Residui quadratici

(1)

p primo > 2, dispari

$$a \in \mathbb{Z}_p^* \qquad a \nmid p$$

quali $\quad a \equiv b^2 \pmod p$?

$a = \{1, 2, \dots (p-1)\}$, $(p-1)$ residui in $\mathbb{Z}_p^*$

$\varphi(p) = p-1$

radici primitive $= \varphi(p-1)$ ($p-1$ pari sempre)

quali a sono residui quadratici tali che

$$a = b^2$$

e cioè a ha due radici $\pm b$ esattamente

Per calcolare i quadrati in $\mathbb{Z}_p^*$ basta prendere

$$b = 1, 2, 3 \dots \frac{(p-1)}{2}$$

e fare $\quad b^2 \bmod p$

per i rimanenti

$$+\frac{(p-1)}{2}+1, \frac{(p-1)}{2}+2 \dots (p-1)$$

risultano tutti $\equiv -b \pmod p$ per alcuni b.

perché la presenza di una metà degli elementi di $\mathbb{Z}_p^*$, nel senso di $\left(\frac{p-1}{2}\right)$, che sono quadrati.

ES. $p=11$ $\quad \mathbb{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$

$(p-1) = 10$ elementi

$\frac{p-1}{2} = 5$ elementi
sono quadrati
e sono residui quadratici

gli altri
$\frac{p-1}{2} = 5$ elementi sono non residui

---

i residui sono:

b	
1	$1^2 = 1$
2	$2^2 = 4$
3	$3^2 = 9$
4	$4^2 = 16 = 5$
5	$5^2 = 25 = 3$

$a_q = 1, 3, 4, 5, 9$

i non residui sono:

$-b$

$(-5)^2 = 6^2 \equiv 36 \equiv 3$

$(-4)^2 = 7^2 \equiv 49 \equiv 5$

$(-3)^2 = 8^2 \equiv 64 \equiv 9$

$(-2)^2 \equiv 9^2 \equiv 81 \equiv 4$

$(-1)^2 \equiv 10^2 \equiv 100 \equiv 1$

$a_{\bar{q}} = 2, 6, 7, 8, 10$

non c'è $b^2 \equiv a_{\bar{q}} \pmod{p}$

Se $\alpha = g$ è un elemento generatore di $\mathbb{Z}_p^*$

Allora $g^i = \left(\pm g^{\frac{i}{2}}\right)^2 = a_q = g^i$ con i pari

$a_{\bar{q}} \equiv g^i$ con i dispari

ES. $p = 11$ $\quad p-1 = 10 = 2 \times 5$ $\quad$ es. $g = 2$

$g^{\frac{10}{2}} \equiv g^5 \equiv 2^5 = 32 = 10 \not\equiv 1$ OK

$g^{\frac{10}{5}} \equiv g^2 \not\equiv 1$ $\quad 2^2 = 4 \not\equiv 1$ OK

$g = 2$

$2^0 \equiv 1$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

$2^4 \equiv 16 \equiv 5$

$2^5 \equiv 32 \equiv 10$

p $\quad 2^6 \equiv 64 \equiv 9$

$2^7 \equiv 128 \equiv 7$

$2^8 \equiv 256 \equiv 3$

$p-2$ $\quad 2^9 \equiv 512 \equiv 6$

$p-1$ $\quad 2^{10} \equiv 1024 \equiv 1$

$a_q = g^{i\,\text{PARI}}$

(mod 11)

4

$p=11 \qquad p-1=10=2\times 5$

mod 11

$\alpha=3 \qquad 3^5 \equiv 243 \equiv 1$ NO

$3^2 \equiv 9 \not\equiv 1$ OK

$\alpha=4 \qquad 4^5 \equiv 2^{10} \equiv 1024 \equiv 1$ NO

$\alpha=5 \qquad 5^5 \equiv 15625 \equiv 1$ NO

$\alpha=2 \qquad \left.\begin{array}{l} 2^5 \equiv 32 \equiv 10 \not\equiv 1 \\ 2^2 \equiv 4 \not\equiv 1 \end{array}\right\}$ OK 2

$\alpha=6 \qquad \left.\begin{array}{l} 6^5 \equiv 10 \not\equiv 1 \\ 6^2 \equiv 36 \equiv 4 \not\equiv 1 \end{array}\right\}$ OK 6

ver

$\underline{\alpha=g=2}$

	a_g		$b=$
	$2^2 \equiv 4$	$j=2$	$2^{\frac{j}{2}} = 2$
	$2^4 \equiv 5$	$j=4$	$2^2 = 4$
	$2^6 \equiv 9$	$j=6$	$2^3 = 8$
	$2^8 \equiv 3$	$j=8$	$2^4 = 16 \equiv 5$
	$2^{10} \equiv 1$	$j=10$	$2^5 \equiv 32 \equiv 10$

$b = \pm 2, \pm 4, \pm 8, \pm 5, \pm 10.$

$b^2 \equiv a \pmod{p}$

$\underline{a = 4, 5, 9, 3, 1}$

$x^2 \equiv a \pmod p$

Esempio $p = 13$ $p \equiv 1 \pmod 4$

Trovare i residui quadratici di $\mathbb{Z}_p^*$, $a \in \mathbb{Z}_p^*$

$\mathbb{Z}_p^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ RQ

$p - 1 = 12 = 3 \times 2^2$

6 quadratici $\frac{p-1}{2} = 6$

6 non residui

Trovo un elemento primitivo es. 2

$$\begin{cases} 2^{\frac{12}{3}} \equiv 2^4 \equiv 16 \equiv 3 \pmod{13} \not\equiv 1 \text{ ok} \\ 2^{\frac{12}{2}} \equiv 2^6 \equiv 64 \equiv 12 \pmod{13} \not\equiv 1 \end{cases}$$

$2^1 \equiv 2 \equiv 2$

$2^2 \equiv 4 \equiv 4 \rightarrow x = 2 \rightarrow 2^2 = 4$ ± 2

$2^3 \equiv 8 \equiv 8$

$2^4 \equiv 16 \equiv 3 \rightarrow x = 4 \rightarrow 4^2 \equiv 16 \equiv 3$ ± 4

$2^5 \equiv 32 \equiv 6$ $\pmod{13}$

$2^6 \equiv 64 \equiv 12 \rightarrow x = 8 \longrightarrow 8^2 \equiv 64 \equiv 12$ ± 8

$2^7 \equiv 128 \equiv 11$

$2^8 \equiv 256 \equiv 9 \rightarrow x = 3 \rightarrow 3^2 \equiv 9$ ± 3

$2^9 \equiv 512 \equiv 5$

$2^{10} \equiv 1024 \equiv 10 \rightarrow x = 6$ $6^2 \equiv 36 \equiv 10$ ± 6

$2^{11} \equiv 2048 \equiv 7$

$2^{12} \equiv 4096 \equiv 1 \rightarrow x = 1$ $1^2 \equiv 1$ ± 1

(6)

$M \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\quad M^{-1} \equiv \frac{1}{\det M}\begin{pmatrix} +d & -c \\ -b & +a \end{pmatrix}^{T} \equiv$

$\det M \neq 0$

$\mathrm{mcd}(\det M, n) = 1$ $\quad \equiv \frac{1}{\det M}\begin{pmatrix} +d & -b \\ -c & +a \end{pmatrix} \equiv$

$$M^{-1} \equiv \frac{1}{\det M}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

funzione totiente

$\varphi(n)$ è pari $\quad n = \prod_{i=1}^{m} p_i^{e_i}$

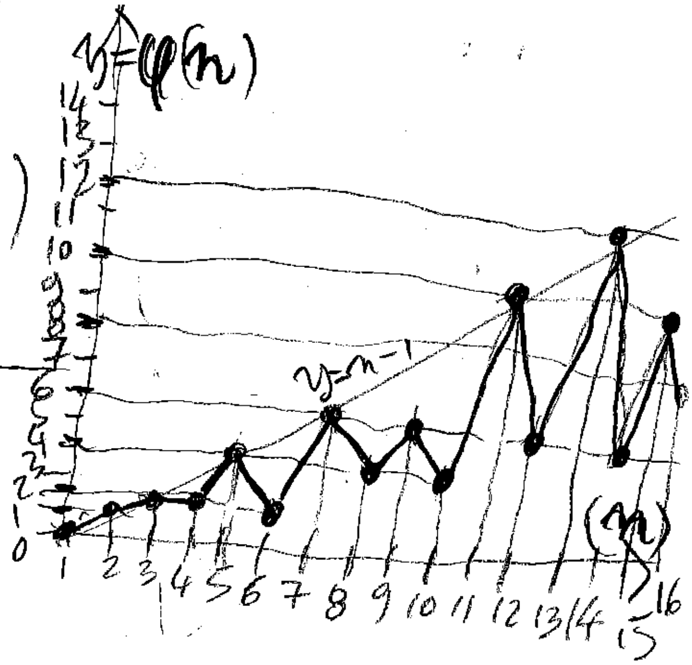
$n > 2$

true

$\varphi(2) = 1$

$$\varphi(n) = \prod_{i=1}^{m} \left(p_i^{e_i} - p_i^{e_i - 1}\right)$$

$$\varphi(n) = n \cdot \prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right)$$



