Cifrario di Rabin

Chiara Gasparri

Simbolo di Legendre

Sia p un numero primo dispari, definiamo il Simbolo di Legendre come

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ se p divide a} \\ 1 \text{ se a è un quadrato di } Z_p^* \\ -1 \text{ se a non è quadrato } Z_p^* \end{cases}$$

Proprietà del Simbolo di Legendre

- In Z_N^* ci sono $\frac{(p-1)}{2}$ elementi quadrati

e l'altra metà degli elementi non sono quadrati

- Si dimostra che: $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$

che ci permette di valutare facilmente se a è quadrato o meno

In particolare -1 è quadrato se $p \equiv 1 \bmod 4$

e non è quadrato se $p \equiv 3 \bmod 4$

Esempio

- in Z_7^* trovo

a	$\left(\frac{a}{7}\right) \equiv a^{(7-1)/2} \bmod 7$
1	$1^3 = 1 \bmod 7$
2	$2^3 = 8 \equiv 1 \bmod 7$
3	$3^3 = 27 \equiv -1 \bmod 7$
4	$4^3 = 16 \equiv 1 \bmod 7$
5	$5^3 = 125 \equiv -1 \bmod 7$
6	$6^3 = 216 \equiv -1 \bmod 7$

Proprietà del Simbolo di Legendre

Se a è un quadrato in Z_p^*, si dimostra che esistono due elementi y, distinti, tali che $y^2 = a \bmod p$

Se uno di essi è α , l'altro è $(p-\alpha)$

infatti $(p-\alpha)^2 = \alpha^2$

L'equazione $y^2 = a \bmod p$ si risolve molto facilmente

se $p \equiv 3 \bmod 4$ oppure se $p \equiv 5 \bmod 8$

in quanto vale il seguente teorema

Proprietà del Simbolo di Legendre

Teorema. Se $p \equiv 3 \bmod 4$ e $p = 4k - 1 \ (= 4k' + 3)$

Allora una soluzione di $y^2 = a \bmod p$ è $y = a^k \bmod p$

Dimostrazione. Perché l'equazione abbia soluzione, a deve essere un quadrato in Z_p^*

quindi il simbolo di Legendre vale $\left(\frac{a}{p}\right) = 1 = a^{(p-1)/2} \bmod p$

Dato che $k = (p+1)/4$ possiamo calcolare

$$y^2 = (a^k)^2 = (a^{(p+1)/4})^2 = a^{(p+1)/2} = (a^{(p-1)/2}) \cdot a \equiv a \bmod p$$

Esempio

In Z_{11}^{*} mi chiedo quali siano le radici per $3 \bmod 11$

So che 3 è un quadrato, infatti il suo Simbolo di Legendre vale

$$\left(\frac{a}{p}\right) = \left(\frac{3}{11}\right) = 3^{(11-1)/2} = 3^5 = 243 \equiv 1 \bmod 11$$

p verifica la condizione $p = 11 \equiv 3 \bmod 4$ e $p = 12 - 1 = 4 \cdot 3 - 1$

Determinato $k = 3$ possiamo andare a calcolare

$$y = 3^3 \bmod p = \begin{cases} 5 \bmod 11 \\ -5 \equiv 6 \bmod 11 \end{cases}$$

Possiamo verificare che $5^2 = 3 \bmod 11$ e $6^2 = 3 \bmod 11$

Cifrario di Rabin

Sviluppato nel 1979, si basa sul problema della radice quadrata in Z_p^*

Dato $n = p \cdot q$ con p e q due numeri primi distinti

e dato un intero a , $1 < a < n$ con $y^2 = a \bmod n$

trovare y

Il cifrario di Rabin ha una notevole importanza teorica, in quanto è stato dimostrato che dal punto di vista computazionale la ricostruzione di un testo in chiaro equivale alla scomposizione di n nei due fattori

Generazione delle chiavi

Ciascun utente sceglie randomicamente due numeri primi dello stesso ordine di grandezza

p e q tali che $p \equiv q \equiv 3 \bmod 4$

Chiave pubblica: $n = pq$

Chiave privata: (p,q)

Cifratura

Un utente U vuole inviare un messaggio ad A

- Legge la chiave pubblica di A
- Codifica il messaggio in un elemento m di Z_m^* e introduce una ridondanza
  (ad esempio replica gli ultimi 64 bit)
- Computa $c = m^2 \bmod n$
- Invia c ad A

Decifratura

Per ricostruire il messaggio m, A deve risolvere l'equazione

$$c = m^2 \bmod n$$

Le radici di questa equazione sono quattro, tranne nella rara eventualità in cui $(m, n) \neq 1$ dove le radici sono solo una o due

Il problema è computazionalmente impossibile se non si conosce la scomposizione di n.

Tuttavia la chiave privata del ricevente sono proprio i fattori p, q con

$$n = p \cdot q \quad \text{e} \quad p \equiv q \equiv 3 \bmod 4$$

È quindi possibile usare il seguente algoritmo …

Decifratura

- Con l'algoritmo di Euclide si trovano due numeri interi *a* e *b* tali che $ap + bq = 1$
- Si calcolano

$$r = c^{(p+1)/4} \bmod p$$
$$s = c^{(q+1)/4} \bmod q$$

- e poi

$$x = (aps + bqr) \bmod n$$
$$y = (aps - bqr) \bmod n$$

- Troviamo così i valori delle quattro radici : $x, -x, y, -y$

?

Come scegliere la radice giusta?

Attraverso la ridondanza introdotta in fase di codifica, che si presenta (con molta probabilità) solo in una delle quattro radici.

Esempio

Chiave pubblica di A : n = 21
Chiave privata di A : (p,q) = (3,7)

- Voglio inviare il messaggio **m = 4** ad A e cerco la sua chiave pubblica
- Calcolo $c = 4^2 = 16 \bmod 21$ ed invio il messaggio
- A riceve il messaggio e calcola a , b tali che $3a + 7b = 1$

E trova $a = 5$, $b = 1$

- A calcola dunque $r = 16^{(3+1)/4} \bmod 3 = 1 \bmod 3$

$$s = 16^{(7+1)/4} \bmod 7 = 4 \bmod 7$$

- da cui può ricavare $x = (aps + bqr) \bmod n$
  $y = (aps - bqr) \bmod n$

$$x = (5 \cdot 3 \cdot 4 + 1 \cdot 7 \cdot 1) \bmod 21 = (60 + 7) \bmod 21 = 67 \bmod 21 = 4 \bmod 21$$

$$y = (60 - 7) \bmod 21 = 53 \bmod 21 = 11 \bmod 21$$

Le quattro radici di c sono 4,17, 11, 10.

Tra esse possiamo scegliere quella giusta con l'analisi della ridondanza

Firma di Rabin

- È possibile utilizzare la tecnica studiata da Rabin anche per firmare i messaggi.
  - Lo spazio dei messaggi è l'insieme dei quadrati di Z_n^*
  - Le firme sono le radice quadrate degli stessi.

- Chi firma un messaggio m sceglie come sig(m) una delle 4 radici in Z_n^*

- Chi vuole verificare la validità di una firma su un messaggio m calcola:

$$sig^2 = m \bmod n$$