CIFRARI SIMMETRICI (DES, AES)

Gli esercizi (1), (2) (3) e (5) sono tutti molto simili: si tratta di simulazioni del DES [si faccia riferimento alla figura 7.3 del libro]

Vediamo come esempio la soluzione dell'esercizio (1). Le altre si ottengono in modo del tutto simile.

ESERCIZIO 1

1) Matricola = $65\underbrace{43}21$

$$C = \underbrace{100}_{4}\underbrace{011}_{3}$$

2) I bit di C entrano nella S box, e diventano l'input della prima delle 8 funzioni (quella riportata nella figura 7.6 del libro).

INPUT S_1: $1\underbrace{0001}1$

indice di riga: $(11)_2 = 3$

indice di colonna: $(0001)_2 = 1$

L'output è $(12)_{10} = (1100)_2$

I quattro bit 1100 sono i primi 4 bit in uscita dalla Sbox e per effetto della permutazione P, finiscono nelle posizioni

POS: 9, 17, 23, 31

Infatti, la matrice P manda i primi 4 bit (1, 2, 3, 4) nelle posizioni 9, 17, 23 e 31, rispettivamente.

Dunque, le posizioni dei bit di $D[i]$ influenzate dalla sequenza C sono

$D[i]_9$, $D[i]_{17}$, $D[i]_{23}$ e $D[i]_{31}$

3) L'uscita dalla permutazione P viene posta in XOR bit a bit, con $S[i-1]$, e in questo modo si ottiene la sequenza $D[i]$. Risulta dunque:

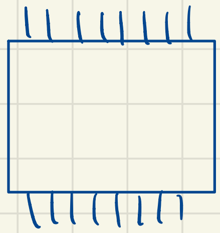
$$D[i]_9 = S[i-1]_9 \oplus 1 = 1 \oplus 1 = 0$$

$$D[i]_{17} = S[i-1]_{17} \oplus 1 = 1 \oplus 1 = 0$$

$$D[i]_{23} = S[i-1]_{23} \oplus 0 = 1 \oplus 0 = 1$$

$$D[i]_{31} = S[i-1]_{31} \oplus 0 = 1 \oplus 0 = 1$$

ESERCIZIO 4



8 bit di input $\rightarrow 2^8$ configurazioni possibili

8 bit di output $\rightarrow 2^8$ configurazioni

Per ogni configurazione di input, posso scegliere in 2^8 modi l'output.

$\rightarrow$ # funzioni $= (2^8)^{2^8} = 2^{8 * 2^8}$

ESERCIZIO 6

Sia c il crittogramma relativo ad un generico messaggio m:

$$c = G(m, k)$$

Possiamo rappresentare $c = c_1 c_2, \dots, c_{128}$ in questo modo:

$$c = \bigoplus_{i : c_i = 1} e^{(i)}$$

dove

$$e^{(i)} = 000 \dots 0\underset{i}{1}0 \dots 0 ,$$

cioè $e^{(i)}$ è un blocco di 128 bit, in cui l'i-esimo bit è uguale a 1, e tutti gli altri sono 0.

Ad esempio:

$$c = \underset{1\,2\,3\,4}{1011} = \underbrace{1000}_{e^{(1)}} \oplus \underbrace{0010}_{e^{(3)}} \oplus \underbrace{0001}_{e^{(4)}}$$

Sfruttiamo quindi la proprietà delle funzioni di cifratura e di decifrazione:

$$m = \mathcal{D}(c, k) = \mathcal{D}\left(\bigoplus_{i: c_i = 1} e^{(i)}, k\right) =$$

$$= \bigoplus_{i: c_i = 1} \mathcal{D}(e^{(i)}, k)$$

Si chiede la decifrazione dei 128 testi cifrati $e^{(i)}$, $i \in [1, 128]$:

$$f^{(i)} = \mathcal{D}(e^{(i)}, k) \qquad i \in [1, 128]$$

Si può così decifrare qualsiasi crittogramma c anche senza conoscere la chiave k:

$$m = \bigoplus_{i: c_i = 1} f^{(i)}$$

ESERCIZIO 7

$$c = C_{DESX}(m, k, w) = w \oplus C_{DES}(m \oplus w, k)$$

$$\Rightarrow \quad c \oplus w = C_{DES}(m \oplus w, k)$$

$$\mathcal{D}_{DES}(c \oplus w, k) = \mathcal{D}_{DES}(C_{DES}(m \oplus w, k), k)$$

$$\Rightarrow \quad D_{DES}(c \oplus \omega, k) = m \oplus \omega$$

$$\Rightarrow \quad m = \omega \oplus D_{DES}(c \oplus \omega, k)$$

ESERCIZIO 8

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

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

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

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

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

2) Se c_i è danneggiato anche m_i lo sarà. Se m_i è danneggiato, lo sarà anche il blocco successivo m_{i+1}, e così via. Dunque, da m_i in poi tutti i blocchi saranno danneggiati.

ESERCIZIO 9

Vedi libro di testo.