(1)

CIFRARIO AFFINE

$$\begin{cases} C \equiv aP + b \pmod{n} \\ P \equiv a^{-1}(C-b) \pmod{n} \end{cases}$$

ove $a \in \mathbb{Z}_n^*$; $mcd(a,n) = 1$ e $a^{-1} \equiv a^{\varphi(n)-1} \pmod{n}$

$P, C, b \in \mathbb{Z}_n$

CIFRARIO DI HILL

$$\underset{\sim}{C} \equiv \underset{\sim}{P} \cdot \underset{\sim}{H} \pmod{n}$$

ove $\underset{\sim}{C}$ e $\underset{\sim}{P}$ sono vettori $[1 \times d]$ e $\underset{\sim}{H}$ è la matrice $[d \times d]$

i coefficienti dei vettori $\{C_1, C_2 \cdots C_d\} \equiv \underset{\sim}{C}$

$\{P_1, P_2 \quad P_d\} \equiv \underset{\sim}{P}$

e della matrice $\begin{bmatrix} h_{11} & h_{12} \cdots & h_{1d} \\ h_{d1} & h_{d2} & h_{dd} \end{bmatrix} \equiv \underset{\sim}{H}$

sono residui $\in \mathbb{Z}_n$

ove

$mcd(\det \underset{\sim}{H}, n) = 1$ e cioè $\det \underset{\sim}{H} \in \mathbb{Z}_n^*$

e implicitamente si ha che $\det \underset{\sim}{H} \neq 0$.

$(mcd(0,n) = n)$

CIFRARIO A CATENA

Ricorrenza generatrice

$$X_{i+m} = X_{i+m-1} \cdot C_{m-1} + \ldots X_{i+1} c_1 + X_i c_0 \pmod{2}$$

periodo sequenza $= d$

$d = \frac{2^m - 1}{k}$ se il polinomio monico di grado m: $f(X) = X^m + c_{m-1} X^{m-1} + \quad + c_1 X + c_0 \pmod{2}$ è irriducibile

se poi $2^m - 1 =$ primo $\rightarrow d = 2^m - 1$.

CRITTOSISTEMA

RSA

$n = p \cdot q$ p e q primi

$\boxed{\begin{array}{l} \text{BOB} \\ K_B = e \\ K_B^{-1} = d \end{array}}$

A→B $\left\{ \begin{array}{l} C = P^e \bmod n \\ P = C^d \bmod n \end{array} \right.$ Bob decifra

$P, C \in \mathbb{Z}_n$

$e, d \in \mathbb{Z}^*_{\varphi(n)}$

$\mathrm{mcd}[(e,d), \varphi(n)] = 1$

ove

$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$

e cioè $d \equiv e^{-1} \equiv e^{\varphi[\varphi(n)]-1} \pmod{\varphi(n)}$

Protocollo di Shamir a tre passi

$\boxed{\begin{array}{l} \text{Alice} \\ K_A \text{ e } K_A^{-1} \\ \text{Bob} \\ K_B \text{ e } K_B^{-1} \end{array}}$

Alice cifra con K_A

M1. $A \to B: E_{K_A}(P)$

Bob cifra con K_B

M2. $B \to A: E_{K_B}[E_{K_A}(P)] \equiv E_{K_A}[E_{K_B}(P)]$

Alice decifra e manda

M3. $A \to B: E_{K_B}(P)$

Bob decifra e ottiene P.

$\boxed{\begin{array}{l} E_K(\cdot) \text{ può essere} \\ \text{RSA o altri} \\ \text{algoritmi} \end{array}}$

FIRMA RSA

$P \equiv$ hash di M

Alice
$e = K_A$
$d = K_A^{-1}$

$$SIG(P) \equiv P^d \pmod n$$

Alice manda $\{P, SIG(P)\}$

chiunque riceve e conosce K_A esegue la verifica

calcola $VER[SIG(P)] = (P^d)^e \equiv P \bmod n$

e confronta con P ricevuto $\left\{ \begin{array}{l} \text{se i due } P \text{ sono} \\ \text{uguali OK!} \\ \text{Altrimenti si rifiuta!} \end{array} \right.$

DIFFIE-HELLMAN

p primo tale che $p-1 = 2 \cdot q$ con q primo

$\alpha \in \mathbb{Z}_p^*$ è elemento primitivo di $\mathbb{Z}_p^*$

chiave segreta di Alice a_A

$1 \leq a_A, a_B \leq p-2$

chiave segreta di Bob a_B

$a_A, a_B \in \mathbb{Z}_{p-1}$

$a_A, a_A \neq 0$

M1. $A \to B$: $\alpha^{a_A} \pmod p$

M2. $B \to A$: α^{a_B} (mod p

Bob calcola $K_{AB} \equiv (\alpha^{a_A})^{a_B} \equiv \alpha^{a_A a_B} \pmod p$

Alice calcola K_{AB} $(\alpha^{a_B})^{a_A} \equiv \alpha^{a_A a_B} \pmod p$

$K_{AB} \equiv$ chiave segreta condivisa tra Bob e Alice

CRITTOSISTEMA DI ELGAMAL

p primo; α elemento primitivo di $\mathbb{Z}_p^*$: $\alpha \in \mathbb{Z}_p^*$

$P \in \mathbb{Z}_p^*$; $1 \leq P \leq p-1$

- chiave privata $a \in \mathbb{Z}_{p-1}$; $a \neq 0$ $\quad 1 \leq a \leq p-2$

- chiave pubblica $\beta \equiv \alpha^a \pmod p$ $\quad \beta \in \mathbb{Z}_p^*$

BOB

PUBBLICO $(p; \alpha; \beta)$; PRIVATO(a)

segue $\rightarrow$

Alice vuole cifrare P per Bob.
Sceglie un nonce $k \in \mathbb{Z}_{p-1}$; $k \neq 0$ $\quad 1 \leq k \leq p-2$

e manda $\quad CIP(P, k) = (r, t)$

$$M1.\ A \to B: (r, t) \qquad r, t \in \mathbb{Z}_p^*$$

ove
$$\begin{cases} r \equiv \alpha^k \pmod p \\ t \equiv \beta^k P \pmod p \end{cases}$$

Bob decifra
$$t r^{-a} \equiv P \pmod p$$

FIRMA DI ELGAMAL

---

p primo; α elemento primitivo $\alpha \in \mathbb{Z}_p^*$
$P \in \mathbb{Z}_p$; $0 \leq P \leq p-1$
- chiave segreta $a \in \mathbb{Z}_{p-1}$; $a \neq 0$ $\quad 1 \leq a \leq p-2$
- chiave pubblica $\quad \beta \equiv \alpha^a \pmod p \quad \beta \in \mathbb{Z}_p^*$