$D \cdot P = P$

$D \cdot D = D$

$P \cdot D = P$

$P \cdot P = P$

se $p_i > 2$

$p_i \equiv D$

$p_i^{e_i} \equiv D$

$\varphi(n)$ è pari per $n > 2$

$\left(p_i^{e_i} - p_i^{e_i - 1}\right)$

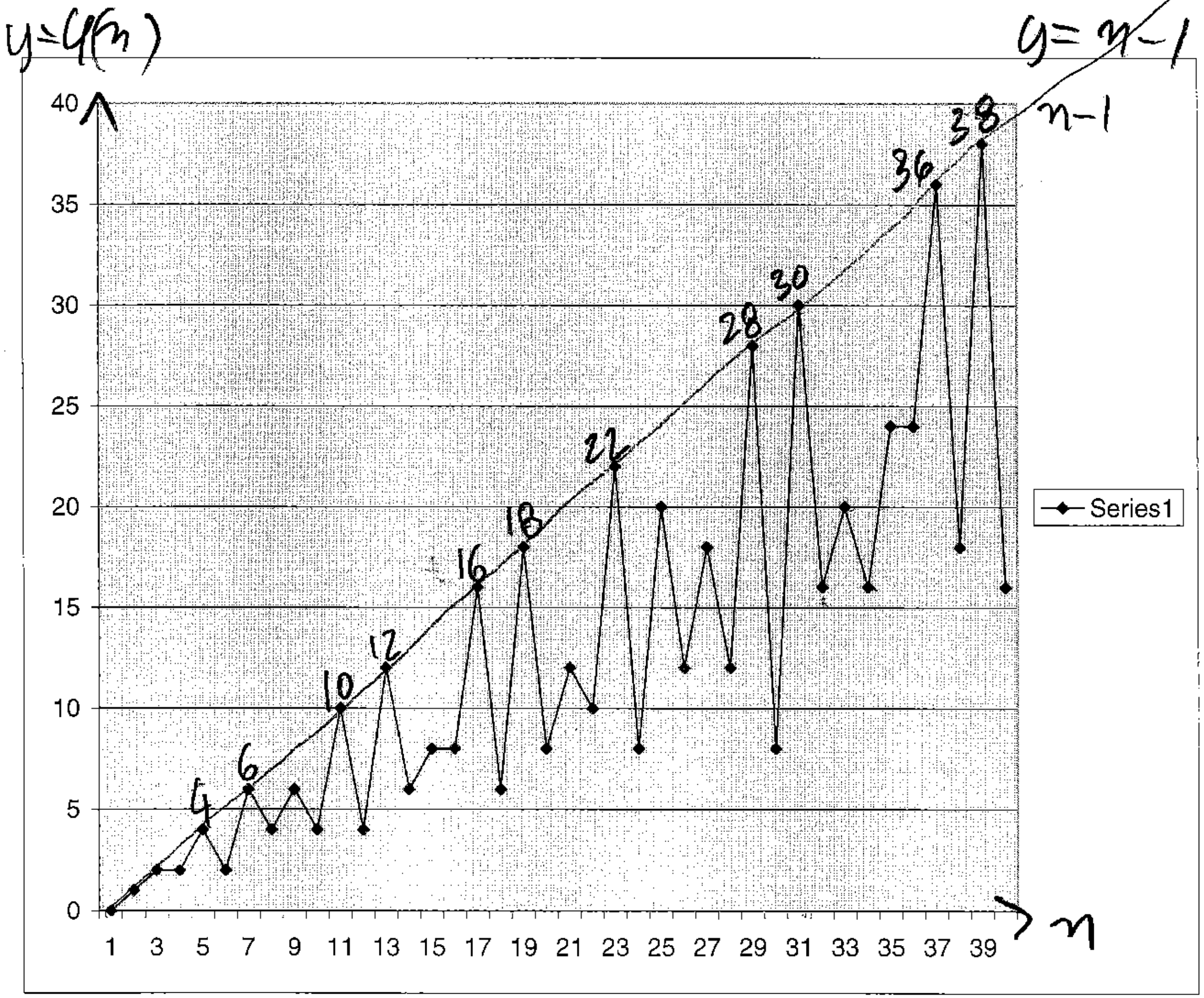
$\varphi(6) = 2$

$6 = 2 \cdot 3$

$1 \cdot 2 = 2$

$\varphi(n)$

n	φ(n)
1	0
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8
31	30
32	16
33	20
34	16
35	24
36	24
37	36
38	18
39	38
40	16



8

per $n>2$ è $\varphi(n) = $ pari $\neq q$ dispari primo $q>2$

$2 \cdot 4 \cdot 6$

$n = 3 \cdot 5 \cdot 7$

$n = 2 \cdot 3 \cdot 5$

$1 \cdot 2 \cdot 4 = 6$

DSA

p dispari

$p-1$ pari ORD

q dispari ORD

	i
$=1$	0
$=\alpha$	1
PIVOT	
$=\alpha^{p-2} \equiv \alpha^{\varphi(n)-1}$	
$=1$	$p-1$

$p-1$, $\varphi(n)$; $\varphi(n)-1$ dispari

	i
$=1$	0
α	1
senza pivot	
α^{q-1}	$q-1$

$q-1$ pari; $q-1$ pari

$1 = \alpha^q$

$\mathbb{Z}_{2^n}$

ord $2^n-1 =$ dispari

$2^n -$ pari

se $2^n-1 =$ primo

$\boxed{\text{campo del primo ordine}}$

$\mathbb{Z}_8 \equiv$

$n = 8 = 2^3$

$2^3-1 = 7 = p$

$\{0,1,2,3,4,5,6,7\}$

$\varphi(8) = 4$

8 elementi con 0 e 1

solo 1, 3, 5, 7 hanno l'inverso

$$\begin{cases} 3^{-1} \equiv 3 \\ 5^{-1} \equiv 5 \\ 7^{-1} \equiv 7 \\ 1^{-1} \equiv 1 \end{cases} \mod 8$$

$3^1 \equiv 3$ ord. 2

$3^2 \equiv 1$

$3^3 \equiv 3$

$3^4 \equiv 1$

6

Quesito 1

Sia dato un alfabeto composto da 256 simboli (byte di 8 bit). Bob decide di utilizzare soltanto i 128 caratteri numerati da 0 a 127, e di impiegare un algoritmo di *'cifratura a catena'* definito dalle equazioni:

$$[1] \qquad Z_i = E_K(P_{i-1} \oplus C_{i-1})$$
$$C_i = E_K(Z_i \oplus P_i); \qquad i=1,2; \; C_0=00000001 \; ; \; P_0=00000001.$$

a) Descrivere l'operazione di cifratura e decifratura che trasforma due simboli in chiaro P_1, P_2 in due simboli cifrati C_1, C_2 e viceversa, sia in forma di schemi a blocchi che con equazioni del tipo [1].

Bob decide inoltre di adottare per la funzione $E_K(x)$ il *sistema di cifratura RSA*. Egli pubblica i parametri:

$$m = 221; \; b = 25$$

e le equazioni [1], inclusi i valori di inizializzazione P_0 e C_0. Bob mantiene il segreto sulla *trapdoor:* $m=p.q=13.17$.

b) Verificare la validità dei parametri *m, b* pubblicati da Bob, secondo RSA, e calcolare il parametro $a=b^{-1}$.
c) Cifrare i simboli $P_1=3$, $P_2=3$ (Alice cifra con la chiave pubblica di Bob).
d) Decifrare i simboli C_1, C_2 risultato della domanda precedente (Bob decifra con la chiave privata).
e) Si supponga che Oscar intercetti C_1, C_2 e conosca le informazioni rese pubbliche da Bob. Determinare la complessità dell'attacco, in termini di numero di tentativi, per i valori numerici di questo esercizio.

