

## “LA CRITTOGRAFIA RSA” (esempi e prospettive)

Com'è noto, la crittografia moderna usa i numeri primi, e noi, studiosi di questi ultimi, non possiamo in questo sito trascurare tale metodologia, specialmente il sistema RSA (un sistema concorrente sfrutta le curve ellittiche; ma anche questo usa i numeri primi, sebbene con chiavi numeriche più corte e più adatta a piccoli elettronici come telefonini, palmari, ecc). Riporteremo brevemente alcuni siti o blog che ne parlano e fanno esempi pratici per capirne il funzionamento matematico, e ai quali i visitatori interessati e appassionati possono rivolgersi per saperne di più: eccone tre dei più interessanti:

<http://digilander.libero.it/decrittazione>

diretto dal Prof. Giovanni Fraternali, dove si trova anche molta buona matematica divulgativa da consultare, anche in inglese (Teoria dei numeri, ecc.).

<http://MATHbuildingBlock.blogspot.com>

del nostro collaboratore Ing. Rosario Turco, informatico (vedi Link sul nostro sito) con diverse e competenti considerazioni su algoritmi di fattorizzazione e sul sistema RSA:

- *Fattorizzazione e algoritmo di Shor*
- *Algoritmo veloce di primalità e fattorizzazione (AKS)*

- *Algoritmi polinomiali*
- *Quadratic Sieve*

(oltre che sulla ex - congettura di *Collatz* e sull'*ipotesi di Riemann*).

<http://alpha01.dm.unito.it/personalpages/cerruti/luglio04-gennaio28.html#riemann>

relativo all'articolo "Congettura di Riemann e sicurezza mondiale"; nell'Archivio del blog, diretto dal Prof. Umberto Cerruti dell'Università di Torino, si trovano anche altri ottimi lavori sui numeri primi, sulla fattorizzazione, ecc.

La fattorizzazione veramente veloce per violare il sistema crittografico RSA è ancora molto però lontana, nonostante i buoni algoritmi di fattorizzazione (come per esempio l'algoritmo di Fermat, parzialmente connesso alla congettura di Goldbach tramite la semisomma  $(s = (p+q)/2)$  e la semidifferenza  $d = (q-p)/2$  tali che  $p = s - d$  e  $q = s + d$ ); e non si sa ancora bene se tale fattorizzazione veloce è connessa anche con l'ipotesi di Riemann: c'è chi pensa che se questa è vera, allora deve esistere un polinomio di fattorizzazione veloce (cioè in tempo polinomiale); e chi, invece, pensa che sia molto difficile ottenere la fattorizzazione veloce a partire dall'ipotesi di Riemann.

Il nostro Gruppo stà facendo qualche progresso, oltre che sulla congettura di Goldabch, anche sull'ipotesi di Riemann, soprattutto con l'ipotesi equivalente RH1 basata sui criteri di Robin e Lagarias ( "*I multipli di 6 e la Riemann Hypothesis*"); ma non escludiamo del tutto

nostre future ricerche anche in questo campo (crittografia RSA), a completamento del nostro progetto iniziale di ottenere dei progressi teorici nel campo della Teoria dei Numeri in generale e dei numeri primi in particolare. Questi ultimi, oltre che in crittografia (con i numeri RSA o con le curve ellittiche), sembrano anche, com'è noto, sempre più coinvolti anche nella fisica (Modello Standard, stringhe), per esempio tramite la funzione zeta di Riemann e della relativa ipotesi, ancora non del tutto dimostrata (la maggior parte dei matematici, noi compresi, ritengono che essa sia vera). Riprenderemo probabilmente le nostre ricerche sulla fattorizzazione veloce solo quando l'ipotesi di Riemann sarà definitivamente dimostrata (oppure anche quando avremo fatto noi stessi qualche passo in tale direzione, e che ci possa eventualmente essere utile anche a tale scopo) e anche quando si comprenderà meglio anche qualche altra importante relazione tra fattorizzazione veloce con l'ex congettura di Goldbach.

Pensiamo infatti che la soluzione potrebbe trovarsi, molto probabilmente, proprio in future e avanzate evoluzioni di tale ex- congettura, e sue possibili connessioni anche con il prodotto anziché con la sola somma di due numeri primi (oltre a quella già nota con la semisomma), e quindi anche ben oltre il già noto ed efficiente algoritmo di Fermat; ma non ancora al punto da poter violare il sistema crittografico RSA. Per fare questo occorre ben altro, e che potrebbe tuttavia essere basato su tale algoritmo, o meglio ancora su una sua possibile ed eventuale versione più evoluta, anche se non sappiamo ancora bene come. In ogni caso esso potrebbe essere il nostro punto di partenza.

Un'altra possibilità sarebbe anche una migliore conoscenza, oltre alla ex-congettura di Goldbach, anche dell'ipotesi di Riemann (connessa in qualche modo ad un polinomio veloce di fattorizzazione, che si pensa possa esistere se la RH fosse vera, e che sia o no collegato alla ex-congettura di Goldbach); e con tale migliore conoscenza di entrambe le congetture, si potrebbe infine sfruttare qualche eventuale punto debole dei numeri RSA per trovare una soluzione definitiva.

Inoltre, i futuri computer quantistici, ancora in fase iniziale di sperimentazione, saranno in grado di scomporre in pochi secondi qualsiasi numero RSA, tramite l'algoritmo di Shor già pronto per essi, o altri futuri algoritmi analoghi.

In ogni caso, è questione di pochi anni, al massimo un decennio o poco più.

Però sarebbe bello, per noi matematici, sia dilettanti che professionisti, arrivare a scomporre rapidamente tali numeri con l'intelligenza, tramite appositi algoritmi polinomiali veramente veloci, e possibilmente anche prima dell'avvento ormai vicino dei computer quantistici con la loro "forza bruta". Dopo tale avvento, infatti, la ricerca di tale polinomio perderebbe gran parte dell'attuale fascino e importanza, e pochissimi matematici continuerebbero a cercarlo ugualmente.

***GRUPPO ERATOSTENE***

***Caltanissetta 9.4.2009***