<u>Alice</u> PUBBLICO $(p; \alpha; \beta)$; PRIVATO (a)
sceglie un nonce $k \in \mathbb{Z}_{p-1}^*$ $\quad \mathrm{mcd}(k, p-1) = 1$
$$SIG(P, k) = (r, s)$$
ove
$$\begin{cases} r \equiv \alpha^k \pmod p ; & r \in \mathbb{Z}_p^* \\ s \equiv k^{-1}(P - ar) \pmod{p-1} ; & s \in \mathbb{Z}_{p-1} \end{cases}$$

segue →

ove $k^{-1} = k^{\varphi(p-1)-1} \pmod{p-1}$; $k^{-1} \in \mathbb{Z}^*_{p-1}$ (5)

Alice manda $\{ P, (r,s) \}$

chiunque conosca
la chiave pubblica di Alice $(p; \alpha; \beta)$
esegue la verifica e calcola se

$$\boxed{\beta^r \cdot r^s \equiv \alpha^P \pmod p}$$

se l'uguaglianza è verificata la firma è valida, altrimenti è forgiata.

FIRMA DSA

p primo tale che
$p - 1 = k \cdot q$
k intero
q primo
e cioè $q | p-1$

g radice primitiva $\in \mathbb{Z}^*_p$

$\alpha \equiv g^{\frac{p-1}{q}} \pmod p$

tale che
$\alpha^q \equiv 1 \pmod p$

- chiave segreta
$a \in \mathbb{Z}^*_q$; $1 \leq a \leq q-1$

- chiave pubblica
$\beta \equiv \alpha^a \pmod p$

Alice
PUBBLICO (p, q, α, β)
PRIVATO (a)

Alice sceglie un nonce $k \in \mathbb{Z}^*_q$ $1 \leq k \leq q-1$

Calcola $\begin{cases} r \equiv (\alpha^k \bmod p) \pmod q \\ s \equiv k^{-1}(P + ar) \pmod q \end{cases}$ $r, s \in \mathbb{Z}^*_q$

(1) vedi pag 6

per firmare $P \in \mathbb{Z}_q$

e ove $r \in \mathbb{Z}_q^*$ e $s \in \mathbb{Z}_q^*$

mentre $k^{-1} \equiv k^{q-2} \pmod q$

$$SIG(P, k) \equiv \{P, (r, s)\}$$

Per la verifica

$$\begin{cases} u_1 \equiv s^{-1} P \pmod q \\ u_2 \equiv s^{-1} r \pmod q \end{cases}$$

la firma è valida se

$$\boxed{(\alpha^{u_1} \beta^{u_2} \bmod p) \bmod q = r}$$

essendo: $s^{-1} \equiv s^{q-2} \pmod q$

---

(1) in realtà $s \in \mathbb{Z}_q$ e cioè se

$$(P + ar) = k\, q$$

allora $s \equiv (P + ar) \equiv 0 \pmod q$

e allora s^{-1} non esiste e <u>va provato un altro k.</u>

quando:

$$\underline{P \equiv -ar \pmod q}$$

---

ricordo che $r = f(k) = (\alpha^k \bmod p) \bmod q$

$$a \bmod m = a - \left\lfloor \frac{a}{m} \right\rfloor m = r \qquad \left\lfloor \frac{a}{m} \right\rfloor = k$$

7

$$363 \bmod 17 = 363 - \left\lfloor \frac{363}{17} \right\rfloor 17 =$$

$$363 - 21 \times 17 = 363 - 357 = 6 \qquad \frac{363}{17} = 21{,}35\ldots$$

Remainder!

S&M

$$3^{13} \bmod 17 \equiv 12$$

$13 \equiv 1101$

	1	
1	$1^2 \cdot 3 \equiv 3$	
1	$3^2 \cdot 3 \equiv 10$	(mod 17)
0	$100 \equiv 15$	
1	$15^2 \cdot 3 \equiv 675 \equiv \underline{12}$	

$$3^{15} \bmod 17 \equiv 6$$

$15 \equiv 1111$

1	3	
1	10	
1	$15 \cdot 3 \equiv 45 \equiv 11$	(mod 17)
1	$11^2 \cdot 3 \equiv 363 \equiv \underline{6}$	

AEE $8^{-1} = 8^{15} \bmod 17$ $\qquad a = 17 \quad b = 8 \qquad a > b \qquad a = r_0 \quad b = r_1$

$b^{-1} \bmod a$ $(a > b)$

$r_0 = q_1 r_1 + r_2$	t	s
	$t_0 = 0$	$s_0 = 1$
	$t_1 = 1$	$s_1 = 0$
$17 = 2 \cdot 8 + 1$	$t_2 = -2$	$s_2 = 1$
$8 = 8 \cdot 1 + 0$	$t_3 = 17$	$s_3 = -8$

