

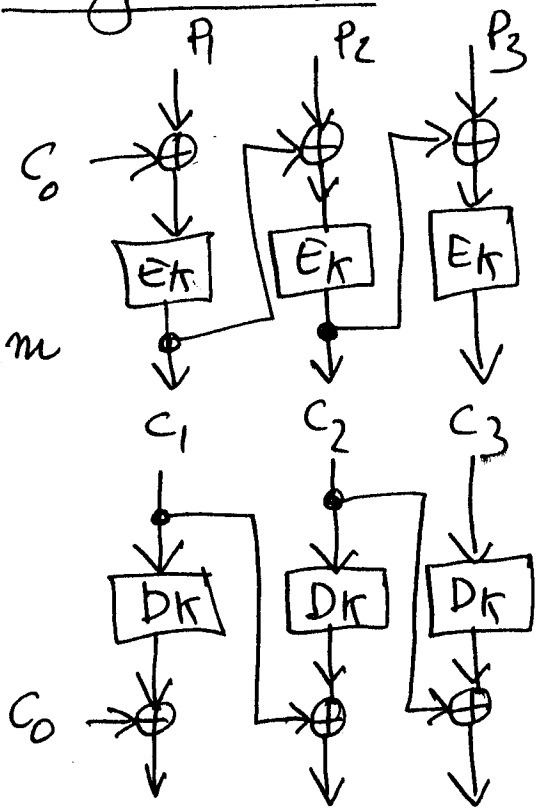
QUESTO 1

Recupero 'sicurezza delle Ret'
Luglio 2003 ①

(a) encrypt

$$c_i = E_K(c_{i-1} \oplus p_i)$$

$$E_K(x) = (ax + b) \bmod m$$



decrypt

$$p_i = c_{i-1} \oplus D_K(c_i)$$

$$D_K(x) = a^{-1}(x - b) \bmod m$$

(b) $m = 16$
 $c_0 = 1010 =$ Affinché $\exists a^{-1}$ deve essere
 $a = 5$ $\gcd(16, 5) = 1$ $a \perp m$
 $b = 3$ ok

$$a^{-1} = a^{\varphi(m)-1} \bmod m = 5^7 \bmod 16 = 13$$

infatti: $\varphi(m) = 2^4 - 2^3 = 2^3 = 8$

e inoltre:

S&M		$12 \times 5 = 5$	} mod 16
		$25 \times 5 = 125 = 13$	
		$13^2 \times 5 = 845 = \underline{13}$	

$7 \rightarrow 111$

$$(c) \quad \pi \equiv (a, b, IV)$$

(2)

$$|\mathcal{K}| = N_{\text{char}} = m \varphi(m) 2^{\frac{m}{2}} = 16 \times 8 \times 16 = 2048$$

(d) cifratura

$$P_1 = 12; \quad P_2 = 15; \quad P_3 = 0$$

$$P_1 \equiv 1100 = 'C' \text{ hex}$$

$$P_2 \equiv 1111 = 'F' \text{ hex}$$

$$P_3 \equiv 0000 = '0' \text{ hex}$$

$$\bullet C_1 = E_K(P_1 \oplus IV)$$

$$\begin{array}{r} 1100 \\ 1010 \\ \hline 0110 \rightarrow '6' \text{ hex} \end{array}$$

$$C_1 \equiv 5 \times 6 + 3 \equiv 33 \pmod{16} = 1 \text{ hex} \equiv 0001$$

$$\bullet C_2 = E_K(P_2 \oplus C_1)$$

$$\begin{array}{r} 1111 \\ 0001 \\ \hline 1110 \rightarrow 'D' \equiv 14 \end{array}$$

$$C_2 = 5 \times 14 + 3 = 73 \pmod{16} = 9 \equiv 1001 \text{ hex}$$

$$\bullet C_3 = E_K(P_3 \oplus C_2)$$

$$\begin{array}{r} 0000 \\ 1001 \\ \hline 1001 \rightarrow '9' \text{ hex} \end{array}$$

$$C_3 = 5 \times 9 + 3 \equiv 48 \pmod{16} = 0 \text{ hex}$$

$$C_1 C_2 C_3 \equiv 190$$

(e) decifratura

$$\bullet P_1 = D_K(C_1) \oplus IV$$

$$D_K(1) = 13(1-3) = -26 \pmod{16} = 6 \equiv 0110$$

$$P_1 = 1100 = 'C' \text{ hex}$$

$$\bullet P_2 = D_K(C_2) \oplus C_1 = 1111 = 'F' \text{ hex}$$

$$\bullet P_3 = D_K(C_3) \oplus C_2 = 0000 = '0' \text{ hex}$$

$$\begin{array}{r} 0110 \\ 1010 \\ \hline 1100 \rightarrow (2) \\ \rightarrow 'C' \end{array}$$

