RSA: attacco common modulus

Scenario: due utenti u_1, u_2 con chiavi pubbliche (e_1, n) e (e_2, n) (stesso n). Se $(e_1, e_2) = 1$ e gli utenti ricevono lo stesso messaggio m, il crittoanalista può calcolare in tempo polinomiale i coefficienti dell'identità di Bézout r e s tali che:

$$re_1 + se_2 = 1$$

con $r < 0$, $s > 0$ senza perdita di generalità.
Quindi:

$$\begin{aligned} m &= m^{re_1+se_2} \\ &= m^{re_1+se_2} \bmod n && m < n \\ &= (m^{re_1} \bmod n)(m^{se_2} \bmod n) \bmod n \\ &= (\underbrace{m^{e_1} \bmod n}_{c_1})^r (\underbrace{m^{e_2} \bmod n}_{c_2})^s \bmod n \\ &= c_1^r c_2^s \bmod n \end{aligned}$$

visto che $s > 0$, c_2^s si calcola in tempo polinomiale con quadrature successive; per c_1^r:

- se $(c_1, n) = 1$ si calcola c_1^{-1} in tempo polinomiale con l'algoritmo di Euclide e si eleva alla $|r|$ con QS;
- altrimenti abbiamo trovato un divisore di n, e quindi la sua fattorizzazione.