$n = 2$

$r_1 = q_2 r_2 + 0$

(1) $t_2 = b^{-1} = -2 = 15$ $\qquad 8 \cdot 15 \equiv 1 \pmod{17}$ ok

$17^{-1} \bmod 8 = 1^{-1} \equiv 1 \pmod 8$

(2) $s_2 = 1$

(3) $t_2 \cdot s_3 - s_2 t_3 = (-1)^{n+1}$ $\qquad n = 2$

$(-2)(-8) - 1 \times 17 = -16 - 17 = -1$ ok

(4) $s_i r_0 + t_i r_1 = r_i \qquad 0 \leq i \leq n$

in particolare

$n = 2 \qquad s_n \underline{a} + t_n \underline{b} = r_n$

$s_2 \cdot 17 + t_2 8 = r_2$

$1 \cdot 17 + (-2) 8 = 1$ ok

Studio di $\mathbb{Z}_{17}^* \equiv \{1, 2, 3 \ldots 15, 16\}$

$p = 17$ $\qquad p \equiv 1 \bmod 4$

$p - 1 = 2^4 = 16$

Radice primitiva

$2^{\frac{16}{2}} \equiv 2^8 \equiv 256 \bmod 17 \equiv 1$ No

$3^8 \equiv 16 \equiv -1 \not\equiv 1$ OK

$3^1 \equiv 3$

$3^2 \equiv 9$ $\qquad$ mod 17

$3^3 \equiv 27 \equiv 10$

$3^4 \equiv 13$

$3^5 \equiv 5$ $\qquad$ inversi

$3^6 \equiv 15$

$3^7 \equiv 11$

PIVOT $3^8 \equiv 16 \equiv 16^{-1}$ inverso di se stesso

$3^9 \equiv 14$

$3^{10} \equiv 8$

$3^{11} \equiv 7$

$3^{12} \equiv 4$

$3^{13} \equiv 12$

$3^{14} \equiv 2$

$3^{15} \equiv 6$

$3^{16} \equiv 1$ $\qquad$ Unità

$3^i : 1 \leq i \leq p-1$

- Radici primitive

$\text{mcd}(i, 16) = 1$

$3^1 \equiv 3;\ 3^3 \equiv 10;\ 3^5 \equiv 5$

$3^7 \equiv 11$ e i loro inversi

$3^{15} \equiv 6;\ 3^{13} \equiv 12$

$3^{11} \equiv 7$ e $3^9 \equiv 14$

- Residui quadratici

indici i pari $= \frac{p-1}{2} = 8$

$RQ = \{3^2, 3^4; 3^6, 3^8; 3^{10}, 3^{12}, 3^{14}, 3^{16} \equiv 1\}$

Radici $= \{\pm 3, \pm 9, \pm 10, \pm 13, \pm 5, \pm 15, \pm 11, \pm 1\}$

- Ordine elementi

— Radici primitive ordine $16 = p - 1$

cantolino
- ordine 2: 3^8
- ordine 4: $3^4; 3^{12}$
- ordine 8: $3^2; 3^{14}; 3^6; 3^{10}$

Logaritmi discreti $\quad a^x \equiv b \pmod{17}$ (11)

$$3^x \equiv b \pmod{17}$$

ha sempre soluzione perché $3 \equiv \alpha$ elemento generatore genera tutti gli elementi del campo $b \in \mathbb{Z}_{17}^*$ per valori di $x \bmod 17 \equiv \{1, 2 \ldots 16\}$

Supponiamo che

$$3^{14} \equiv 2 \pmod{17}$$

allora $14 \equiv L_3(2) \pmod{17}$

supponiamo che se $a^x \equiv a^y \pmod{p}$ allora $x \equiv y \pmod{p-1}$ per $a \in \mathbb{Z}_p^*$

residui quadratici

$$a^2 \equiv b \pmod{17}$$

$$(\pm a)^2 \equiv b \pmod{17}$$

essendo $b \in \mathbb{Z}_{17}^*$

esiste $\pm a$? $\pm a$ esiste solo se b è un residuo quadratico

es. $\quad a^2 \equiv 8 \pmod{17}$

vero per $\underline{a \equiv 5}$ e $\underline{a \equiv -5}$ $\quad a \equiv \pm 5 \bmod 17$

OH

$5 \equiv 3^5 \quad 5^2 \equiv 3^{10} \equiv 8$

(12)

$n = pq$

RSA

$$\begin{cases} C = P^e \bmod n \\ P = C^d \bmod n = P^{ed} \bmod n \end{cases}$$

$$e \cdot d \equiv 1 \bmod \varphi(n)$$

$$d \equiv e^{-1} \equiv e^{\varphi[\varphi(n)]-1} \pmod{\varphi(n)}$$

---

primapu base

$$a^x \equiv a^y \pmod n$$

se $\mathrm{mcd}(a, n) = 1$: $a \in \mathbb{Z}_n^*$

allora

$$x \equiv y \pmod{\varphi(n)}$$

---

se $n = 15 = 3 \cdot 5$

e $a \in \mathbb{Z}_{15}^*$ esempio $a = 2$: $\mathrm{mcd}(2, 15) = 1$

gli esponenti da dare ad a (mod n) forniscono lo stesso risultato mod $\varphi(n)$.

$n = p \cdot q$

esempio $\quad n = 15 = 3 \cdot 5$

$\mathbb{Z}_n = \mathbb{Z}_{15}$ $\qquad \varphi(n) = 8 = 2^3$

$\{0, 1, 2 \dots, 13, 14\}$ $\qquad \varphi[\varphi(n)] = 2^2 = 4$

ora

$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ $\qquad |\mathbb{Z}_{15}^*| = \varphi(15) = 8$

gli 8 elementi hanno l'inverso moltiplicativo

infatti per ogni residuo

$a \in \mathbb{Z}_{15}^*$: $\operatorname{mcd}(a, 15) = 1$

si ha $\qquad a^{\varphi(15)} \equiv 1 \pmod{15}$

$$a^8 \equiv 1 \pmod{15}$$

per cui

$$a^{-1} \equiv a^7 \bmod 15 \equiv a^{\varphi(15)-1} \bmod 15$$

RSA

BOB PUBBLICA

$n = 253$

$e_B = 13$

Alice invia

$c \equiv 58 \pmod{253}$

quale lettera dell'alfabeto italiano $(A \div Z) \equiv (0 \div 20)$ di 21 lettere ha inviato?

$n = 253 = 23 \cdot 11$

$\varphi(n) = 22 \times 10 = 220 = 2^2 \cdot 5 \cdot 11$

$\varphi[\varphi(n)] = \varphi(220) = 2 \cdot 4 \cdot 10 = 80$

$e_B = 13 \quad \text{mcd}(13, 220) = 1$ OK!

$e_B^{-1} = d_B = 13^{-1} \bmod 220 = 13^{79} \bmod 220 = 17$

Euclide Esteso

		0	1
		1	0
1	$220 = 16 \cdot 13 + 12$	-16	1
2	$13 = 1 \cdot 12 + 1$	17	-1
$n=3$	$12 = 12 \cdot 1 + 0$	$-16-17 \cdot 12 = -220$	13

$\varphi(n) = 220$

$e_B = 13 \qquad e_B^{-1} = t_3 = 17$

verifica $17 \times 13 = 221 \equiv 1 \pmod{220}$

allora $P = c^{17} \bmod 253 = 58^{17} \bmod 253 = 9$

infatti $9^{13} \bmod 253 = C = 58$

Esempio

$$58^{17} \equiv \quad (\bmod 253)$$

$17 \equiv 10001$

	1
1	$1^2 \cdot 58 \equiv 58$
0	$58^2 \equiv 3.364 \equiv 75$
0	$75^2 \equiv 59$
0	$59^2 \equiv 192$
1	$192^2 \cdot 58 \equiv \underline{9}$

mod 253

RSA $n = 11 \cdot 13 = 143$

$\varphi(n) = 10 \cdot 12 = \underline{120} = 2^3 \cdot 5 \cdot 3$

$\varphi[\varphi(n)] = \varphi(120) = 2^2 \cdot 2^2 \cdot 2 = 2^5 = \underline{32}$