OK

QUESITO 2 Recupero ~~Simone~~ Luglio 2003 ①

(a) p primo; $0 \leq k \leq p-2$; $k \in \mathbb{Z}_{p-1}^* \equiv k \perp (p-1)$

(i) i valori di p mo
 $p \in \mathcal{P} \equiv \mathbb{Z}_p^* \equiv \{1, 2, 3, 4, \dots, 52\}$

(ii) $1 \leq k \leq 51$

essendo $k \in \mathbb{Z}_{p-1}^*$ devo scegliere solo i valori di $k \perp (p-1)$ e cioè $k \perp 52$. Analizzando a uno a uno (sappiamo che $|\mathbb{Z}_{p-1}^*| = \varphi(p-1) = 24$) si ottiene

$\mathcal{H} \equiv \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 41, 43, 45, 47, 49, 51\}$ 24 termini

(b) gli elementi primitivi di \mathbb{Z}_p^* sono nel numero di:

$$\#_{\substack{\text{elementi} \\ \text{primitivi} \\ \mathbb{Z}_p^*}} = \varphi(p-1) = \varphi(52) = (13-1)(2^2-2) = 24$$

(c) α è primitivo di \mathbb{Z}_p^* se $\alpha^{\frac{p-1}{q_i}} \pmod p \neq 1, \forall i$

$$\alpha = 5$$

$$p-1 = 52 = 13 \times 2^2$$

$$5^{26} \pmod{53} = (5^{13} \pmod{53})^2 \pmod{53} = 52 \text{ ok}$$

$$5^4 \pmod{53} = 42 \text{ ok}$$

ok - $\alpha = 5$ è primitivo

$$(d) \quad \beta = \alpha^a \pmod{p} = 5^{19} \pmod{53} = 35 \quad (2)$$

$$19 \rightarrow 10011$$

1	$12 \times 5 \equiv 5$	
0	$25 \equiv 25$	
0	$(25^2) \equiv 625 = 42$	$\pmod{53}$
1	$(42)^2 \times 5 = 8820 = 22$	
1	$(22)^2 \times 5 = 2420 = \underline{\underline{35}}$	

$$(e) \quad \text{SIB}_k(P, k) = (\gamma, \delta) \quad \begin{cases} \gamma = \alpha^k \pmod{p} \\ \delta = [(P - a\gamma)k^{-1}] \pmod{(p-1)} \end{cases}$$

$$k=1 \quad k^{-1} \pmod{(p-1)} = 1$$

$$\begin{cases} \gamma = 5^1 \pmod{53} = \underline{\underline{5}} \\ \delta = [(42 - 19 \cdot 5)1] \pmod{52} = \underline{\underline{51}} \end{cases}$$

$$\begin{cases} P = 42 \\ k = 1 \end{cases}$$

$$(f) \quad \text{VER}_k(P, \gamma, \delta) \\ \text{e'Vera } \alpha \quad \beta^\delta \gamma^\delta \equiv \alpha^P \pmod{p}$$

$$\beta^\delta \gamma^\delta \pmod{p} = 35^5 5^{51} \pmod{53} = 35^5 (5^{10 \cdot 5}) \pmod{53} = \\ = 41 (4^5 \cdot 5) \pmod{53} = \underline{\underline{40}}$$

$$\alpha^P \pmod{p} = 5^{42} \pmod{53} = (5^{10 \cdot 4} \cdot 5^2) \pmod{53} = 4^4 \cdot 5^2 \pmod{53} = \underline{\underline{40}}$$

$$(* \text{ encudo } 5^{10} \pmod{53} = 4) \quad \Rightarrow \text{OK!}$$