Parcial1-AA-Problema7

Oriol Miró López-Feliu

April 2023

1 Problema 7

> *Espiant RSA.* Suposeu que en el sistema RSA l'espia Eve aconsegueix (N, d), la clau privada d'Alice. La clau pública d'Alice és (N, e) amb $e = 3$. Demostreu que per aquesta clau pública, l'espia Eve pot calcular eficientment la factorització de N.

Suposem que l'Eve ha obtingut la clau privada (N, d) de l'Alice en el sistema RSA, on $N = pq$ per a alguns nombres primers p i q. Demostrem que l'Eve pot factoritzar eficientment N usant la clau pública (N, e) amb $e = 3$ i la clau privada (N, d) de l'Alice.

Com que la clau pública de l'Alice és (N, e) amb $e = 3$, tenim:

$$d < \phi(N) \implies 3 * d < 3 * \phi(N) \ (1)$$

$$ed \equiv 1 \pmod{\phi(N)} \implies 3d = 1 + k * \phi(N) \text{ per un } k \in \mathbb{Z}^+ \ (2)$$

$$(1) \text{ y } (2) \implies 3 * \phi(N) > 3 * d = 1 + k * \phi(N) > k * \phi(N)$$

$$\implies$$

$$3 * \phi(N) > k * \phi(N) \implies k < 3$$

Com $k \in \mathbb{Z}^+$ i $k \neq 0$, desde aquí es poden donar dos casos: $\begin{cases} 1) k = 1 \\ 2) k = 2 \end{cases}$

Per els dos casos podem calcular un candidat a $\phi(N)$ com a $\phi N = \frac{3d-1}{k}$.

Sigui $c_1 = \frac{3d-1}{1}$ i $c_2 = \frac{3d-1}{2}$, com sabem que $\phi(N) < N$ i a més que es un número proper a N, assignem $\phi(N)$ com el candidat inferior a N més proper a aquest.

Una vegada tenim N i ϕN, podem simplement resoldre el seguent sistema

d'equacions:

$$N = pq \implies p = \frac{N}{q}$$
$$\phi(N) = (p-1)(q-1)$$
$$\implies$$
$$\phi N = (\frac{N}{q} - 1)(q-1) = N - \frac{N}{q} - q + 1 \implies$$
$$q\phi N = qN - N - q^2 + q \implies$$
$$q^2 + (\phi N + N - 1)q + N = 0$$

I després només hauriem de resoldre l'equació cuadrática per obtenir q, i computar $p = \frac{N}{q}$

Hem doncs demostrat que, donats N, d, e, podem obtenir eficientment la factorització de N, p, q.