PUBBLICA $e = 7$ $\quad d = e^{-1} = 7^{31} \bmod 120 = 103$

$7 \cdot 103 \equiv 1 \bmod 120$

$\mathrm{mcd}(e, 120) = 1$

• attacco di fattorizzazione (forza bruta)

provo da $\overset{\text{ovvi}}{(1,2)}$ 3 a $\lfloor \sqrt{n} \rfloor \equiv \lfloor \sqrt{143} \rfloor = 11$ dividendo per:

$(1,2)\ 3, 5, 7, 11$ $\quad$ 4 colpi trovo $n = 11 \cdot 13$

• attacco del piccolo plaintext

es. $P \equiv 6$; $C = 6^e \equiv 6^7 \bmod 143 \equiv 85 \pmod{143}$

	x	$85\, x^{-7}$	y^7	y	(mod 143)
(avvio)	1	85	1	1	(ovvie)
x^*	2	$85 \cdot 2^{120-7} \equiv 85 \cdot 19 \equiv 42$	$2^7 \equiv 128$	2	
	3	$85 \cdot 3^{113} \equiv 85 \cdot \equiv 126$	$3^7 \equiv 42$	3	y^* (mod 143)

Alla 2da prova l'ho beccato!

$P = x^* y^* = 2 \cdot 3 = 6$ ok!

Esempio $\quad \varphi(n)=8 \quad \varphi[\varphi(n)]=4$

$n = 3 \cdot 5 = 15$

$e = 3 \quad d = 3^{-1} = 3^3 \bmod 8 = 3$

$3 \times 3 \equiv 1 \bmod 8$

ok

$e, d \in \mathbb{Z}^*_{\varphi(n)}$

$mcd[e, d, \varphi(n)] = 1$

$e, d \in \mathbb{Z}^*_8 = \{1, 3, 5, 7\}$

$e=3 \quad d=3$

$e=5 \quad d=5$

$e=7 \quad d=7$

se tolgo $e=1$, $d=1$

$$\left| \mathbb{Z}^*_{\varphi(n)} \right| = \varphi[\varphi(n)] = 4 = \left| \mathbb{Z}^*_8 \right|$$

allora per ogni $P \in \mathbb{Z}^*_{15}$ si ha

$P = 2 \qquad 2^{ed} \bmod n = 2$

$2^9 \bmod 15 = 2$

$2^{25} \bmod 15 = 2$

$2^{49} \bmod 15 = 2$

$\mathbb{Z}^*_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

ma è vero anche per $P \in \mathbb{Z}_{15}$
$P \neq 0$

ad esempio

$$3 \notin \mathbb{Z}^*_{15} \qquad 3^{ed} \bmod n = 3$$

$$3^9 \bmod 15 = 3$$

$$3^{25} \bmod 15 = 3$$

$$3^{49} \bmod 15 = 3$$

La prova che RSA funziona anche per $P \in \mathbb{Z}_n \notin \mathbb{Z}^*_n$ è complicata

---

Comunque se n è un numero di 512 cifre decimali allora la probabilità che $P \in \mathbb{Z}_n$ e non $\in \mathbb{Z}^*_n$ è molto, molto piccola ($\sim 10^{-25}$) ☺

---

si pensi che $n=15$, $\varphi(15)=8$, $\frac{8}{15} \simeq 0{,}53$; $n = 47 \cdot 53 = 2{,}491$, $\varphi(n) = 46 \cdot 52 = 2{,}392$; $\frac{2{,}392}{2{,}491} \simeq 0{,}96$; $\lim_{n \to \infty} \frac{\varphi(n)}{n} = 1$

$\varphi(n)=12 \quad \varphi(12)=4$

$n=3\cdot 7=21$

$p=7$

$q=3$

RSA

19

$$\mathbb{Z}_n \equiv \mathbb{Z}_{21} \equiv \{0,1,2 \ldots 20\}$$

$$\mathbb{Z}_{21}^* \equiv \{1,2,4,5,8,10,11,13,16,17,19,20\} \quad |\mathbb{Z}_{21}^*| = \varphi(21)=12$$

$$\mathbb{Z}_{\varphi(n)}^* \equiv \mathbb{Z}_{12}^* \equiv \{1,5,7,11\} \quad |\mathbb{Z}_{12}^*| = \varphi(12)=4$$

$12=2^2\cdot 3$

RSA $\quad P\in\mathbb{Z}_{21} \to C\in\mathbb{Z}_{21}$

$$\begin{cases} C = P^e \bmod n \\ P = C^d = P^{ed} \bmod n \end{cases}$$

$$ed \equiv 1 \bmod \varphi(n)$$

$$d \equiv e^{-1} \bmod \varphi(n) \qquad e,d\in\mathbb{Z}_{\varphi(n)}^*$$

$n=21$

$\begin{cases} e=5 \\ d=5 \end{cases}$ $\quad d=5^{-1} \bmod 12 = 5^3 = 5$

$5\cdot 5\equiv 1 \bmod 12$

$\begin{cases} e=7 \\ d=7 \end{cases}$ $\quad d=7^{-1} \bmod 12 = 7 = 7^3 = 7$

$\begin{cases} e=11 \\ d=11 \end{cases}$ $\quad d=11^{-1}\equiv 11$

(20)

se $P \in \mathbb{Z}_{21}^*$ $\quad P^{ed} \equiv P \bmod 21$

$mcd(P, 21) = 1$ $\quad ed \equiv 1 \bmod \varphi(21)$

es. $P \equiv 2 \in \mathbb{Z}_{21}^*$ $\quad mcd(2, 21) = 1$

$21 = 3 \cdot 7$

$e = 5$

$d = 5$

$$\begin{cases} C = 2^5 \bmod 21 \equiv 11 \in \mathbb{Z}_{21}^* \\ P = 11^5 \bmod 21 \equiv 2 \text{ ok} \end{cases}$$

prendiamo $\quad P = 3 \notin \mathbb{Z}_{21}^* \in \mathbb{Z}_{21}$

$\underline{mcd(3, 21) = 3}$

$$\begin{cases} C = 3^5 \bmod 21 = 12 \in \mathbb{Z}_{21} \\ P = 12^5 \bmod 21 = 3 \ \underline{\text{ok}} \end{cases}$$

proviamo ancora $\quad P = 7 \notin \mathbb{Z}_{21}^* \in \mathbb{Z}_{21}$

$\underline{mcd(7, 21) = 7}$

$$\begin{cases} C = 7^5 \bmod 21 = 7 \in \mathbb{Z}_{21} \\ P = 7^5 \bmod 21 = 7 \end{cases}$$

