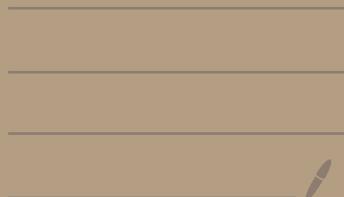


# CRITOGRAFIA

Versione del 2/11/2020

3DES e AES

ore 11:15



## VARIANTI DEL DES

① scelta indipendente delle sottochiavi di fase

$$\# \text{bit} : 56 \rightarrow 16 \times 48 = 768 \text{ bit}$$

Crittanalisi differenziale  $\rightarrow 2^{61}$

② Cifratura multipla

$\forall k_1, k_2$

$$C_D(C_D(m, k_1), k_2) \neq C_D(m, k_3)$$

$\forall m, \forall k_3$

# Spazio delle chiavi =  $2^{112}$  → non sono 112 bit  
di sicurezza

sicurezza pari a quello di una chiave di 57 bit

Attacko "Meet in the middle"

$$c = C(C(m, k_1), k_2)$$

$k_1, k_2$  ché si  
di 56 bit

$$\rightarrow D(c, k_2) = C(m, k_1)$$

si prende una coppia  $\langle m, c \rangle$

- $\forall k_1$ , calcolo e salvo  $C(m, k_1)$
- $\forall k_2$  calcolo  $D(c, k_2)$  e lo cerco nella lista delle cifrature

dove esistere certamente almeno una corrispondenza

$$N = 2^{56}$$

$N = 2^{56}$  cifrature +  $O(N)$  decifrature

costo:  $2^N \ll N^2 \rightarrow$  costo dell'enumerazione  
di tutte le copie  $(k_1, k_2)$

3DES

2TDEA  
↓  
# chiavi

3TDEA  
↓  
# chiavi

TDEA

Triple Data Encryption  
Algorithm

$$c = G(D(C(m, k_1), k_2), k_1)$$

$k_1$  e  $k_2$  sono chiavi di  
56 bit, tra loro indipendenti.

$k_1 = k_2 \Rightarrow$  2TDEA equivale a una singola  
cripto funzione DES

CDC non è più robusto di CCC

112 bit di sicurezza

3 TDEA

$$c = C(D(C(m, k_1), k_2), k_3)$$

$k_1, k_2, k_3$   
che si chi  
56 bit

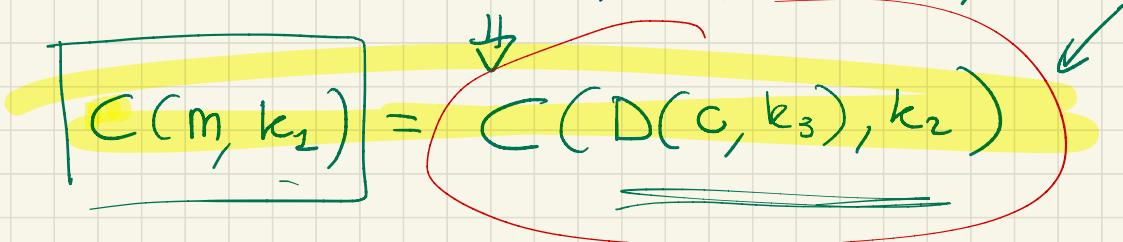
# bit della chiaie:  $56 \times 3 = 168$

vulnerabile a ~~padding~~ "Meet-in-the-middle"



112 bit di sicurezza

$$m = D(C(D(c, k_3), k_2), k_1)$$



1) enumero le clausi di 56 bit, e salvo le liste  
 $C(m, k_1)$  t.c.  $k_1 \in [0, 13^{56}]$

2) ~~per~~  $k_2, k_3$  calcolo  
 $C(D(c, k_3), k_2)$  e lo cerco  
nella lista

$$2^{56} + 2^{112}$$

(1)

costo di enumerare le coppie  $k_2, k_3$

# AES

bando con Scadema

06/98 → 21 cipher

## NIST

→ SICUREZZA, COSTO DI REALIZZAZIONE,  
CARATTERISTICHE ~~di~~ ALGORITMI

MARS	(IBM)	08/98	→ 15 cipher
RC6	(RSA)	04/99	→ 5 cipher
Rijndael	(Proton World Int. + Universitè Leuven, BELGIO)	10/00	→ 1: <u>AES</u>
Serpent	(Univ. Sheddele, UK, USA)		new standard dal 2001
TWOFISH	(Berkeley, Princeton)		
DAEMEN, RIJNEN		128, 192, 256	

