Una introduzione alla crittografia: RSA, gli attacchi di Shamir, le Curve Ellittiche

Teo Mora

Abstract

La crittografia a chiave pubblica si basa su *funzioni a senso unico dotate di una trappola*.

La più semplice tale funzione è l'esponenziazione in $\mathbb{Z}_m^\star$, m prodotto di due primi, la cui solidità si basava sul fatto che l'algoritmo più efficiente per la fattorizzazione aveva complessità

$$\exp\left(\log^{\frac{1}{v}}(n)\log\log^{1-\frac{1}{v}}(n)\right), v=2$$

(risultato poi migliorato a $v=3$).

La progettazione da parte di Shamir, prima di una macchina analogica, poi di Twirl, rese meno solida la sicurezza sulla proclamata inattaccabilità di RSA.

Questo ha fatto sì che si preferisse usare, come funzione crittografica, il logaritmo di un sottogruppo ciclico del gruppo dei punti di una conica.