RSA

$n = 3 \cdot 11 = 33$ $\qquad \varphi(n) = \underline{20} = 2^2 \cdot 5$

$\varphi[\varphi(n)] = \varphi(20) = 2^3 = 8$

$\mathbb{Z}_{33} \equiv \{0, 1, 2 \ldots 31, 32\}$

$\mathbb{Z}^*_{33} = \{1, 2, 4, 5, 7, 8, 10, \ldots, 31, 32\}$ $\qquad |\mathbb{Z}^*_{33}| = 20$

$\mathbb{Z}^*_{20} \equiv \{1, 3, 7, 9, 11, 13, 17, 19\}$ $\qquad |\mathbb{Z}^*_{20}| = 8$

$20 = 2^2 \cdot 5$

$e, d \in \mathbb{Z}^*_{20}$

$$\begin{cases} e=3 & d = 3^{-1} = 3^7 \bmod 20 \equiv 7 \\ e=9 & d = 9^{-1} = 9^7 \bmod 20 \equiv 9 \\ e=11 & d = 11^7 \bmod 20 = 11 \\ e=13 & d = 13^7 \bmod 20 = 17 \\ e=19 & d = 19^7 \bmod 20 = 19 \end{cases}$$

esempio $\quad P \in \mathbb{Z}_{33} \notin \mathbb{Z}^*_{33} = 3 \qquad \underline{mcd(3, 33) = 3}$

$e=3$
$d=7$

$$\begin{cases} C = 3^3 \bmod 33 = 27 \in \mathbb{Z}_{33} \\ P = 27^7 \bmod 33 = 3 \text{ OK} \end{cases}$$

$n = 3 \cdot 11 = 33 \qquad \varphi(n) = 20 = 2^2 \cdot 5 \qquad \varphi(\varphi(n)) = 2^3 = 8$

$\mathbb{Z}^*_{20} \equiv \{1, 3, 7, 9, 11, 13, 17, 19\} \pmod{20}$

$\begin{cases} 3^{-1} \equiv 3^{\varphi(\varphi(n))-1} \equiv 3^7 \equiv 7 \pmod{20} \\ 13^{-1} \equiv 13^7 \equiv 17 \end{cases}$

$9^{-1} \equiv 9$
$11^{-1} \equiv 11 \pmod{20}$
$19^{-1} \equiv 19$

$\mathbb{Z}^*_{20}$ è chiuso per moltiplicazione

Per tutti vale $b^8 \equiv 1 \pmod{20}$

ordine = minimo intero k per cui $b^k \equiv 1 \pmod{20}$
degli elementi b : $\text{mcd}(b, 20) = 1$.

$b \in \mathbb{Z}^*_{20}$

es $b = 3$

ciclo lungo 4 $\begin{cases} 3^1 \equiv 3 \\ 3^2 \equiv 9 \\ 3^3 \equiv 7 \\ 3^4 \equiv 1 \end{cases} \pmod{20}$

è un sottogruppo ciclico di $\mathbb{Z}^*_{20}$ di ordine 4 con radici 3 e 7 di ordine 4

$\varphi(n) = 2^2 \cdot 5 = p_1^2 \cdot p_2$

quindi 3 e così $3^{-1} \equiv 7$ hanno ordine $\underline{4} = \frac{20}{5} = \frac{\varphi(n)}{p_2}$

quindi è vero che (lagrange) $3^{\varphi(20)} \equiv 1 \pmod{20}$ $\quad 3^8 \equiv 1 \pmod{20}$

ma in questo caso anche $3^4 \equiv 1 \pmod{20}$ e quindi $\underline{4}$ è l'ordine di 3.

3 genera un ciclo di periodo 4
con due altri elementi di $\mathbb{Z}^*_{20}$: l'inverso 7 e il 9.

Anche 13 è analogo, con $13^{-1} \equiv 17$ sono di ordine 4,
e generano altri due elementi: l'inverso e 17.

9, 11 e 19 hanno invece ordine 2.

Firma RSA $\quad n = p \cdot q$

Alice $(e_A ; d_A)$ firma P

$$SIG(P) \equiv P^{d_A} \pmod{n}$$

e manda

Messaggio firmato: $\{P, SIG(P)\}$

Bob verifica che

$$VER[SIG(P)] \doteq P$$

e cioè che $\quad (P^{d_A})^{e_A} \equiv y \pmod{n}$

è tale che: $\quad y \equiv P \pmod{n}$, essendo la verifica, la cifratura con e_A della firma.

Shamir 3-pass Protocol

Alice zgjedh $K_{AB}=P$, e shifron e e dërgon

$$M1.\ A \to B:\quad E_{K_A}(P)$$

Bob merr, shifron e dërgon

$$M2.\ B \to A:\quad E_{K_B}[E_{K_A}(P)] = E_{K_A}[E_{K_B}(P)]$$

Alice merr, deshifron e dërgon

$$M3.\ A \to B:\quad E_{K_B}(P)$$

Bob deshifron $\quad D_{K_B}[E_{K_B}(P)] = \underline{P} = K_{AB}$ OK!

Alice	K_A e K_A^{-1}	$K_A=e_A;\ K_A^{-1}=d_A$
Bob	K_B K_B^{-1}	$K_B=e_B;\ K_B^{-1}=d_B$

RSA

$n = p \cdot q$

$$\begin{cases} C = P^e \bmod n & (1) \\ P = C^d \bmod n & (2) \end{cases}$$

$e \cdot d \equiv 1 \pmod{\varphi(n)}$

$d \equiv e^{\varphi(\varphi(n))-1} \bmod \varphi(n)$

infatti

proprietà

sostituendo (2) in (1)

$$P = P^{ed} \bmod n$$

è vera se e solo se

$$1 \equiv ed \pmod{n}$$

nel caso in cui quando $P \in \mathbb{Z}_n^*$ [$mcd(P,n)=1$]

SHAMIR-OMURA

$p : \frac{p-1}{2} = q$

$$\begin{cases} C = P^e \bmod p \\ P = C^d \bmod p \end{cases}$$

$d, e \in \mathbb{Z}_{p-1}^*$

e cioè $mcd(e,(p-1))=1$ e $mcd(d,p-1)=1$

cui

$$d \equiv e^{-1} \equiv e^{\varphi(p-1)-1} \pmod{p-1} \; : \; e\,d \equiv 1 \pmod{p-1}$$

è vera

$$P \equiv P^{ed} \pmod{p}$$

se

$$e \cdot d \equiv 1 \pmod{p-1}$$

RSA esempio (firma)

$n = p \cdot q = 13 \cdot 17 = 221$

$\varphi(n) = 12 \cdot 16 = 192 = 2^6 \cdot 3$

$\varphi(\varphi(n)) = (2^6 - 2^5)\, 2 = 64 = 2^5$

$e_A = 25 \quad d_A = 25^{-1} \equiv 25^{63} \equiv 169 \pmod{192}$

mcd(25,192)=1 ok

Alice firma $P = 10$

$10^{169} \equiv 75 \pmod{221} \Rightarrow SIG(P)$

chiunque verifica, noti e_A e n, se

$75^{25} \equiv 10 \pmod{221}$ se $VER(SIG(P)) = P$ ok!