N:B: Riportare il calcolo degli esponenziali modulari complessi secondo il metodo adottato (S & M, Euclide esteso, riduzioni esponenziali)

Quesito 2

Bob adotta lo schema di *'firma di ElGamal'* e sceglie $p=97$. Pubblica quindi i valori:

$$p = 97; \; \alpha = 5; \; \beta = ?$$

e tiene segreti i valori:

$$a = 13; \; k = 95.$$

a) Enunciare le ipotesi dello schema di *firma di ElGamal* per i parametri (p, a, k): quanti sono i possibili valori di *P*, di *k* e di *a*?
b) Dire quanti sono gli elementi primitivi $\in Z^*_p$ e verificare che $\alpha=5$ è un elemento primitivo di Z^*_p.
c) Determinare il valore di β.
d) Qual e' la firma del messaggio in chiaro $P=31$?
e) Verificare la firma determinata al punto precedente.
f) Quante firme diverse sono possibili in base ai dati numerici di questo esercizio?

N:B: Riportare il calcolo degli esponenziali modulari complessi secondo il metodo adottato (S & M, Euclide esteso, riduzioni esponenziali)

Quesito 3

Bob adotta lo schema di *'firma di ElGamal'* e sceglie $p=43$. Pubblica quindi i valori:

$$p = 43$$
$$\alpha = 3$$
$$\beta = ?$$

e tiene segreti i valori:

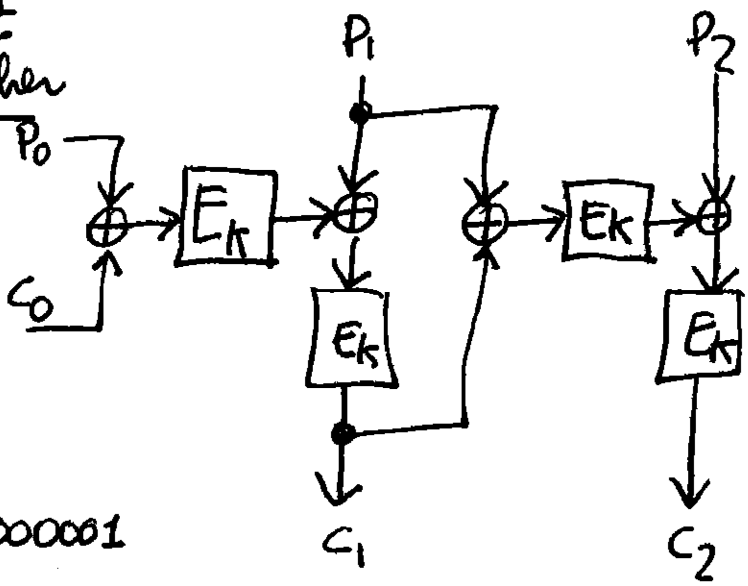
$$a = 10$$
$$k = 11$$

a) Enunciare le ipotesi dello schema di firma di ElGamal per i parametri (p, a, k): quanti sono i possibili valori di *P*, di *k* e di *a*?
b) Dire quanti sono gli elementi primitivi $\in Z^*_p$.
c) Verificare che $\alpha=3$ è un elemento primitivo di Z^*_p.
d) Determinare il valore di β.
e) Qual e' la firma del messaggio in chiaro $P=15$?
f) Verificare la firma determinata al punto precedente.

QUESITO 1

(a) • Cipher

1,5

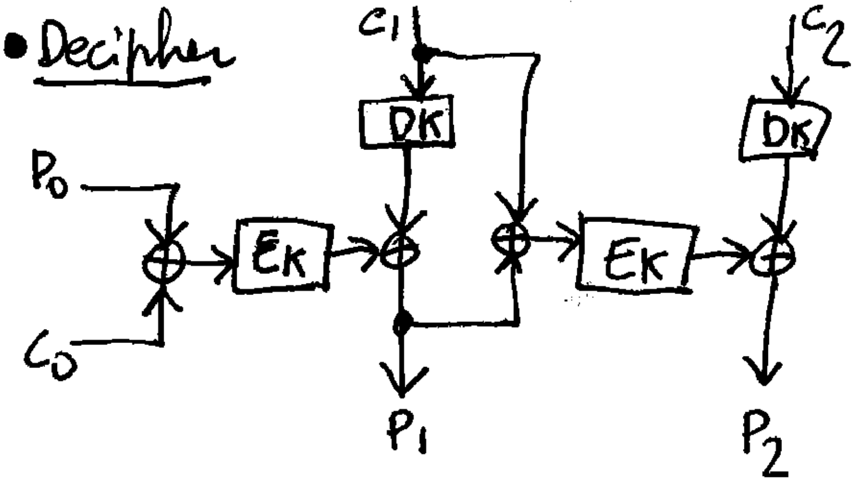


$P_0 \equiv C_0 \equiv 00000001$

$$\begin{cases} Z_1 = E_K(P_0 \oplus C_0) \\ C_1 = E_K(Z_1 \oplus P_1) \end{cases}$$

$$\begin{cases} Z_2 = E_K(P_1 \oplus C_1) \\ C_2 = E_K(Z_2 \oplus P_2) \end{cases}$$

• Decipher



$$\begin{cases} P_1 = E_K(P_0 \oplus C_0) \oplus D_K(C_1) \\ P_2 = D_K(C_2) \oplus E_K(P_1 \oplus C_1) \end{cases}$$

8

RSA

(b) $m = p \cdot q = 13 \times 17 = 221$

2 $\varphi(m) = 12 \times 16 = 192 = 2^6 \times 3$

$\varphi[\varphi(m)] = (2^6 - 2^5)(3-1) = 64$

$b = 25 \perp 192$ ok

$P_1 = 3$; $P_2 = 3$

$a = b^{-1} = 25^{63} \bmod 192 = \left(25^7 \bmod 192\right)^9 \bmod 192 =$

$= 169^9 \bmod 192 = 169 = b^{-1} = a$

(c) $Z_1 = E_K(P_0 \oplus C_0) = 0$

1.5 $C_1 = E_K(0 \oplus 3) = E_K(3) = 3^{25} \bmod 221 =$

$\left(3^5 \bmod 221\right)^5 \bmod 221 =$

$C_1 = 22^5 \bmod 221 = 133$

$Z_2 = E_K(3 \oplus 133) = E_K(134) = 134^{25} \bmod 221 =$

$= \left(134^5 \bmod 221\right)^5 \bmod 221 = 36^5 \bmod 221 = 134$

$C_2 = E_K(134 \oplus 3) = E_K(133) = 133^{25} \bmod 221 =$
$= 3$

$C_1 = 133$; $C_2 = 3$

0000 0011	3	$\oplus$	1000 0110	134	$\oplus$
1000 0101	133		0000 0011	3	
1000 0110 $\Rightarrow$	134		1000 0101	133	

(d) $P_1 = E_K(P_0 \oplus C_0) \oplus D_K(C_1) =$ ③ ⑨

$= 133^{169} \bmod 221 = 3$

1,5 OK

$P_2 = D_K(C_2) \oplus E_K(P_1 \oplus C_1) =$

$= (3^{169} \bmod 221) \oplus E_K(3 \oplus 133) =$

$= 133 \oplus 134 = 3$ OK.

(e) Oscar conosce P_0, C_0 e m: deve individuare p e q. Prende $m = 221$ e incomincia a dividerlo per tutti i numeri primi a cominciare da 3 (1 e 2 sono ovviamente esclusi essendo m dispari)

0,5

221 diviso

3; 5; 7; 11; 13 OK

sono in tutto 5 tentativi: la complessità dell'attacco è 5.

