Quanti numeri primi a 512 bit ci sono?

La stima di Hadamard dice

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

ove $\pi(n)$ indica il numero di numeri primi minori o uguali ad n. Supponiamo di voler memorizzare tutti i numeri primi che sono possibili divisori di chiavi, prodotti di due primi, a 1024 bit, per poterli poi usare come possibili divisori al fine di fattorizzare la chiave. Essi sono dunque numeri a 512 bit (nel senso che occupano effettivamente 512 bit e non meno): il fatto che siano entrambi a 512 bit rende più difficile trovare i fattori della chiave (nessuno dei suoi due fattori è piccolo). Quindi

$$\pi(2^{512}) \approx \frac{2^{512}}{\ln 2^{512}} \approx 3.78 \cdot 10^{151}$$

e

$$\pi(2^{511}) \approx \frac{2^{511}}{\ln 2^{511}} \approx 1.90 \cdot 10^{151}$$

da cui il numero di numeri primi a (esattamente) 512 bit

$$\pi(2^{512}) - \pi(2^{511}) \approx 1.89 \cdot 10^{151}$$

Ora vediamo quanto spazio occupano per essere memorizzati: $1.89 \cdot 10^{151} \cdot 512$ bit. Dividendo per $8 \cdot 1024^4$ otteniamo $1.1 \cdot 10^{141}$ terabyte. Il numero di atomi dell'universo[1] è stimato tra 10^{72} e 10^{87}...

[1] `http://it.wikipedia.org/wiki/Googol`