3-Pass Protocol Shamir-Omura

$p = 107 \qquad \frac{p-1}{2} = 53 = q$ ok

$\varphi(p-1) = \varphi(106) = 52$

$e_A = 23$; $d_A = 23^{-1} = 23^{51} \bmod 106 = 83$

$e_B = 3$; $d_B = 3^{51} \bmod 106 = 71$

Alice sceglie $K_{AB} \equiv 11 \bmod 107$, cifra e manda

M1. $A \to B$: $11^{23} \bmod 107 = 90$

Bob cifra M1 e manda

M2. $B \to A$: $90^3 \bmod 107 = 9$

Alice decifra M2 e manda

M3. $A \to B$: $9^{83} \bmod 107 = 47$

Bob decifra $47^{71} \equiv 11 \equiv K_{AB} \pmod{107}$

SHAMIR 3-PASSI

$n = 221$

$n = 13 \times 17 = 221$

$\varphi(n) = 192 = 2^6 \cdot 3$

$\varphi[\varphi(n)] = 64 = 2^6$

Alice

$$\begin{cases} e_A = 25 \perp 192 \text{ ok} \\ d_A = e_A^{-1} \equiv 25^{63} \equiv 169 \pmod{192} \end{cases}$$

Bob

$$\begin{cases} e_B = 35 \perp 192 \text{ ok} \\ d_B = e_B^{-1} = 35^{63} \equiv 11 \pmod{192} \end{cases}$$

Alice sceglie $K_{AB} = 10$, cifra e manda

$\pmod{221}$

M1. $A \to B$: $10^{25} \equiv 75$

Bob cifra e manda

M2. $B \to A$: $75^{35} \equiv 173$ $\pmod{221}$

Alice decifra e manda

M3. $A \to B$: $173^{169} \equiv 82$

Bob infine decifra

$$82^{11} \equiv 10 \equiv K_{AB}$$

OK!

Protocollo a 3 passi di Shamir Omura (27)

$p=59 \qquad \frac{p-1}{2}=q=29$ primo $\qquad \varphi(58)=28$

$a_A, a_A^{-1} \in \mathbb{Z}^*_{58}\,;\ a_B, a_B^{-1} \in \mathbb{Z}^*_{58}$ $\qquad a \cdot a^{-1} \equiv 1 \pmod{p-1}$

$\qquad\qquad a^{-1} \equiv a^{\varphi(p-1)-1} \pmod{p-1}$

$$\begin{cases} C = P^{a} \bmod p \\ P = C^{a^{-1}} \bmod p \end{cases} \qquad P, C \in \mathbb{Z}^*_p$$

Alice sceglie $K_{AB} \equiv 11 \in \mathbb{Z}^*_{59} \pmod{59}$

$a_A = 23 \qquad a_A^{-1} \equiv 23^{-1} \equiv 23^{27} \bmod 58 = 53 \pmod{58}$

$a_B = 3 \qquad a_B^{-1} = 3^{-1} \equiv 3^{27} \bmod 58 = 39 \pmod{58}$

$$M1.\ A \to B:\ 11^{23} \bmod 59 \equiv 24$$

Bob cifra e manda

$$M2.\ B \to A:\ 24^{3} \bmod 59 \equiv 18$$

Alice decifra M2 e manda

$$M3.\ A \to B:\ 18^{53} \bmod 59 \equiv 33$$

Bob decifra

$$33^{39} \equiv 11 \equiv K_{AB}$$

LOG DISCRETI $\quad q=2 \quad k=2$ (28)

$p=59 \qquad p-1=58=2\times 29 \qquad 29=q$

$\alpha = 3^{\frac{58}{2}} \equiv 3^{29} \equiv 1$ NO $\quad \pmod{59}$

$3^{\frac{58}{29}} \equiv 3^2 = 9$

$\alpha=2 \begin{cases} 2^{29} \equiv -1 \\ 2^2 \equiv 4 \end{cases}$ OK

$1 \le a \le 57 \quad (a \in \mathbb{Z}_{p-1};\ a \neq 0)$

- DH alice $a_A=3$ $\quad K_{AB} = \alpha^{a_A a_b} = 2^{18} \equiv 7$ $\begin{cases} 2^3 \equiv 8 \\ 2^6 \equiv 5 \end{cases} \pmod{59}$

  bob $a_A=6$

- ElGamal Cryptosystem

Bob $a_B=6$

$\alpha=2 \qquad \beta \equiv 2^6 \equiv 5 \pmod{59}$

Alice sceglie $k=3$ e mappa $\begin{cases} r \equiv 2^3 \equiv 8 \\ t \equiv 5^3 \cdot 5 \equiv 5^4 \equiv 35 \end{cases} \pmod{59}$

e manda $P=5$

$Sig(P) \equiv \{5, (8,35)\}$

Verifica Bob $\quad t\,(r^a)^{-1} \equiv P \pmod{p}$

$35\,(8^6)^{-1} \equiv 35 \cdot 7^{-1} \equiv 35 \cdot 7^{57} \equiv 35 \cdot 17 \equiv 5$

OK

Crittosistema di ElGamal

p-primo $\quad$ α primitiva di $\mathbb{Z}_p^*$

(ce ne sono $\varphi(p-1)$ di radici primitive)