133	$\oplus$	1 0 0 0 0 1 0 1
134		1 0 0 0 0 1 1 0
3		0 0 0 0 0 0 1 1

$133^{169} \bmod 221 = 3$ $\qquad 169 \equiv 10101001$ 4 10

1	133
0	$133^2 \equiv 9$
1	$81 \times 133 \equiv 165$
0	$165^2 \equiv 42$
1	$42^2 \times 133 \equiv 131$
0	$131^2 \equiv 144$
0	$144^2 \equiv 183$
1	$183^2 \times 133 \equiv 3$. OK

$(\bmod 221)$

$3^{169} \bmod 221 = 133$

1	3
0	9
1	$81 \times 3 = 243 = 22$
0	$484 = 42$
1	$42^2 \times 3 \equiv 209$
0	$209^2 \equiv 144$
0	$144^2 \equiv 183$
1	$183^2 \times 3 \equiv \underline{133}$ OK

$(\bmod 221)$

QUESITO 2

(a) p primo $p = 97$ ok

$q = 13$ $q \in \mathbb{Z}_{p-1}$; $a \neq 0$

$k = 95$ $k \in \mathbb{Z}^*_{p-1}$ $mcd(k, p-1) = 1$

$(p-1) = 96$ $k \perp 96$

$95 \perp 96$ ok

$96 = 2^5 \cdot 3 = q_1^5 \cdot q_2$; $(q_1 = 2 ; q_2 = 3)$

Plaintext $\equiv P \in \mathbb{Z}^*_p$

Numero di $q = |\mathbb{Z}_{p-1}| - 1 = p-2 = 95$

Numero di $k = |\mathbb{Z}^*_{p-1}| = \varphi(p-1) = (2^5 - 2^4) \times 2 = 32$

Numero di $P = |\mathbb{Z}^*_p| = \varphi(p) = p-1 = 96$

(b) il numero di elementi primitivi $\in \mathbb{Z}^*_p$ è

$$\varphi(p-1) = 32$$

(c) $5^{\frac{96}{2}} \equiv 5^{48} \mod 97 = 96 \neq 1$ ok

$5^{\frac{96}{3}} \equiv 5^{32} \mod 97 = 35 \neq 1$ ok

$\alpha = 5$ è primitivo $\in \mathbb{Z}^*_p$.

(d) $\beta = \alpha^{a} \bmod p = 5^{13} \bmod 97 = 29$

$$\beta \in \mathbb{Z}_p^*$$

(e) Firma di ElGamal di $P = 31 \in \mathbb{Z}_p^*$

$$SIG(P, k) = (r, s) \in \mathbb{Z}_p^* \cdot \mathbb{Z}_{p-1}$$

$r \in \mathbb{Z}_p^*$

$s \in \mathbb{Z}_{p-1}$

$r = \alpha^{k} \bmod p = 5^{95} \bmod 97 = 39$

$s = [(P - a r)\, k^{-1}] \bmod (p-1)$

$k^{-1} = k^{\varphi(p-1)-1} \bmod (p-1) = 95^{31} \bmod 96 = 95.$

$\left(\text{verifica} \quad k \cdot k^{-1} \equiv 1 \equiv 95^{2} \bmod 96 = \underset{ok}{1}\right)$

$s = [(31 - 13 \cdot 39)95] \bmod 96 = 92$

$$r = 39 \; ; \; s = 92$$

(f) $SIG(31, 95) = (39, 92)$

$VER(P, r, s)$ $\quad \beta^{r} \cdot r^{s} = \alpha^{P} \pmod p$ $\quad \beta^{r} r^{s} \equiv \alpha^{P}$

$$\left.\begin{array}{l} 29^{39} \cdot 39^{92} \bmod 97 = 7 \\ 5^{31} \bmod 97 = 7 \end{array}\right\} \text{ok!}$$

(13)

(g) $\cancel{?}$ r e $\cancel{?}$ s dipendono da a e da k, allora il numero di possibili firme ($\cancel{?}$ r, $\cancel{?}$ s) non è, essendo:

$r \in \mathbb{Z}_p^* \equiv \{1, 2 \ldots 96\}$; $\# r = 96$

$s \in \mathbb{Z}_{p-1} \equiv \{0, 2 \ldots 95\}$; $\# s = 96$

uguale a 96^2, ma è 96×32, e cioè il numero di possibili scelte di k e e di a.

Numero diverse firme $= 96 \times 32 = 3.072$

$s = 0 \quad - \quad P \equiv a r \pmod{p-1}$

noto r e P

posso ricavare $a \equiv r^{-1} P \pmod{p-1}$

se $mcd(r, p-1) = 1$

---

per $s = 0$ per verificare: $\beta^r \equiv \alpha^P$

firma $\{P, (r, s)\}$

se Firma $\{P, (r, 0)\}$

e se $mcd(r, p-1) = 1$ allora ricavo $a \equiv r^{-1} P \pmod{p-1}$

QUESITO 1 del 9-2-2004 (14)

(a) - $p=43$: primo OK

- $1 \leq a \leq p-2$: OK, $1 \leq 10 \leq 41$

- $k \in \mathbb{Z}^*_{p-1}$, $k \perp (p-1)$ // $\perp 42$, OK

• $|a| \equiv p-2 = 41$

• $P \in \mathbb{Z}^*_p \rightarrow |\mathbb{Z}^*_p| = p-1 = 42 \equiv |P|$

• $|k| \equiv |\mathbb{Z}^*_{p-1}| = \varphi(p-1) = \varphi(42) = 1 \times 2 \times 6 = 12 =$

$\equiv \{1, 5, 11, 13, 17, 19, 23, 25, 31, 37, 39, 41\}$

(b)

elementi primitivi di $\mathbb{Z}^*_p$ è

$\varphi(p-1) = 12$

(c) $\alpha \in \mathbb{Z}^*_p \equiv \{1, 2 \ldots 42\}$

$p-1 = 42 = 2 \cdot 3 \cdot 7 = q_1 q_2 q_3$

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

$\alpha = 3$

• $3^{\frac{42}{2}} = 3^{21} \bmod 43 = 42$ OK

• $3^{14} \bmod 43 = 36$ OK

• $3^{6} \bmod 43 = 41$ OK

OK - $\alpha = 3$ è primitivo.

(d) $\beta = \alpha^{a} \bmod p = 3^{10} \bmod 43 = 10$ 15

(e) $SIG(P, k) = (r, s)$

$r = \alpha^{k} \bmod p = 3^{11} \bmod 43 = 30$

$s = \left[(P - a r) k^{-1} \right] \bmod (p-1)$

$k^{-1} \bmod (p-1) = k^{\varphi(p-1)-1} \bmod (p-1) = 11^{11} \bmod 42 = 23$

$s = \left[(15 - 10 \cdot 30) \times 23 \right] \bmod 42 = 39$

(f) $VER(P, r, s) =$ vero se $\boxed{\alpha^{P} \equiv \beta^{r} r^{s} \pmod p}$

$\beta^{r} r^{s} = 22 = \alpha^{P} \bmod p =$

$= 3^{15} \bmod 43 =$

$= 10^{30} \cdot 30^{39} \bmod 43 = 22$ ok

RICORRENZE LFSR

(16)

x^4+x+1

$$X_{i+4} = X_i + X_{i+1}$$

d ≠ primo

$d = 15 = 2^4 - 1$, $k=1$

1010 | 1111 | 0001 | 0011 | 0101

x^4+x^3+1

$c_0=1$
$c_1=0$
$c_2=0$
$c_3=1$

$$X_{i+4} = X_i + X_{i+3}$$

$d=15$

1010 | 1100 | 1000 | 1111 | 0101

è $$X_{i+m} = c_0 X_i + c_1 X_{i+1} + \quad + c_{m-1} X_{i+m-1} \pmod 2$$

$$X^m = c_0 + c_1 X + \dots + c_{m-1} X^{m-1} \pmod 2$$

$$0 = c_0 + c_1 X + \quad + c_{m-1} X^{m} + X^m \bmod 2$$

$$p(x) = x^m + c_{m-1} X^{m-1} + \quad + c_1 X + c_0$$

$x^4+x^3+x^2+x+1$

$$X_{i+4} = X_i + X_{i+1} + X_{i+2} + X_{i+3}$$

sono tutti e tre di grado 4 irriducibili!

Attacco K-P $m=4$ con $2m=8$ bit
ne ho 8 di bit

$$M_4 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$\det M_4 = 1 \times (1+1) + 1(1) = 0 + 1 = 1 \quad \text{OK}$$

allora svolgo la moltiplicazione tra matrici e ho

$$\begin{cases} c_0 + c_2 = 1 & (1) \\ c_1 + c_3 = 1 & (2) \\ c_0 + c_2 + c_3 = 0 & (3) \\ c_1 + c_2 = 0 & (4) \end{cases}$$

sommo (1) $\oplus$ (3) e ottengo $c_3 = 1$

da (2) $c_1 = 0$

da (4) $c_2 = 0$

da (1) $c_0 = 1$ OK!

perché $$M_m = \begin{pmatrix} X_1 & X_2 & \dots & X_m \\ X_2 & X_3 & \dots & X_{m+1} \\ \dots & & \dots & \\ X_m & X_{m+1} & \dots & X_{2m-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{m-1} \end{pmatrix} = \begin{pmatrix} X_{m+1} \\ X_{m+2} \\ \vdots \\ X_{2m} \end{pmatrix}$$

