# 2021-06-08

Jun 8, 11:18 AM — IIC 3253

Recordatorio RSA:

$P, Q$ primos grandes, $N := P \cdot Q$

$\phi(N) = (P-1)(Q-1)$

$d \cdot e \equiv 1 \mod \phi(N)$

$(d, N)$ llave pública

$(e, N)$ llave privada

$Enc((d,N), m) = m^d \mod N =: c$

$m \in \{0, \ldots, N-1\}$

$Dec((e,N), c) = c^e \mod N = m$

$m^{d \cdot e} \mod N = 1$.

---

V genera $(S_K, P_K)$

A genera $m_0, m_1$

V toma al azar $b \in \{0,1\}$ y envía a A $Enc(P_K, m_b)$

A decide si $b = 0$ ó $b = 1$ y gana si le acierta.

A puede ganar fácil, la llave pública es pública!!!...

Introducir algo "aleatorio" podría ayudarnos...

---

Elgamal