- chiave pubblica

$$\beta = \alpha^a \bmod p$$

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

- chiave privata a

$$1 \le a \le p-2 \qquad a \in \mathbb{Z}_{p-1}$$

$$a \neq 0$$

genera tutti i possibili elementi $\beta \in \mathbb{Z}_p$

PUBBLICO

$$(p, \alpha, \beta)$$

Alice sceglie $k \in \mathbb{Z}_{p-1}$, $k \neq 0$ NONCE

$1 \le k \le p-2$

e manda

$$C = (r, t)$$

per cifrare il plaintext $P \in \mathbb{Z}_p^*$

$$(r, t) \in \mathbb{Z}_p^*$$

$$\begin{cases} r = \alpha^k \bmod p \\ t = \beta^k P \bmod p \end{cases}$$

Bob decifra C con la chiave privata a

$$t(r^a)^{-1} \equiv P \pmod p$$

essendo $\beta^k r^{-a} \equiv 1 \pmod{p}$; e cioè $\beta^k \equiv r^a \pmod{p}$

Esempio

$p = 59$

$p-1 = 58 = 2 \cdot 29 = 2 \cdot q$

$\alpha = 2$

$2^{29} \equiv 58 \not\equiv 1 \pmod{59}$ OK

$\beta \equiv 2^{57} \equiv 30 \pmod{59}$

$a = 57 = p-2$ OK

$1 \leq a \leq p-2$

PUBBLICO $(59, 2, 30)$

Alice sceglie $k = 23$ per cifrare $P = 10$

$1 \leq k \leq p-2$

$$\begin{cases} r \equiv 2^{23} \equiv 47 \\ t \equiv 30^{23} \cdot 10 \equiv 9 \end{cases} \pmod{59}$$

Bob decifra $t\,(r^a)^{-1} \equiv 9 \cdot (47^{57})^{-1} \equiv 9 \cdot 54^{-1} \equiv$

$\equiv 9 \cdot 54^{57} \equiv 9 \cdot 47 \equiv 10$ OK!

ora Alice apre $P_2 = 11$
e maldestramente usa lo stesso
nonce $k = 23$

$$\begin{cases} r_2 = 2^{23} \equiv 47 \equiv r_1 \\ t_2 \equiv 30^{23} \cdot 11 \equiv 4 \end{cases} \pmod{59}$$

Quindi Alice manda in sequenza

$$\begin{matrix} (r_1, t_1); (r_2; t_2) \\ (47, 9); (47, 4) \end{matrix} \pmod{59}$$

Oscar si accorge che $r_1 = r_2 = 47$
supponiamo che abbia decifrato $P_1 = 10$
allora

$$(1) \quad P_2 \equiv \frac{t_2 P_1}{t_1} \equiv \frac{4}{9} \cdot 10 =$$

$$\equiv 40 \cdot 9^{-1} \equiv 40 \cdot 9^{57} \equiv 40 \cdot 46 \equiv 11 \equiv P_2$$

BINGO!

infatti $\quad B^k \equiv r^a \equiv \dfrac{t_1}{P_1} \equiv \dfrac{t_2}{P_2} \pmod{p}$

cifrario ElGamal

$$p = 47 \qquad \alpha = 5$$

$$p - 1 = 46 = 23 \times 2$$

$$5^{\frac{46}{23}} = 5^2 \bmod 47 = 25 \quad \text{ok}$$

$$5^{\frac{46}{2}} = 5^{23} \bmod 47 = 46 \quad \text{ok}$$

$$q = 13$$

$$\beta = 5^{13} \bmod 47 = 43$$

Alice sceglie $K = 21$ e manda per $P = 40$

$$\begin{cases} r = 5^{21} \bmod 47 = 15 \\ t = 43^{21} \, 40 \bmod 47 = 21 \end{cases}$$

Bob decifra

$$21 \times \left(15^{13}\right)^{-1} \equiv 21 \times 44^{-1}$$

$$44^{-1} \equiv 44^{45} \bmod 47 \equiv 31$$

$$21 \times 31 \equiv 651 \equiv 40 \equiv P \quad \text{ok}$$

Cifrario di ElGamal

esempio $p = 113$; $\alpha = 5$

$$a \in \mathbb{Z}_{p-1} \qquad a = 13 \mod 113$$

$$\beta = 5^{13} \bmod 113 = 59$$

$P = 10$, Alice sceglie $k = 11$ e manda (x, y)

$$\begin{cases} r = 5^{11} \bmod 113 = 34 \\ t = (59^{11} \times 10) \bmod 113 = 105 \end{cases}$$

Bob decifra con $a = 13$

$$105 \times (34^{13})^{-1} \equiv 105 \cdot 67^{-1} \equiv 105 \times 67^{-1}$$

$$67^{-1} \equiv 67^{111} \equiv 27$$

$$2835 \equiv 105 \times 27 \equiv 10 \pmod{113} \text{ ok}$$

Firme ElGamal $\qquad \varphi(58)=28$ $\qquad$ 34

$p=59$

$a_B=6$ Bob di nuovo firma $\overset{P=5}{V}$ e sceglie $k_B=3 \in \mathbb{Z}^*_{58}$

$\alpha=2$ $\qquad$ e calcola $\qquad$ $mcd(3,58)=1$

$\beta=5\equiv 2^6$

$$\begin{cases} r \equiv 2^3 \equiv 8 \pmod{59} \\ s \equiv 39(5-6\cdot 8) \pmod{58} \equiv \\ \quad \equiv 39(-43)\equiv -53 \pmod{58} \equiv 5 \end{cases}$$

$k_B^{-1}\equiv 3^{-1}\equiv 3^{27}\equiv 39 \pmod{58}$

$$Sig(P)\equiv\{5,(8,5)\}$$

verifica $\beta^r r^s \equiv \alpha^P$ $\qquad$ $5^8\cdot 8^5 \equiv 45\cdot 2 \equiv 32 \equiv 2^5 \equiv \alpha^P$ ok

Firma DSA

$q \mid p-1$ $\qquad$ $t=2$

$q=29$

$a_B=6$ $\qquad$ $g=2$ $\qquad$ $\alpha=g^{\frac{p-1}{q}}\equiv 2^2=4$

$\beta\equiv 4^6\equiv 25$ $\qquad$ $P=5$ $\qquad$ $4^{29}\equiv 1 \pmod{59}$

$k_B=3\in\mathbb{Z}^*_{29}$

$k_B^{-1}\equiv 3^{27} \bmod 29 \equiv 10$ $\qquad$ $r=(4^3 \bmod 59) \bmod 29 =$

$= 5 \bmod 29$

$s=10(5+6\cdot 5)\equiv 350\equiv 2 \pmod{29}$

$$Sig\ \{5,(5,2)\}$$

$s^{-1}\equiv 2^{-1}\equiv 2^{27}\equiv 15$

35

$$\begin{cases} u_1 = s^{-1} p \equiv 15 \cdot 5 \equiv 17 \pmod{29} \\ u_2 = s^{-1} r \equiv 15 \cdot 5 \equiv 17 \pmod{29} \end{cases}$$

$$\alpha^{u_1} \cdot \beta^{u_2} \equiv (4^{17} \cdot 25^{17} \bmod 59) \pmod{29} \equiv$$

$$\equiv 27 \cdot 57 \equiv 5 \bmod 29 \equiv r$$

OK!