In generale
$$X \cdot X^{m-1} = X^m = c_0 + c_1 X + \dots + c_{m-1} X^{m-1}$$

Moltiplicazione per X

$$M_m = \begin{pmatrix} 0 & 0 & \dots & 0 & c_0 \\ 1 & 0 & \dots & 0 & c_1 \\ \vdots & & \dots & & \vdots \\ 0 & 0 & \dots & 1 & c_{m-1} \end{pmatrix} \begin{pmatrix} \\ \\ \\ \end{pmatrix}$$

$$M_m^{2^m-1} = I = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Matrici Mod m

mod m

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

per poter invertire deve esse

$$(ad-bc) \perp m \qquad mcd[(ad-bc), m] = 1$$

esempio

$$\underline{M} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \bmod 11$$

$$\det \underline{M} = 4-6 = -2 \bmod 11 = 9 \bmod 11$$

$$9^{-1} = \frac{1}{-2} = 9^9 \bmod 11 = 3^{18} \bmod 11$$

$$= 3^{10}\cdot 3^8 \bmod 11 = 3^8 \bmod 11$$

$$= 5 \bmod 11$$

un caso di indifferenza moltiplicazione a destra o a sinistra

$$\underline{M}^{-1} = \frac{-1}{2}\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} \equiv$$

$$M^{-1}M = I = M\cdot M^{-1} \qquad = 5\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} \equiv \begin{pmatrix} 9 & 1 \\ 7 & 5 \end{pmatrix} \bmod 11$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} 9 & 1 \\ 7 & 5 \end{pmatrix} = \begin{pmatrix} 23 & 11 \\ 55 & 23 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 11$$

CIFRARIO DI LESTER HILL

M matrici di cifratura $n \times n$ quadrate

$n \geq 2$ intero

coefficienti mod 26 $\quad c_{ij} \in \mathbb{Z}_{26} \quad m = 26$

$26 = 2 \times 13$

det M deve essere $\quad \varphi(26) = 12$

Condizione di invertibilità $\boxed{\text{mcd}(\det M, m) = 1}$ $\quad \det M \perp 26$

Esempio

$$M = \begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix} \bmod 26$$

$$M^{-1} \equiv \frac{1}{3 \times 7 - 2 \times 5} \begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix} \pmod{26}$$

$\det M = 11 \bmod 26 \qquad 11 \perp 26$ OK

$$M^{-1} \equiv \frac{1}{11} \begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix} \bmod 26 \qquad 11^{-1} \equiv 11^{11} \bmod 26 = 19$$

$$M^{-1} = 19 \begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix} \bmod 26 = \begin{pmatrix} 3 & -12 \\ -17 & 5 \end{pmatrix} \equiv \begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix}$$

$$M^{-1} \cdot M = I = \begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26}$$

$1 = 3 \times 3 + 14 \times 5 = 9 + 70 = 79 \bmod 26 = 1$

$0 = 3 \times 2 + 14 \times 7 = 6 + 98 = 104 \bmod 26 = 0$

$0 = 9 \times 3 + 5 \times 5 = 27 + 25 = 52 \bmod 26 = 0$

$1 = 9 \times 2 + 5 \times 7 = 18 + 35 = 53 = 1 \bmod 26$

OK

allora **messaggi da cifrare**

a n caratteri alla volta

es. $n = 2$ $\quad P \equiv (a, b) \equiv (0, 1) \bmod 26$

cifratura moltiplicazione a destra

$$(0, 1) \times \begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix} = (5, 7) = (f, h) \equiv C$$

a 0
b 1
c 2
d 3
e 4
f 5
g 6
h 7
i

decifratura moltiplicazione a destra

$$(5, 7) \times \begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix} = (5 \times 3 + 7 \times 9, 5 \times 14 + 7 \times 5)$$

$$= (15 + 63 = 78 \bmod 26 = 0, 70 + 35)$$

$$= (0, 1) \underset{OK}{=} P$$

$P \cdot M = C$

$C \cdot M^{-1} = P$

Cifrario affine

$$\begin{cases} C = (aP+b) \bmod m \\ P = a^{-1}(C-b) \bmod m \quad b \in \mathbb{Z}_m \\ \qquad \text{ove } a \perp m \end{cases}$$

Cifrario affine di Hill

$$\begin{cases} (\underline{P} \times \underline{M} + \underline{B}) = \underline{C} \\ (\underline{C} - \underline{B}) \times \underline{M}^{-1} = \underline{P} \end{cases} \pmod m$$

+ moltiplicazione a destra

ove $\det \underline{M} \perp m$ matrice $\underline{M} \Rightarrow (n \times n)$

vettore $\underline{B} \Rightarrow (1 \times n)$

$\underline{P}, \underline{C} \Rightarrow (1 \times n)$ vettori

i coefficienti di $(\underline{M}, \underline{B}, \underline{P}, \underline{C}) \in \mathbb{Z}_m$

la chiave

$$\underline{K} \equiv (\underline{M}, \underline{B})$$

$$n^2 + n = n(1+n)$$

parametri interi $x \in \mathbb{Z}_m$

ma $\det M \perp m$

per cui il numero delle chiavi è ridotto fino al 23% rispetto al teorico

Affine Hill cipher

④ 23

Cifrario di Hill affine $K \equiv (a, b, c, d, e, f)$

$P \equiv (X_1, X_2)$

DIGRAMMI

HEX mod 16

$$(X_1, X_2)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e, f) = (y_1, y_2)$$

$C \equiv (y_1, y_2)$

$P \equiv (A, B)_{hex}$ $m = 16$ $P \equiv (0, 1)$ $\varphi(16) = 8$

$$\underline{M} = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \quad \underline{B} = (2, 3)$$

$$M^{-1} = \frac{1}{5}\begin{pmatrix} 4 & -1 \\ -3 & 2 \end{pmatrix} \equiv \quad \frac{1}{5} \equiv 5^{-1} \equiv 5^{7} \equiv 13 \mod 16$$

$$\equiv 13\begin{pmatrix} 4 & -1 \\ -3 & 2 \end{pmatrix} \equiv \begin{pmatrix} 52 & -13 \\ -39 & 26 \end{pmatrix} \equiv \begin{pmatrix} 4 & 3 \\ 9 & 10 \end{pmatrix} (\mod 16)$$

$$M M^{-1} \equiv \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 4 & 3 \\ 9 & 10 \end{pmatrix} = \begin{pmatrix} 17 & 16 \\ 48 & 49 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod 16$$

OK

Allora: cipher

$$(0, 1)\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} + (2, 3) = (3, 4) + (2, 3) = (5, 7)$$

mod 16

decipher

$$[(5, 7) - (2, 3)]\begin{pmatrix} 4 & 3 \\ 9 & 10 \end{pmatrix} = (3, 4)\begin{pmatrix} 4 & 3 \\ 9 & 10 \end{pmatrix} = (0, 1)$$

mod 16

OK

Altro esempio $m=4$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod 4 \qquad \mathbb{Z}_4 \equiv \{0,1,2,3\}$

$4 = 2^2$

Quante chiavi?

\# teorico $(2^2)^4 = 2^8 = 256$ DEVE ESSERE $(ad-bc) \Rightarrow$ DISPARI!

i numeri $x = ad$, $y = bc$ nelle 16 combinazioni risultano

0	0
1	1
2	2
3	3

(0) 8 ZERI $\equiv 0\times0=0;\ 0\times1=0;\ 0\times2=0;\ 0\times3=0;\ 1\times0;\ 2\times0;\ 3\times0=0;\ \underline{2\times2=4=0 \pmod 4}$

(2) 4 PARI $\equiv 1\times2=2;\ 2\times1=2;\ \underline{2\times3=6\equiv2};\ \underline{3\times2=6\equiv2} \pmod 4$

(1;1; 3;3) 4 DISPARI $\equiv 1\times1=1;\ 1\times3=3;\ 3\times1\equiv3;\ 3\times3\equiv9\equiv1 \pmod 4$

16

Solo 4 su 16 sono dispari. Allora affinché

$$x - y = ad - bc \Rightarrow \text{dispari}$$

ci sono $(4\times12)+(12\times4) = 96$ combinazioni utili

su $\overset{D-D}{(4\times4)} + \overset{D-P}{(4\times12)} + \overset{P\times D}{(12\times4)} + \overset{P-P}{(12\times12)} = 256$ combinazioni complessive.

