UNIVERSITAT POLITÈCNICA DE CATALUNYA

3/3

☐ E.T.S. d'Enginyeria de Telecomunicació de Barcelona

☐ E.T.S. d'Enginyers de Camins, Canals i Ports de Barcelona

☐ Facultat d'Informàtica de Barcelona

Pàgina _____ de _____

Titulació

Assignatura

Sanfeliu Ichihashi — Cognoms

Joel — Nom

[redacted] — DNI

③ Donat $N, d, e$ i $e=3$ podem calcular la factorització de $N$ eficientment.

Sabem que al RSA $N = p \cdot q$, llavors si donem quin primer és $p$ i $q$ hem trobat la factorització d'$N$.

① $d < \phi(N) \Rightarrow ed < e\phi(N) \Rightarrow 3d < 3\phi(N)$

② $ed \equiv 1 \bmod(\phi(N)) \Rightarrow 3d \equiv 1 \bmod(\phi(N)) \Rightarrow$

$\Rightarrow 3d = 1 + K \cdot \phi(N)$ on $K \in \mathbb{Z}^+$

Per ① i ② $\Rightarrow 3\phi(N) > 3d = 1 + K \cdot \phi(N) > K \cdot \phi(N)$

$\Rightarrow K < 3$ i $K \neq \emptyset$ per les propietats del producte, ja que altrament no es satisfà l'equació

Llavors sabem que $\begin{cases} K=1 \\ K=2 \end{cases}$, i aillant $\phi(N)$ a l'equació

sabem que $\phi(N) = \frac{3d-1}{K}$.

Tenim 2 candidats:

$$c_1 = \frac{3d-1}{1} \qquad c_2 = \frac{3d-1}{2}$$

Resolem el següent sistema d'equacions:

$$\phi(N) = (p-1)(q-1) \quad \wedge \quad N = p \cdot q.$$

$$p = \frac{N}{q} \Rightarrow \phi(N) = \left(\frac{N}{q} - 1\right)(q-1) \Leftrightarrow$$

$$\Leftrightarrow \phi(N) = \left(\frac{N-q}{q}\right) \cdot (q-1) \Leftrightarrow$$

$$\Leftrightarrow q \cdot \phi(N) = Nq - N - q^2 + q \Leftrightarrow$$

$$\Leftrightarrow q^2 + q\cdot\phi(N) - Nq - q + N = 0 \Leftrightarrow$$

$$\Leftrightarrow q^2 + q(\phi(N) - N - 1) + N = 0.$$

Sabem $N$ i $\phi(N)$. Si resolem aquesta equació amb els candidats $c_1$ i $c_2$ trobarem $q$. i després podrem trobar $p = \frac{N}{q}$.

Calcular la factorització de $N$ és eficient ja que hem de resoldre una equació de segon grau que es pot fer en temps polinòmic

ORL