

- Conggettura sui numeri RSA -

Gruppo Eratostene

Abstract

In this paper we propose an our conjecture about RSA number:

**“In all RSA number $N=p*q$, the prime factor p is always between $n/2$ and n ,
whit $n = \sqrt{N}$ ”**

Osservando bene alcuni numeri RSA già fattorizzati e i loro fattori (anche per piccoli numeri RSA, per esempio di 5 cifre, RSA-5, per esempio $29083 = 127*229$) abbiamo ideato la seguente **“congettura sui numeri RSA”** :

**“Per tutti i numeri RSA, p è compreso tra $n/2$ e n , con $n = \sqrt{N}$ ”
(e quindi è inutile cercarlo tra 3 ed $n/2$)**

Se fosse vera, come cercheremo di dimostrare, si risparmierebbe almeno metà dei tempi di calcolo.

Per alcuni numeri RSA, p si potrebbe trovare vicino alla media aritmetica $(n/2 + n)/2$; un piccolo esempio (RSA - 5, cioè con cinque

cifre, è : $29083 = 127 * 229$, con $n = 170,53 \approx 170$

$p' \approx (170/2 + 170)/2 \approx (85 + 170)/2 = 255/2 = 127,5 \approx 127 = p$

Un altro esempio potrebbe essere il numero RSA (617), che inizia con le cifre 25 195... molto simili alle cifre di 29083 dell'esempio precedente, quindi potrebbe trovarsi anch'esso nel mirino della media aritmetica:

$n \approx \sqrt{25195...} \approx 158....$; $p' \approx (158.../2 + 158...)/2 = 118... le prime tre cifre, seguite da altre 305 cifre (questa è la nostra previsione, per quando RSA(617) sarà fattorizzato da altri ricercatori)$

Ma è ancora molto difficile individuare questi numeri RSA particolari, piccoli o grandi che siano, e quindi questa congettura non sarebbe alla fine molto pericolosa per il noto sistema crittografico basato sui numeri RSA.

Caltanissetta 1.10.2010

Gruppo Eratostene