$\ 16 \quad 48 \quad 48 \quad 144$

per cui $\dfrac{96}{256} = 37{,}5\%$ di copertura dello spazio delle chiavi.

infatti

1, 1
3 3

D-D $\begin{cases} 1-1=0 \\ 1-3=-2=2 \to P \\ 3-1=2\ P \\ 3-3=0 \end{cases}$ NO DISPARI

P-P $\begin{cases} 2-2=0 \\ 2-4=-2=2 \to P \\ 4-2=2 \to P \\ 4-4=0 \end{cases}$ NO DISPARI

D-Z $\begin{cases} 1-0=1 \to D \\ 3-0=3 \to D \end{cases}$ SI

D-P $\begin{cases} 1-2=-1=3 \to D \\ 1-4=-3=1 \to D \\ 3-2=1 \to P \\ 3-4=-1=3 \to D \end{cases}$ SI

Z-D $\begin{cases} -1=3 \to D \\ -3=1 \to D \end{cases}$ SI

P-D $\begin{cases} 2-1=1 \to D \\ 2-3=-1=3 \to D \\ 4-1=3 \to D \\ 4-3=1 \to D \end{cases}$ SI

25

1.5 Cifratura con matrici e attacco Known Plaintext

Esercizio 1.12 *Alice e Bob usano una tecnica di cifratura affine basata sull'aritmetica in $\mathbb{Z}_{10}$. L'algoritmo di cifratura è la espressione:*

$$C_i = P_i \cdot K + B \pmod{10}$$

I vettori riga 1×2 C_i e P_I contengono rispettivamente la coppia i-esima di numeri cifrata e in chiaro, mentre la chiave è composta dalla matrice K e dal vettore B.

La chiave condivisa è:

$$K = \begin{pmatrix} 3 & 7 \\ 2 & 7 \end{pmatrix}$$
$$B = \begin{pmatrix} 4 & 9 \end{pmatrix}$$

1. *Verificare che K sia una chiave valida.*
2. *Cifrare il messaggio:*
$$P = \begin{pmatrix} 6 & 7 & 3 & 9 & 3 & 6 \end{pmatrix}$$
3. *Decifrare il messaggio cifrato.*
4. *Portare un attacco di tipo* known-plaintext *e trovare la chiave (K e B).*

Soluzione Perché K sia valida devono essere rispettate le seguenti condizioni:

$$\begin{cases} \det(K) \neq 0 \\ \gcd(\det(K), 10) = 1 \end{cases}$$

Nel nostro caso abbiamo che $\det(K) = 7$ e le due condizioni sono rispettate.

Scomponiamo il messaggio P in 3 vettori riga:

$$P_1 = \begin{pmatrix} 6 & 7 \end{pmatrix}$$
$$P_2 = \begin{pmatrix} 3 & 9 \end{pmatrix}$$
$$P_3 = \begin{pmatrix} 3 & 6 \end{pmatrix}$$

26

cipher

Calcoliamo i testi cifrati:

$$C_1 = (6 \quad 7)\begin{pmatrix}3 & 7\\ 2 & 7\end{pmatrix} + (4 \quad 9) = (6 \quad 0)$$

$$C_2 = (3 \quad 9)\begin{pmatrix}3 & 7\\ 2 & 7\end{pmatrix} + (4 \quad 9) = (1 \quad 3)$$

$$C_3 = (3 \quad 6)\begin{pmatrix}3 & 7\\ 2 & 7\end{pmatrix} + (4 \quad 9) = (5 \quad 2)$$

Il testo cifrato è quindi:

decipher

$$C = (6 \quad 0 \quad 1 \quad 3 \quad 5 \quad 2)$$

Per decifrare il messaggio occorre invertire la matrice K. L'algoritmo di decifratura è l'espressione:

$$P = CK^{-1} - BK^{-1}$$

$$K^{-1} = \frac{1}{7}\begin{pmatrix}7 & -7\\ -2 & 3\end{pmatrix} \bmod 10$$

L'inverso di 7 (mod 10) si può trovare usando l'algoritmo esteso di Euclide:

r_j	q_j		s_j	t_j
10	–	–	1	0
7	1	–	0	1
3	2	$10 = 1 \cdot 7 + 3$	1	−1
1	3	$7 = 2 \cdot 3 + 1$	−2	3
0	–	$3 = 3 \cdot 1 + 0$	7	−10

L'inverso di 7 è 3, infatti:

$$7 \cdot 3 \bmod 10 = 21 \bmod 10 = 1$$

Quindi:

$$K^{-1} = 3\begin{pmatrix}7 & 3\\ 8 & 3\end{pmatrix} \bmod 10 = \begin{pmatrix}1 & 9\\ 4 & 9\end{pmatrix}$$

$$-BK^{-1} = -(4 \quad 9)\begin{pmatrix}1 & 9\\ 4 & 9\end{pmatrix} = (0 \quad 3)$$

Calcoliamo i testi in chiaro:

$$P_1 = (6 \quad 0)\begin{pmatrix}1 & 9\\ 4 & 9\end{pmatrix} + (0 \quad 3) = (6 \quad 7)$$

$$P_2 = (1 \quad 3)\begin{pmatrix}1 & 9\\ 4 & 9\end{pmatrix} + (0 \quad 3) = (3 \quad 9)$$

$$P_3 = (5 \quad 2)\begin{pmatrix}1 & 9\\ 4 & 9\end{pmatrix} + (0 \quad 3) = (3 \quad 6)$$

27

Attack K-P

X Per scoprire la chiave dato un insieme di coppie P_i, C_i, occorre scrivere un sistema di equazioni:

$$C_1 = P_1K + B \tag{1.1}$$
$$C_2 = P_2K + B \tag{1.2}$$
$$C_3 = P_3K + B \tag{1.3}$$

Sottraendo la (1.3) alla (1.2) e alla (1.1), si ottiene una nuova equazione in cui la costante B non è presente e da cui si può ricavare la matrice K:

$C_1 = (6\ 0)$ $C_2 = (1\ 3)$ $C_3 = (5\ 2)$

$P_1 = (6\ 7)$ $P_2 = (3\ 9)$ $P_3 = (3\ 6)$

$$\begin{pmatrix} C_1 - C_3 \\ C_2 - C_3 \end{pmatrix} = \begin{pmatrix} P_1 - P_3 \\ P_2 - P_3 \end{pmatrix} K \tag{1.4}$$

$$K = \begin{pmatrix} P_1 - P_3 \\ P_2 - P_3 \end{pmatrix}^{-1} \begin{pmatrix} C_1 - C_3 \\ C_2 - C_3 \end{pmatrix} \tag{1.5}$$

$C_1 - C_3$

$[(6-5 \equiv 1)(0-2 \equiv 2)]$

$$K = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 1 & -2 \\ -4 & 1 \end{pmatrix} \tag{1.6}$$

Perché l'attacco abbia successo è necessario che la matrice dei testi in chiaro sia invertibile. Poiché:

$$\det \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix} = 9$$

la matrice è invertibile e non ci sono fattori comuni con 10, pertanto l'inversa è unica:

$$K = \frac{1}{9} \begin{pmatrix} 3 & -1 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ -4 & 1 \end{pmatrix} = 9 \begin{pmatrix} 7 & -7 \\ -12 & 3 \end{pmatrix} = \begin{pmatrix} 63 & -63 \\ -108 & 27 \end{pmatrix}$$

$$K \equiv \begin{pmatrix} 3 & 7 \\ 2 & 7 \end{pmatrix} \pmod{10}$$

Da notare che $9^{-1} \equiv 9 \pmod{10} = 9$, infatti $9 \cdot 9 \bmod 10 = 1$.

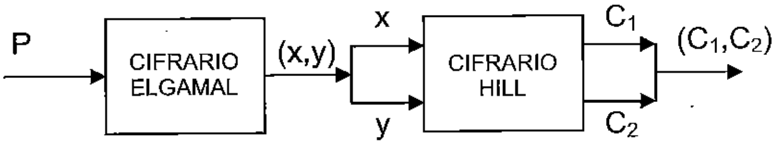
Trovato K si può usare la (1.1) per trovare B:

$$B = C_1 - P_1K = (6 \quad 0) - (2 \quad 1) = (4 \quad -1)$$
$$B \equiv (4 \quad 9) \pmod{10}$$

28

Quesito n.1

La figura mostra il cifrario in cascata usato da Alice e composto da uno stadio di **cifratura di ElGamal** che produce due blocchi (x, y), a fronte di un blocco di testo in chiaro P in ingresso. Il testo cifrato (x, y) viene poi utilizzato come digramma di ingresso a un **cifrario di Hill** a matrice 2x2.



Si assumano operazioni modulo 17: p = 17, e che sia P = 10. Per il cifrario di ElGamal si assuma che sia: $\alpha = 5$ una radice primitiva di Z_p^* e che la chiave privata di Bob sia: a = 11. Bob pubblica p, α, β (chiave pubblica) e Alice sceglie il numero casuale segreto k = 9.