FIRMA DSA

36

altro esempio

$p = 47$

$p-1 = 46 = 2 \cdot 23$

$q = 23$

$g = 5$

$$\begin{cases} g^{\frac{p-1}{2}} = 5^{23} \equiv 46 \\ g^{\frac{p-1}{23}} \equiv 5^2 = 25 \text{ ok} \end{cases}$$

$$\alpha = g^{\frac{p-1}{q}} = 5^{\frac{46}{23}} \equiv 25$$

$$\alpha^q \equiv 25^{23} \equiv 1 \mod 43$$

$25 \equiv \alpha$ è di ordine 23

mentre 5 è di ordine 46

$\alpha \equiv 25$ genera α^i per $1 \le i \le 22$

$22 = q-1$ elementi

$a \in \mathbb{Z}_q^* \equiv \mathbb{Z}_{23}^*$

β

$\alpha^1 \equiv 25$

$\alpha^2 \equiv 14$

$\alpha^3 \equiv 21$

$\alpha^4 \equiv 8$

$\alpha^5 \equiv 12$

$\alpha^6 \equiv 18$

$\alpha^7 \equiv 27$

$\alpha^8 \equiv 17$

$\alpha^9 \equiv 2$

$\alpha^{10} \equiv 3$

$\alpha^{11} \equiv 28$

$\alpha^{12} \equiv 42 \equiv 28^{-1} \equiv 28^{45}$

$\alpha^{13} \equiv 16$

$\alpha^{14} \equiv 24$

$\alpha^{15} \equiv 36$

$\alpha^{16} \equiv 7$

$\alpha^{17} \equiv 34 \equiv 18^{-1} \equiv 18^{45}$

(mod 47)

inversi

B

$$\begin{cases} \alpha^{18} \equiv 4 \\ \alpha^{19} \equiv 6 \\ \alpha^{20} \equiv 9 \\ \alpha^{21} \equiv 37 \\ \alpha^{22} \equiv 25^{-1} \equiv 25^{45} \equiv 32 \equiv 25^{22} \end{cases}$$

$$\alpha^{23} \equiv 1$$

$$\alpha^{24} \equiv 25 \equiv \alpha^{1}$$

$$\alpha^{26} \equiv 14 \equiv \alpha^{2}$$

$\vdots$ ecc.

per calcolare gli inversi basta fare

$$(\alpha^{i})^{-1} \equiv \alpha^{-i} \equiv \alpha^{23-i}$$

es. $(\alpha^{6})^{-1} \equiv \alpha^{-6} \equiv \alpha^{23-6} \equiv \alpha^{17}$

$$\begin{cases} \alpha^{6} \equiv 18 \equiv 25^{6} \\ \alpha^{17} \equiv 34 \equiv 18^{-1} \equiv 18^{45} \equiv 25^{17} \end{cases}$$

(mod 47)

es $(\alpha^{1})^{-1} \equiv \alpha^{-1} \equiv \alpha^{22}$

$$\begin{cases} \alpha^{1} \equiv 25 \\ \alpha^{22} \equiv 25^{-1} \equiv 25^{45} \equiv 32 \equiv 25^{22} \end{cases}$$

Alice sceglie $1 \leq a \leq q-1$: $a=3$ (38)

$1 \leq a \leq 22$

$1 \leq k \leq q-1$: $k=5$

$k^{-1} \equiv 5^{21} \equiv 14 \mod 23$

e forma $0 \leq P \leq 22$: $P = 20 \mod 23$

$$\begin{cases} r = (\alpha^k \mod p) \mod q \equiv (25^5 \mod 47) \mod 23 \\ r \equiv 12 \mod 23 \\ s = k^{-1}(20 + 3 \cdot 12) \mod 23 \equiv 14 \cdot 56 \equiv \\ \equiv 2 \pmod{23} \end{cases}$$

$\underline{\text{FIRMA}(20,(12,2))}$

Verifica

$\hookrightarrow (\alpha^{s^{-1}P} \beta^{s^{-1}r} \mod p) \mod q = r$

$s^{-1} \equiv 2^{21} \pmod{23}$
$\equiv 12$

$$\begin{cases} s^{-1}P \equiv 12 \cdot 20 \equiv 10 \pmod{23} \\ s^{-1}r \equiv 12 \cdot 12 \equiv 6 \end{cases}$$

$\beta \equiv \alpha^a \equiv 25^3 \equiv 21$

$(25^{10} \cdot 21^6 \mod 47) \mod 23 =$
$(3 \cdot 14) \mod 47 \equiv 12 \mod 23 = r$ OK !

$\boxed{\text{NB}}$ $\boxed{\text{se } P = 10\text{, allora va scelto un'altro } k\text{ !}}$

se $P \equiv -ar \pmod{q} \equiv -3 \cdot 12 \equiv 20 \cdot 12 \equiv 10 \pmod{23}$

allora $s \equiv k^{-1}(10 + 3 \cdot 12) \equiv 14 \cdot 46 \equiv 0 \pmod{23}$

per esempio $K=6$ e $P=10$

$6^{-1} \equiv 6^{21} \equiv 4$ mod 23

$$\begin{cases} r = 25^{6} \equiv 18 \bmod 23 \\ s = 4(10+3\cdot 18) \bmod 23 \equiv 4\cdot 64 \equiv \underline{3} \end{cases}$$ ok!

FIRMA $\{10, (18, 3)\}$.

$$s^{-1} \equiv 3^{-1} \equiv 3^{21} \equiv 8 \pmod{23}$$

$$\begin{cases} s^{-1}P \equiv 8\cdot 10 \equiv 80 \equiv 11 \\ s^{-1}r \equiv 8\cdot 18 \equiv 144 \equiv 6 \end{cases} \pmod{23}$$

verifico $(25^{11}\cdot 21^{6} \bmod 47) \equiv 2^{8\cdot 4} \bmod 47 \equiv$

$\equiv 18 \bmod 47 \equiv 18 \bmod 23 \equiv 18 \pmod{23}$

ok!