RSA: attacchi a tempo

Studiando il tempo di decifrazione ($c^d \bmod n$) si può stimare la quantità di bit a 1 nella chiave privata d. Infatti, l'algoritmo di esponenziazione veloce effettua un certo numero di quadrature seguite da tante moltiplicazioni quanti sono i bit 1 in d.