Per il cifrario di Hill, Alice adotta la matrice 2X2 di cifratura segreta: $M = \begin{bmatrix} 5 & 3 \\ 1 & 1 \end{bmatrix}$

1. Enunciare le ipotesi del cifrario di ElGamal per i parametri: p, a, k e P. Quanti sono gli elementi primitivi $\in Z^*_p$?
2. Verificare che $\alpha = 5$ è un elemento primitivo di Z^*_p e determinare il valore di β.
3. Qual e' il testo cifrato (x, y) del messaggio in chiaro P = 10?
4. Qual e' l'ipotesi del cifrario di Hill sulla matrice M? Determinare la matrice M^{-1}.
5. Determinare il testo cifrato (C_1, C_2) all'uscita del cifrario di Hill.
6. In ricezione Bob conosce M^{-1} e decifra il testo cifrato (C_1, C_2).
7. Infine Bob decifra quanto ottenuto al passo precedente con la sua chiave privata.

Riportare il calcolo degli esponenziali modulari complessi (S & M, Euclide esteso, riduzioni esp.)

Quesito 2

L'identità di Alice è certificata da una Trusted Authority, TA, tramite un **Certificato digitale**. Lo scenario crittografico è **basato su RSA** e sul numero intero n = 65, $n = p \cdot q = 5 \cdot 13$. La chiave pubblica della TA è $k_{TA}=11$ mod65, mentre ad Alice viene assegnata l'identità A=34 mod65, e la chiave pubblica $k_A=5$ mod65. Si suppone inoltre che la funzione hash standard z=h(x,y) sia così definita per $x,y,z \in Z_{65}$: $z = (x \oplus \underline{y}) \wedge SL_2(x \vee y)$, ove $y \oplus \underline{y} = 1111111_2$, $\wedge$=and, $\vee$=or.

1. Verificare le ipotesi RSA per k_A e k_{TA}, e trovare le corrispondenti chiavi private.
2. Il certificato di Alice è costituito da tre stringhe binarie, due sono testi in chiaro, mentre la terza è la firma dei due testi in chiaro: qual'è il codice hash dei due testi in chiaro?
3. Com'è composto il certificato di Alice?
4. Che procedura di verifica viene effettuata quando Alice presenta il certificato ad un verificatore?

Riportare il calcolo degli esponenziali modulari complessi (S & M, Euclide esteso, riduzioni esp.)

1) $p = 17$ primo

$a \in \mathbb{Z}_{16}$ $\quad 0 < a \leq 15 \quad$ $a = 11$

$k \in \mathbb{Z}_{16}$ $\quad 0 < k \leq 15 \quad$ $k = 9$

$P \in \mathbb{Z}_{17}$ $\quad 0 < P \leq 16 \quad$ $P = 10$

2) $p-1 = 16 = 2^4 \Rightarrow \varphi(p-1) = 2^4 - 2^3 = 2^3 = 8$

$\alpha = 5 \qquad 5^{\frac{16}{2}} \equiv 5^8 \equiv 16 \not\equiv 1 \pmod{17}$

$\beta \equiv \alpha^a \equiv 5^{11} \equiv 11 \pmod{17} \qquad (p, \alpha, \beta) \equiv (17, 5, 11)$

3) Alice sceglie $k = 9$ e cifra $P = 10 \pmod{17}$

$X = \alpha^k = 5^9 \equiv 12 \pmod{17}$

$Y = \beta^k P \equiv 11^9 \cdot 10 \equiv 9$

e manda $(X = 12,\ Y = 9) \bmod 17$

4) $H = \begin{bmatrix} 5 & 3 \\ 1 & 1 \end{bmatrix} \pmod{17}$ $\quad \det H = 5 - 3 = 2 \neq 0$ e $\operatorname{mcd}(2, 17) = 1$

$H^{-1} = \frac{1}{2} \begin{bmatrix} 1 & -3 \\ -1 & 5 \end{bmatrix} \pmod{17} = \qquad 2^{-1} = 2^{15} \bmod 17 = 9$

$H^{-1} = \begin{bmatrix} 9 & -10 \\ -9 & 11 \end{bmatrix}$ infatti $= \begin{bmatrix} 9 & 7 \\ 8 & 11 \end{bmatrix}$

$69=1 \qquad 68=0$

$45+24 \qquad 35+33$

$$\begin{bmatrix}5 & 3\\1 & 1\end{bmatrix}\begin{bmatrix}9 & 7\\8 & 11\end{bmatrix} \equiv \begin{bmatrix}(5\cdot 9+3\cdot 8) & (5\cdot 7+33)\\ (9+8)=17 = 0 & (7+11) \; 18 = 1\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$$

20

OK

5) cifra (x,y) com Hill

$$(12,9)\begin{pmatrix}5 & 3\\1 & 1\end{pmatrix} \equiv (1,11) = (c_1, c_2) \mod 17$$

6) Decifra Hill

$$(1,11)\begin{pmatrix}9 & 7\\8 & 11\end{pmatrix} = (12,9)$$

decifra ElGamal

$$y\cdot x^{-9} \equiv 9\cdot 12^{-11} \equiv 9\cdot(12^{11})^{-1} \equiv 9\cdot 6^{-1} \equiv 27 \equiv 10 \equiv P$$

$$6^{-1} \equiv 6^{15} \mod 17 \equiv 3$$

OK

CERTIFICATO

Alice e **Trusted Authority**

scenario RSA $\quad m = 5 \times 13 = 65$

$$\varphi(m) = 4 \times 12 = 48 = 2^4 \cdot 3$$

$$\varphi(48) = 2^3 \cdot 2 = 2^4 = 16$$

$$\begin{cases} K_A = 5 \quad (5 \perp \varphi(m)) \\ K_A^{-1} = 5^{-1} = 5^{15} \bmod 48 = 29 \end{cases}$$

identità di A

$A \equiv 34 \bmod 65$

$$\begin{cases} K_{TA} = 11 \quad (11 \perp \varphi(m)) \\ K_{TA}^{-1} = 11^{-1} \equiv 11^{15} \equiv 35 \pmod{48} \end{cases}$$

si suppone che sia definita la funzione hash $\quad z = h(x, y)$ **STANDARD NOTO**

così definita per numeri $x, y, z \in \mathbb{Z}_{65}$

(1) $z = (x \oplus \overline{y}) \wedge SL_2(x \vee y)$

Qual è il Certificato di Alice?

$$C_A = A, K_A, \{h(A, K_A)\}_{K_{TA}^{-1}}$$

$$= 34, 5, \{h(34,5)\}_{K_{TA}^{-1}}$$

ove $z = h(x,y)$

$$x = 34 \equiv 100010$$
$$y = 5 \equiv 000101$$
$$\bar{y} \equiv 111010$$

$$x \oplus \bar{y} \quad \begin{array}{r} 100010 \\ 111010 \\ \hline 011000 \end{array} \oplus \rightarrow \alpha$$

$$x \vee y \quad \begin{array}{r} 100010 \\ 000101 \\ \hline 100111 \end{array} \vee$$

$$SL_2(100111) = \equiv 011110 \rightarrow \beta$$

$$\alpha \wedge \beta \quad \begin{array}{r} 011000 \\ 011110 \\ \hline \end{array} \wedge$$

$$h(x,y) = 011000 = 24$$

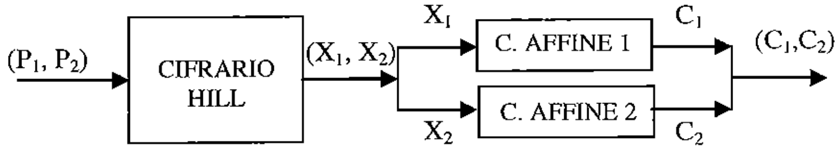
$$C_A = (34, 5, 24^{35}) \bmod 65 \qquad 24^{35} \equiv 19$$

$$C_A \equiv 34, 5, 19 \pmod{65}$$

In ricezione
dunque prende 34 e 5, crea lo standard hash (1)
e può verificare
il terzo numero: $h(34,5) = 19$ ok.

Quesito 2

La figura mostra il cifrario in cascata usato da Alice e composto da uno stadio di *cifratura di Hill* a matrice 2x2 che opera sui digrammi (P1, P2). Per il cifrario di Hill, Alice adotta m=221 e la matrice di cifratura segreta $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, ove A= 3; B= 2; C= 2 e D= 5 (mod221).



