

Matemàtiques de la seguretat

RSA 1970 Rivest, Adi Shamir y Len Adelman

Generem un **valor** n com producte de dos **nombres primers** p i q ($n=p \cdot q$) i un valor e de manera que $\text{mcd}((p-1)(q-1), e)=1$ (*).

En principi tothom coneix el valor de n i el valor de e (no donarem mai els valors p i q) p i q s'anomenen nombres RSA. El parell (n, e) es coneix com clau pública.

El missatge numèric m s'envia com $M = m^e \pmod{n}$. Per xifrar cal e .

Construïm un (únic) valor d –anomenat clau privada- que verifiqui $d \cdot e = 1$ en mòdul $(p-1)(q-1)$ -sabem que existeix pel fet (*)-. Per descifrar cal d i per trobar d ens cal p i q . El secret de l'espia es descomposar n com a producte de p i q .

Aleshores es verifica que:

$$m = M^d = (m^e)^d = m \pmod{n}$$

$p=3$ y $q=11$, $n=33$. $\varphi(33) = (3-1) \cdot (11-1) = 20$, en aquest cas $e=7$ La clau pública serà $(33, 7)$. La clave privada d que serà l'invers de 7 en mòdul 20 , un simple càlcul ens mostra que $7 \cdot 3 \equiv 1 \pmod{20}$, es a dir $d=3$.

Imaginem que en un cert alfabet el dígit “9” és la paraula “SI” i la cifra “15” significa “NO”. Observem el següent exemple:

Missatge numèric que enviem	Element que circula per la xarxa	El receptor sap que $e=7$ ja que e és tal que $ed=1$ mòdul $(p-1)(q-1)$. Per tant li cal saber p i q . Per això ha de saber escriure n com $n=pq$		
9	$9^7 = 4782969 \equiv 15 \pmod{33}$	$15^3 = 3375 \equiv 9 \pmod{33}$		

Mostraremos un ejemplo en el que los cálculos han sido realizados con ordenador, en concreto con el programa de cálculo simbólico MAPLE:

Sea $p=23$ y $q=17$, tenemos que $n=391$. $\varphi(391) = (23-1) \cdot (17-1) = 352$, escogemos e de manera que no tenga divisores comunes con 352, por ejemplo $e=3$. La clave (pública) que ofrecemos al emisor será $(391,3)$.

Nosotros tenemos la clave privada d que será el inverso de 3 módulo 352, un simple cálculo nos muestra que $235 \cdot 3 \equiv 1 \pmod{352}$, con ello $d=235$.

Supongamos que el emisor nos manda el mensaje "34", codificado –según el algoritmo RSA- circulará por el canal:

$$34^3 \equiv 204 \pmod{391} \text{ -se utiliza } e \text{ para cifrar-}$$

Para descifrarlo simplemente realizamos:

$$204^{235} \equiv 34 \pmod{391} \text{ -se utiliza } d \text{ para descifrar-}$$