Il sistema di crittografia RSA

Il *teorema di Fermat* dice che, se p è primo e $a \bmod p \neq 0$, allora

$$a^{p-1} \bmod p = 1$$

Eccone una dimostrazione elementare:
Consideriamo l'insieme $Z_p^* = \{1, 2, ..., p-1\}$ *e l'insieme*

$$M(a) = \{a \bmod p, 2a \bmod p, ..., (p-1)a \bmod p\}$$

Questi due insiemi coincidono: infatti se prendiamo un $m \in Z_p^*$, *possiamo scriverlo come* $(m \times a^{-1} \times a) \bmod p = (m \times a^{-1})a \bmod p$ *e quindi* $m \in M(a)$. *Allora* $Z_p^* \subseteq M(a)$ *ma* Z_p^* *ha* $p-1$ *elementi distinti e non può essere quindi un sottoinsieme proprio di un insieme con al più* $p-1$ *elementi distinti; deve quindi coincidere con* $M(a)$. *Questo significa che* $1 \times 2 \times ... \times (p-1) \bmod p = a \times 2a \times ... \times (p-1)a \bmod p$.

Raccogliendo otteniamo: $(p-1)! \bmod p = a^{p-1} \times (p-1)! \bmod p$. *Essendo* $(p-1)! \bmod p \neq 0$, *perchè* $(p-1)!$ *non contiene* p *come fattore, otteniamo la tesi.*

Dal teorema di Fermat otteniamo un importante risultato:

Se $n = p \times r$ con p e r due numeri primi, poniamo $\varphi(n) = (p-1)(r-1)$ (questa è detta la *funzione di Eulero*).

Dal teorema di Fermat si ottiene che $a^p \bmod p = a \bmod p$ per cui:

$$a^{\varphi(n)} \bmod p = a^{P(r-1)}a^{1-r} \bmod p = a^{r-1}a^{1-r} \bmod p = 1$$

e anche:

$$a^{\varphi(n)} \bmod r = a^{r(p-1))}a^{1-p} \bmod r = a^{p-1}a^{1-p} \bmod r = 1$$

Essendo contemporaneamente $a^{\varphi(n)} \bmod p = 1$ e $a^{\varphi(n)} \bmod r = 1$ (con r e p primi fra loro) si ottiene

$$a^{\varphi(n)} \bmod n = 1$$

Questo è un caso particolare del Teorema di Eulero.

Il sistema di crittografia a chiave pubblica di Rivest-Shamir-Adleman (RSA) (è quello con cui è implementato il protocollo SSL, avete presente il lucchetto chiuso che appare quando visitate una pagina Web protetta?) è basato direttamente sul Teorema di Eulero.

Supponiamo che Alice voglia mandare a Bob il numero segreto del suo cellulare $x = 333123456$

Bob prende due numeri primi:

$$q = 20939$$

e

$$r = 259387.$$

Poi calcola

$$\begin{aligned} n &= q \times r \\ &= 20939 \times 259387 \\ &= 5431304\,393 \end{aligned}$$

$$\begin{aligned} \varphi(n) &= (q-1) \times (r-1) \\ &= 20938 \times 259386 \\ &= 5431\,024\,068 \end{aligned}$$

A questo punto genera la sua *chiave pubblica* (e, n) dove e è un intero relativamente primo con $\varphi(n)$, (ad esempio $e = 1009$) e la sua *chiave privata* (d, n) dove $d = e^{-1} \bmod \varphi(n)$.

$d = 1009^{-1} \bmod 5431\,024\,068 = 4925\,061\,469$.

Sia $x = 333123456$ il testo in chiaro da trasmettere. Messaggi più lunghi di n non sono ammessi per cui bisogna, eventualmente, spezzare il testo in chiaro in frammenti adeguati.

Alice usa la chiave pubblica di Bob per cifrare il messaggio secondo il seguente algoritmo: $y = x^e \bmod n$,

e ottiene $y = 333123456^{1009} \bmod 5431304\,393 = 4978\,962\,229$.

Spedisce a Bob il numero y e *Bob applica la sua chiave privata per riottenere il messaggio in chiaro*:

$$x = y^d \bmod n = 4978\,962\,229^{4925\,061\,469} \bmod 5431304\,393 = 333\,123\,456.$$

Questo metodo funziona per due motivi.

a) se $x^e = y \bmod n$ e $d = e^{-1} \bmod \varphi(n)$, allora $y = x^e + kn$ e $de = 1 - h\varphi(n)$, con h e k numeri interi. Ma allora

$$(x^e + kn)^d = x \cdot (x^{\varphi(n)})^{-h} + m$$

con m un numero intero multiplo di n e, *per il teorema di Eulero*,

$$x^{\varphi(n)} \bmod n = 1$$

Cioè

$$y^d \bmod n = x$$

come si voleva.

b) per ottenere il testo in chiaro non basta avere e,n e y; se non si conoscono q e r l'impresa di invertire la formula di Alice cioè calcolare x da y è quasi disperata perchè la fattorizzazione di numeri molto grandi richiede moltissimo tempo di calcolo.

Ricapitoliamo (in realtà semplificando un po'): ogni sito Web protetto ha un suo numero n (molto grande, non come i nostri esempi) e la corrispondente $\varphi(n)$; quando ci si collega il nostro browser riceve la chiave pubblica del sito, codifica i messaggi e li spedisce. Il sito usa la sua chiave privata per leggere i messaggi ed eseguire le operazioni richieste.

Esempio di calcolo.

$r = 123\,456\,789\,987\,654\,353$

$s = 987\,654\,321\,123\,456\,823$

$n = r \times s = 121\,932\,632\,103\,337\,941\,464\,563\,328\,643\,500\,519$

$\varphi(n) = (r-1)(s-1) = 121\,932\,632\,103\,337\,940\,353\,452\,217\,532\,389\,344$

$\gcd(67777777777771, 121\,932\,632\,103\,337\,940\,353\,452\,217\,532\,389\,344) = 1$

messaggio :8888888888, $y = 8888888888^{67777777777771} \bmod 121\,932\,632\,103\,337\,941\,464\,563\,328\,643\,500\,519 = 78\,687\,260\,944\,075\,815\,618\,371\,573\,626\,229\,331$

$d = 67777777777771^{-1} \bmod 121\,932\,632\,103\,337\,940\,353\,452\,217\,532\,389\,344 = 2604\,717\,670\,245\,025\,077\,664\,852\,739\,463\,811$

$78\,687\,260\,944\,075\,815\,618\,371\,573\,626\,229\,331^{2604\,717\,670\,245\,025\,077\,664\,852\,739\,463\,811} \bmod 121\,932\,632\,103\,337\,941\,464\,563\,328\,643\,500\,519 = 8888\,888\,888$