RSA: scelta di e

- non può essere troppo piccolo: se $m^e < n$ non interviene la riduzione in modulo e per decifrare si calcola (velocemente) una normale radice e-esima;
- se $e = \frac{\phi(n)}{k} + 1$ per qualche k tale che $k \mid p-1$ e $k \mid q-1$, allora

  $$(m, n) = 1 \implies m^e \bmod n = m,$$

  quindi il messaggio non viene cifrato. In particolare $k = 2$ soddisfa sempre le condizioni, quindi

  $$e \neq \frac{\phi(n)}{2} + 1.$$

  Per questo si preferiscono p e q tali che $(p-1, q-1) = 2$ (o comunque è piccolo).

Attacco con lo stesso valore di e

Scenario: almeno e utenti che hanno scelto lo stesso valore di e che ricevono lo stesso messaggio m

$$\begin{aligned} u_1 &: \quad c_1 = m^e \bmod n_1 \\ u_2 &: \quad c_2 = m^e \bmod n_1 \\ &\vdots \\ u_e &: \quad c_e = m^e \bmod n_e \end{aligned}$$

con $m < n_i$ per ogni i.

Supponiamo che $\forall i, j \,.\, (n_i, n_j) = 1$. Se non è così riusciamo a fattorizzare i due moduli che non sono coprimi (caso di riuso di un primo, da evitare nella scelta di p e q).

Allora, fissato

$$n = \prod_{i=i}^{e} n_i,$$

per il teorema cinese del resto:

$$\exists! m' < n \,.\, m' \equiv m^e \mod n$$

e m' si può calcolare in tempo polinomiale.

$$\begin{aligned} m' &\equiv m^e \mod n \\ m' \bmod n &= m^e \bmod n \\ m' &= m^e \bmod n \qquad & m' < n \\ m' &= m^e & m^e < n_1 \cdots n_e = n \\ m &= \sqrt[e]{m'} \end{aligned}$$

Soluzioni:

- scegliere e grandi in modo da rendere improbabili scelte uguali;
- aggiungere padding diverso al messaggio per ogni utente con la stessa e.