RSA: scelta di p e q

- molto grandi (≥ 1024 bit) per resistere ad attacchi brute-force;
- $p-1$ e $q-1$ devono contenere un fattore primo grande;
- $(p-1, q-1)$ deve essere piccolo – idealmente 2, quindi:

$$\left(\frac{p-1}{2}, \frac{q-1}{2}\right) = 1;$$

- diversi da primi già usati:

$$n_1 = pq_1 \ \wedge \ n_2 = pq_2 \implies p = (n_1, n_2).$$

- non troppo vicini tra loro, altrimenti si può fare un attacco brute-force che cerca i fattori vicino a $\sqrt{n}$.

Attacco con p e q vicini

$$\left(\frac{p+q}{2}\right)^2 = \left(\frac{p-q}{2}\right)^2 + n$$

$$\left(\frac{p+q}{2}\right)^2 - n = \underbrace{\left(\frac{p-q}{2}\right)^2}_{>0}$$

$$\left(\frac{p+q}{2}\right)^2 > n \qquad \frac{p+q}{2} > \sqrt{n}$$

quindi $\left(\frac{p+q}{2}\right)^2 - n$ è un quadrato perfetto, e si possono cercare gli interi $> \sqrt{n}$ fino a trovare z tale che

$$z^2 - n = w^2,$$

ovvero $z^2 - n$ è un quadrato perfetto. Allora se $p - q \sim \log n$ probabilmente z è $(p+q)/2$, quindi

$$z = \frac{p+q}{2} \quad w = \frac{p-q}{2} \qquad p = z + w \quad q = z - w.$$

Per questo è opportuno che $p - q \sim n^\epsilon$ con $0 < \epsilon < 1$, cioè la distanza è polinomiale rispetto a n.