

CIFRARI per la sicurezza di massa

Offrono sicurezza computazionale

ADVANCED ENCRYPTION STANDARD

Chiavi brevi: (128 o 256 bit)

Cifrario simmetrico a blocchi

Preceduto da DATA ENCRYPTION STANDARD

La sicurezza e' basata sui PRINCIPI di SHANNON

- DIFFUSIONE Ogni carattere del cattogramma deve dipendere da tutti i caratteri del blocco di messaggio
Il testo in chiaro si deve distribuire su tutto il cattogramma
- CONFUSIONE Il messaggio e la chiave sono combinati in modo molto complesso per non permettere a E di separare le due seguenti tecniche di crittanalisi statistica

CIFRARIO DES

Primo cifrario ufficialmente certificato per la protezione di informazioni non classificate

IBM aveva proposto LUCIFER:

Chiave a 128 bit

S-box non lineare

NSA:

64 bit di cui 56 veramente cruciali

S-box differente, sempre non lineare

Struttura:

- Il messaggio è diviso in blocchi da 64 bit
- Cifrazione e decifrazione procedono attraverso $r=16$ fasi in cui si ripetono le stesse operazioni.
- Chiave K lunga 8 Byte: 7 bit di chiave, l'ottavo è la "parità" (per essere sicuri che K sia corretta).

Messaggio m	Chiave K	PI, PF presenti nelle realizzazioni hardware
+64	+64	
PI	T	
Permutation (m)	Elimina bit di parità; rimanda gli altri	
64 +	56 +	

$$S[0] \rightarrow [0] K[0]$$

$$\backslash \quad | \quad /$$

:

$$S[15] \rightarrow [15] K[15]$$

$$\backslash \quad | \quad /$$

$S[16] \quad D[16]$



$i \in \{1, \dots, 16\}$.

$$S[i] = D[:i]$$

$D[16]$

$S[16]$

$+^{64}$

$$D[:] = S[:i] \oplus f(D[:i], K[i:i])$$

PF

$+^{64}$

Critogramma c

Per : dettagli, ved. slide 4 AES.

Non e' da ricordare per l'esame.

S-box

Divido 48 bit in blocchi da 6

Per ogni blocco :

- Prende primo e ultimo bit:

indicano la riga

- Prende : 4 bit centrali:

indicano la colonna con

eventuale padding.

$c = C_{DES}(m, k)$

$c = C_{DES}(m, E)$

Che relazione c'e'?

$c^* = C_{DES}(m, k')$

$$b : \oplus k :$$

$$\overline{b} : \oplus \overline{k} : = b : \oplus k :$$

$$\text{Dim: } (b : \oplus 1) \oplus (k : \oplus 1)$$

$$b : \oplus k : \oplus (1 \oplus 1) \Rightarrow T_h$$
$$\Rightarrow c = c'$$

Tra c e c' non c'è nessuna relazione

Sicurezza e attacchi al DES

- E' vulnerabile alla crittanalisi lineare
- Architetture costruite ad hoc per decifrare riuscivano in poco tempo e a basso prezzo (1 mil. \$).
- fine anni '80: vengono intraviste le sfide a DES, in 5 mesi viene decifrato un criptogramma con un algoritmo distribuito, viene esplorato il 25% dello spazio delle chiavi
l'anno dopo in 39 giorni esplorando l'85% dello spazio delle chiavi

Si dice che un cifrario ha sicurezza di b bit se il costo del miglior attacco è di ordine $O(2^b)$ operazioni di decifratura

o). La chiave nonostante sia lunga 64 bit ha 55 bit di sicurezza ($64 - 8 - 1$)

k e \bar{k} si controllano simultaneamente

$$c = C(m, k) = C(\bar{m}, \bar{k})$$

Si fa un attacco di tipo chosen plain text

Chiedo $(m, c_1), (\bar{m}, c_2) \dots$

$\forall k$ provo a cifrare m con k :

$$\exists k : m \xrightarrow{k} c_1$$

- $\Rightarrow k$ probabilmente è la chiave,

verifico con altre copie

- altrettanto verifico che

$$C(m, k) = c_2 \Rightarrow \bar{k} \text{ probabilmente}$$

è la chiave

- Se nessuna delle due verifiche viene

passata, scarto le due chiavi $\bar{k}, \bar{\bar{k}}$.

Negli anni '90 viene diffusa la tecnica di crittografia differentiale, fa uso di 2^{47} coppie (m, c) , è un attacco chosen plain text che trova la chiave dopo una analisi statistica di come variazioni su m si percuotono su c .

La crittoanalisi differenziale costa come forza bruta su 16 fasi.

Viene introdotta la cifratura lineare

Known plain text

Costa meno del forte bit

Alternativa al DES:

CIFRATURA MULTIPLA

Idea: concatenare più copie del DES con chiavi diverse

Date due chiavi k_1, k_2

M : messaggio, k_2 : chiave.

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

2 chiavi da 56 bit \rightarrow 112 di sicurezza?

No, 57 bit di sicurezza

Attacco meet in the middle:

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

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

Data una coppia (m, c) :

- per ogni k_1 , calcolo e salvo $C_{(m, k_1)}$ in una tabella
- per ogni k_2 , calcolo $D(c, k_2)$ e lo cerco nella prima tabella

Costa come enumerare 2 volte sequenze di 2^{56} bit:

Costa $2^{57} \rightarrow 57$ bit di sicurezza.