El sistema RSA

a) Sistemas de clave privada, cuando la clave K se elige secretamente entre los comunicantes.

La función de descifrado, d_k se deduce fácilmente de la función de cifrado e_k.

b) Sistemas de clave pública, la función de cifrado puede ser conocida por todos y escribirse en un directorio.

El receptor es la única persona que conoce la regla para descifrar. En este caso el conocimiento de e_k hace computacionalmente difícil obtener d_k

La idea de un sistema de clave pública se debe a W. Diffie y M.E. Hellman que lo publicaron en 1976.

Multiuser cryptographic techniques, AFIPS Conference Proceedings, 45 (1976), 109-112.

La realización de este sistema se debe a R. Rivest, A. Shamir y L. Adleman en 1977, por eso lo conocemos como el sistema RSA.

A method for obtaining digital signatures and public key criptosystems. Communications of the ACM, 21 (1978), 120-126.

Resultados de Teoría de Números

Definición Supongamos que a, m son enteros positivos si $mcd(a, m) = 1$ decimos que a y m son *primos relativos*.

La función de Euler Dado m un entero positivo, definimos $\varphi(m)$ como el número de enteros $1 \leq a < m$ que son primos relativos con m. Coincide con el número de unidades en el anillo Z_m.

La función de Euler es multiplicativa, i.e. si m y n son enteros positivos primos relativos entonces $\varphi(mn) = \varphi(m)\varphi(n)$.

Si p es un número primo y n un entero positivo $\varphi(p^n) = p^{n-1}(p-1)$

Teorema de Lagrange

Supongamos que G es un grupo multiplicativo de orden n. Entonces el orden de cada elemento divide a n.

Corolario 1

Si $b \in Z_m^*$, entonces $b^{\varphi(m)} \equiv 1\,(mod m)$

Corolario 2 (Fermat) Supongamos

Supongamos que p es primo y $b \in Z_p$. Entonces $b^p \equiv b\,(mod p)$.

Teorema

Si p es primo, entonces Z_p^* es un grupo cíclico.

El sistema RSA

Sea $n = pq$, donde p y q son primos. Sea $\mathcal{P} = \mathcal{C} = Z_n$, y definamos

$$\mathcal{K} = \{(n, p, q, a, b) | n = pq,\ p, q \text{ primos},\ ab \equiv 1\,(mod \varphi(n))\}$$

Para $K = (n, p, q, a, b)$, definimos

$$e_K(x) = x^b\, mod n$$

y

$$d_K(y) = y^a\, mod n$$

$(x, y \in Z_n)$.

Los valores n y b son públicos, y los valores de p, q, a son secretos.