AES,  
128 bit di chiave  
/fori

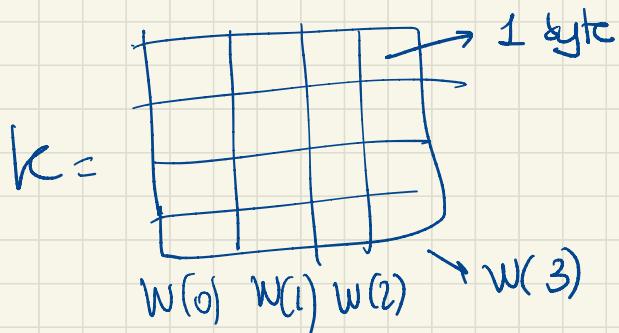
10 → 128 bit di chiave

12 → 192 "

14 → 256 bit "

### SELEZIONE delle SOTTO CHIAVI DI FASE

128



$W(i)$ : sequenze di  $k$  byte

↳ USA le S-box

$w(0), w(1), w(2), w(3)$

$\forall t \geq 4$

$$w(t) = w(t-1) \oplus w(t-4) \quad 4 \nmid t$$

$$w(t) = \underbrace{T(w(t-1))}_{\substack{\text{NO N} \\ \downarrow \\ \text{USA}}} \oplus w(t-4) \quad 4 \mid t$$

linear  
S-box

Choose  $i$ -time for:  
 $1 \leq i \leq 10$

$$w(4i), w(4i+1), w(4i+2), w(4i+3)$$

BB 2012

## CIFRATORA :

blocco di 128 bit

$$B = \begin{pmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{pmatrix}$$

RICETTA PER COLONNE

~~2~~  
~~1000000000000000~~

$$b_{ij} \in \{0, 1\}^8$$

## TRASFORMAZIONE INIZIALE

$k$ : matri $\times$  della chiave

$$B \rightarrow B \oplus k$$

10 fasi da 4 operazioni:

01: SUBSTITUTE BYTES

Ogni byte di B è sostituito ~~con~~ usando S-box

$$b_{ij} \rightarrow S\text{-box}(b_{ij})$$

02: SHIFT ROWS

03: MIX COLUMNS (non si applica nella fase 10)

04: ADD ROUND KEY

alla fine delle 10 fasi

$\rightarrow$  ~~il~~ il blocco B è il ciphertext

S-box

matrice  $16 \times 16$  di interi  $\in (0, 255)$

↳ contiene una permutazione

$b_{ij} \rightarrow S\text{-box } (b_{ij}) \in \{0, 1\}^8$

$$b_{ij} = \underbrace{b_1 b_2 b_3 b_4}_{0 \leq x \leq 15} \left| \begin{array}{cccc} b_5 & b_6 & b_7 & b_8 \\ \hline 0 & 0 & 0 & 0 \end{array} \right. \underbrace{b_5 b_6 b_7 b_8}_{0 \leq y \leq 15}$$

↓  
noga  
colonna

$$b_{ij} = \begin{array}{c|cc} 1000 & 10 & 11 \\ \hline 8 & & 11 \end{array}$$

$$S_{\text{box}} [8, 11] \rightarrow \frac{61}{\downarrow}$$

$$\boxed{00111101}$$

$x$   $\xrightarrow{\text{Sbox}}$   $x^{-1}$   
 byte  $\downarrow$  inverso moltiplicativo in  $\underline{GF(2^8)}$   
 + Componente lineare  
 $\xrightarrow{\text{Somme mod 2}}$   
 moltiplicazione mod  $2^8$

Galois field  
 (Compi finiti di Galois)

## 02 SHIFT ROWS

b <sub>00</sub>	b <sub>01</sub>	b <sub>02</sub>	b <sub>03</sub>
b <sub>10</sub>	b <sub>11</sub>	b <sub>12</sub>	b <sub>13</sub>
b <sub>20</sub>	b <sub>21</sub>	b <sub>22</sub>	b <sub>23</sub>
b <sub>30</sub>	b <sub>31</sub>	b <sub>32</sub>	b <sub>33</sub>

b <sub>00</sub>	b <sub>01</sub>	b <sub>02</sub>	b <sub>03</sub>
b <sub>11</sub>	b <sub>12</sub>	b <sub>13</sub>	b <sub>10</sub>
b <sub>22</sub>	b <sub>23</sub>	b <sub>20</sub>	b <sub>21</sub>
b <sub>33</sub>	b <sub>30</sub>	b <sub>31</sub>	b <sub>32</sub>

### 03 MIX COLUMNS.

M matrice  $4 \times 4$  byte

cogni colonna del blocco B

$$\xrightarrow{b} B_j \rightarrow M * B_j$$

$$0 \leq j \leq 3$$

il nuovo

$b_{ij}$  si vede un valore che dipende  
dei dati i byte delle colonne  
dipende da  $b_{0j}, b_{1j}, b_{2j}, b_{3j}$

$$\text{Oh: } b_{ij} \rightarrow b_{ij} \oplus k_{ij}$$