I messaggi (X_1, X_2) a loro volta sono inviati in parallelo a due *cifrari affini* $C_1= a_1X_1+ b_1$ e $C_2= a_2X_2+ b_2$, ove $a_1=11$, $b_1=3$, $a_2=3$, e $b_2=2$, (mod221) .

1. Qual e' l'ipotesi del cifrario di Hill sulla matrice M? Determinare la matrice M^{-1} e controllarne la validità.
2. Qual e' il testo cifrato (X_1, X_2) del messaggio in chiaro $P_1=100$ e $P_2=200$?
3. Quali ipotesi sui due cifrari affini? Determinare a_1^{-1} e a_2^{-1} e controllarne la validità.
4. Determinare il testo cifrato (C_1, C_2) all'uscita dei cifrari affini
5. In ricezione Bob conosce M^{-1}, a_1^{-1} e a_2^{-1}, come decifra il testo cifrato (C_1, C_2)?

Riportare il calcolo degli esponenziali modulari complessi (S & M, Euclide esteso, riduzioni esp.)

Quesito 3

Alice e Bob procedono alla mutua identificazione e allo scambio di una chiave segreta condivisa secondo il protocollo semplificato di Needham-Schroeder del tipo Public Key secondo RSA. Nel secondo messaggio viene adottato il fix per l'attacco di Loewe dell'uomo nel mezzo. Alice e Bob adottano m = 187, condividono il segreto pxq= 17x11, e adottano rispettivamente i seguenti identificativi: A= 3, B= 2 (mod187), le seguenti chiavi pubbliche: $K_A = 7$, $K_B = 3$ (mod187) e i seguenti numeri casuali: $N_A= 11$ e $N_B = 13$ (mod187). La chiave di sessione scambiata risulta $K_{AB} = N_A \oplus N_B$.

1. Verificare la validità dei parametri m, K_A , K_B pubblicati, e dei parametri A, B, N_A, N_B, secondo RSA, e determinare K_A^{-1} e K_B^{-1}.
2. Qual e' il messaggio M1 inviato da Alice?
3. Come decifra Bob il messaggio M1?
4. Qual è il messaggio M2 inviato da Bob?
5. Come decifra Alice il messaggio M2?
6. Qual è il messaggio M3 inviato da Alice?
7. Come decifra Bob il messaggio M3?

Riportare il calcolo degli esponenziali modulari complessi (S & M, Euclide esteso, riduzioni esp.)

33

Quesito 2

1. $m = 221 = 13 \times 17$

$$M \equiv \begin{pmatrix} 3 & 2 \\ 2 & 5 \end{pmatrix} \equiv \begin{pmatrix} A & B \\ C & D \end{pmatrix} \pmod{221}$$

$$\det M \in \mathbb{Z}^*_{221} \qquad |\mathbb{Z}^*_{221}| = \varphi(221) = 12 \times 16 = 192$$

$\det M = 11 \perp 221$ ok!

$$M^{-1} \equiv 11^{-1} \begin{pmatrix} 5 & -2 \\ -2 & 3 \end{pmatrix} \equiv$$

ma $11^{-1} = 11^{191} \bmod 221 = 201$

verifica $201 \times 11 = 2211 \bmod 221 = 1$ ok!

$$M^{-1} \equiv 201 \begin{pmatrix} 5 & -2 \\ -2 & 3 \end{pmatrix} \equiv \begin{pmatrix} 1005 & -402 \\ -402 & 603 \end{pmatrix} \equiv$$

$$\equiv \begin{pmatrix} 121 & 40 \\ 40 & 161 \end{pmatrix} \pmod{221}$$

$$M \cdot M^{-1} \equiv \begin{pmatrix} 3 & 2 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 121 & 40 \\ 40 & 161 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{221}$$

infatti

$3 \times 121 + 2 \times 40 = 363 + 80 = 443 \equiv 1$

$3 \times 40 + 2 \times 161 = 120 + 322 = 442 \equiv 0$

$2 \times 121 + 5 \times 40 \equiv 0$

$2 \times 40 + 5 \times 161 \equiv 1$ ok $\pmod{221}$

2. $P_1=100$, $P_2=200$

$$(X_1,X_2)\equiv(100,200)\begin{pmatrix}3&2\\2&5\end{pmatrix}\equiv\left[(300+400),(200+1000)\right]\equiv$$

$$\equiv(700,1200)\equiv(37,95)\pmod{221}$$

$$\begin{matrix}X_1\equiv37\\X_2\equiv95\end{matrix}\pmod{221}$$

3. Cifrario affine

$$\begin{matrix}C=aP+b\\P=a^{-1}(C-b)\end{matrix}\pmod{m}$$

ove $b\in\mathbb{Z}_m$ e $a\in\mathbb{Z}_m^*$ $(a\perp m)$

$a_1=11\perp221$ ok $\quad b_1=3\in\mathbb{Z}_{221}$ ok

$a_2=3\perp221$ $\quad b_2=2\in\mathbb{Z}_{221}$ ok

$$a_1^{-1}\equiv11^{\varphi(m)-1}\equiv11^{191}\equiv201\pmod{221}\qquad\varphi(221)=192$$

$201\times11\equiv1$ ok!

$$a_2^{-1}\equiv3^{-1}\equiv3^{191}\equiv74\pmod{221}$$

$74\times3\equiv222\equiv1$ ok!

ict CONSULTING

4. $C_1 \equiv (11 \times 37 + 3) \equiv 410 \equiv 189$

$C_2 \equiv (3 \times 95 + 2) \equiv 287 \equiv 66 \pmod{221}$

5. $$\begin{cases} X_1 \equiv a_1^{-1}(C_1 - b_1) \equiv 201(189-3) \equiv 37.386 \equiv 37 \\ X_2 \equiv a_2^{-1}(C_2 - b_2) \equiv 74(66-2) \equiv 4.736 \equiv 95 \end{cases} \pmod{221}$$

ok!

$$(37, 95)\begin{pmatrix} 121 & 40 \\ 40 & 161 \end{pmatrix} \equiv$$

$$\left[(37 \times 121 + 95 \times 40), (37 \times 40 + 95 \times 161)\right] \equiv$$

$$\equiv (8.277, 16.775) \equiv (100, 200)$$

OK!

COMO

Quesito 3

(37)

NPSK $m = 17 \times 11 = 187$ $p = 17$, $q = 11$

$\varphi(m) = 16 \cdot 10 = 160 = 2^5 \cdot 5$

$\varphi[\varphi(m)] = \varphi(160) = (2^5 - 2^4) \cdot 4 = 16 \times 4 = 64 = 2^6$

		Alice	Bob	mod
	ID	$A = 3$	$B = 2$	187
Pubblico	chiave	$K_A = 7$	$K_B = 3$	64
Privato	chiave	$K_A^{-1} = 23$	$K_B^{-1} = 107$	64
	Nonce	$N_A = 11$	$N_B = 13$	187

1\. $K_A = 7 \perp \varphi(m)$; $K_A^{-1} = 7^{63} \bmod 160 = 23 \perp \varphi(m)$

$K_B = 3 \perp \varphi(m)$; $K_B^{-1} = 3^{63} \bmod 160 = 107 \perp \varphi(m)$

$A, B, N_A, N_B \in \mathbb{Z}_{186}$ $\mathbb{Z}_{m-1}$ $\mathbb{Z}_{186}$

2\. • M1. $A \to B$: $(N_A^{K_B}, A^{K_B}) \equiv (11^3, 3^3) \equiv (22, 27) \pmod{187}$

3\. Bob decifra $(22^{107}, 27^{107}) \equiv (11, 3) \pmod{187}$

$N_A = 11$
Alice $= 3$

$K_{AB} = N_A \oplus N_B$ ha la chiave!

4\. • M2. $B \to A$ $(N_A^{K_A}, N_B^{K_A}, B^{K_A}) \equiv (11^7, 13^7, 2^7) \equiv (88, 106, 128)$ $\pmod{187}$

5. Alice decifra $\left(88^{23}, 106^{23}, 128^{23}\right) \equiv (11, 13, 2)$ (mod 187)

$N_A = 11$; $N_B = 13$; Bob $= 2$

$K_{AB} = N_A \oplus N_B = 6$ $\quad 11 \oplus 13 = \begin{array}{r} 1011 \\ 1101 \\ \hline 0110 \end{array} = 6$

ho la conferma dell'identità di Bob e ho la chiave (mod 187)

6 M3. A → B:

$$N_B^3 \equiv 13^3 \equiv 140 \pmod{187} \qquad K_{AB} \in \mathbb{Z}_{186}$$

7 Bob decifra $140^{107} \equiv 13 \equiv N_B \pmod{187}$

e conferma l'identità di Alice