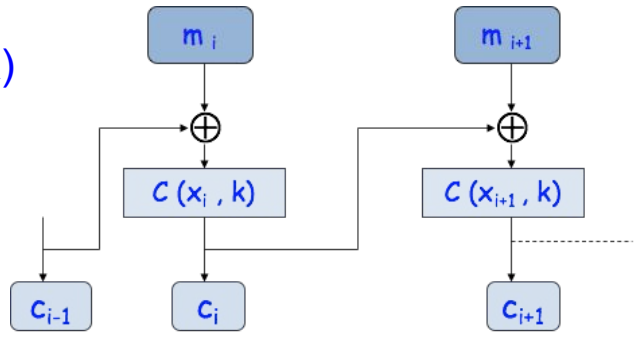
CBC: Cipher Block Chaining

Soluzione

- si compongono i blocchi tra loro
- il cifrario risultante è ancora strutturato a blocchi, ma blocchi uguali nel messaggio vengono (con pratica certezza) cifrati in modo diverso eliminandone così la periodicità

Cifratura

$c_i = C(m_i \oplus c_{i-1}, k)$

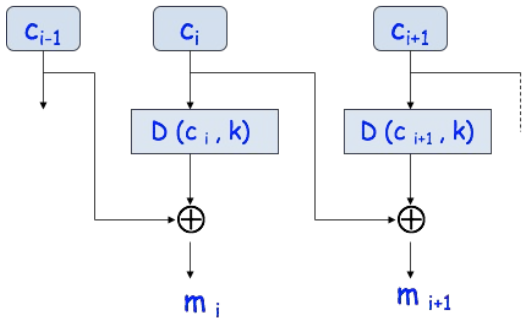


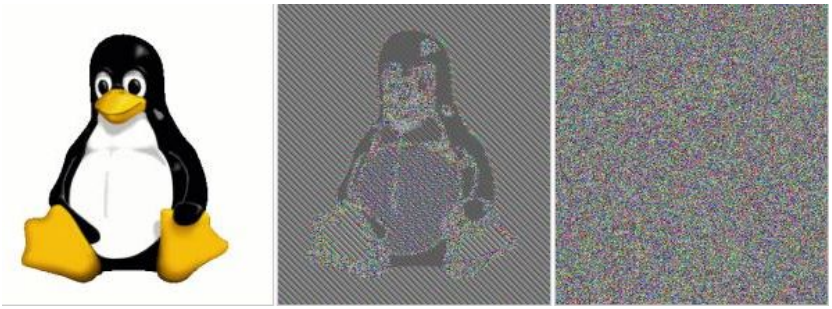
x_i indica il blocco $m_i \oplus c_{i-1}$

CBC: Cipher Block Chaining

Decifrazione

$m_i = c_{i-1} \oplus D(c_i, k)$





Originale Senza CBC CBC

ALTRI CIFRARI A CHIAVE SEGRETA

RC 5 (Ron's Code 5) Ron Rivest

- simile al DES, ne adotta la struttura migliorandone alcune parti
- lascia più libertà all'utente
- blocchi di **64 bit**
- chiave di **c x 32 bit**
- r fasi (valore consigliato: r = 16)
- r e c possono essere scelti a piacere
- usa shift ciclico, XOR, addizione mod 2^{32}
- molto veloce, resiste con successo agli attacchi standard se c e r sono scelti bene
- sicuro e impiegato con una certa frequenza
- SEMPLICITÀ DI REALIZZAZIONE E GRANDE SICUREZZA

IDEA (International Data Encryption Algorithm)

- 1992
- chiave da **128 bit**
- usa shift ciclico, XOR, moltiplicazione mod $(2^{16}+1)$ e addizione mod 2^{16},
- più semplice e più sicuro del DES
- la sicurezza poggia su basi teoriche molto forti
- è rimasto assolutamente inviolato, ma non è diventato il nuovi standard