AMPLIACIÓN DE MATEMÁTICAS

SISTEMAS CRITOGRÁFICOS DE CLAVE PÚBLICA.

En un sistema de cifrado convencional, o de **clave simétrica**, tanto la **cifra** como el **descifrado** se hace con la misma **clave**.

Ejemplo 1. *Si a cada letra del alfabeto le hacemos corresponder un número*

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
$\tilde{N}$	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	
14	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*	

tenemos un modo de cifrado, sustituir una letra por un número. Ahora si usamos el sistema "César" de cifrado, que sonsiste en desplazar la asignación del número correspondiente n unidades tendremos 27 *claves posibles, del* 0 *al* 26.

Usaremos el sistema César con clave 3.

$$C \equiv x + 3 \qquad \text{mód} \qquad 27$$

Así la palabra "AVE" se transforma (o se cifra) en

$$\begin{array}{ccccccc} \text{A} & \to & 0+3 & = & 3 & \to & \text{D} \\ \text{v} & \to & 22+3 & = & 25 & \to & \text{Y} \\ \text{E} & \to & 4+3 & = & 7 & \to & \text{H} \end{array}$$

"DYH". Para descifrar el **mensaje** usamos la misma clave 3 con la función inversa a la usada anteriormente

$$x \equiv C - 3 \qquad \text{mód} \qquad 27 \;\Leftrightarrow\; x \equiv C + 24 \qquad \text{mód} \qquad 27$$

y así

$$\begin{array}{ccccccc} \text{D} & \to & 3+24 & \equiv & 0 & \to & \text{A} \\ \text{Y} & \to & 25+24 & \equiv & 22 & \to & \text{V} \\ \text{H} & \to & 7+24 & \equiv & 4 & \to & \text{E} \end{array}$$

El **emisor** y el **receptor** del **mensaje** acuerdan el **método de encriptación** y la **clave** (en el ejemplo de arriba $n \in \mathbb{Z}_{27}$).

Los sistemas de encriptación de **clave pública** usan claves distintas para cifrar y para descifrar: **sistema de claves asimétricas**.

Idea del Procedimiento.

Proceso:

- **M** mensaje
- **C**(M) mensaje cifrado
- **D**(C(M))=M mensaje descifrado

Características del proceso:

1. Tanto el método de cifrado **C** como el de descifrado **D** tienen que ser fácilmente computables.
2. **C** puede ser hecho público, no así **D**, de modo que hecho público **C** no sea posible o sea muy costoso (computacionalmente) conocer **D**.
3. Un emisor envía **C** a otro para que este cifre su mensaje **C(M)** y lo envíe al primero.
4. El primer emisor que conoce **D**, y solo él, puede descifrar el mensaje cifrado recibido

$$\mathbf{D}(C(M)) = \mathbf{M}.$$

Historia:

En 1978 Rivest, Shamir y Adelman describen un sistema de clave pública, el R.S.A (¡que coincidencia de iniciales!). Esta sistema es, aún hoy, el sistema de encriptación de clave pública más conocido y que parece que sigue conservando su seguridad.

Elementos matemáticos que se emplean:

1. Dado $n \in \mathbb{N}$, para conocer $\phi(n)$, el valor de la función de Euler en n, se necesita conocer la descomposición en potencias de primos de n

   $$n = p_1^{r_1} p_2^{r_2} .....p_k^{r_k}.$$

   Lo cuál es muy costoso computacionalmente.
2. $$a^{\phi(n)} \equiv 1 \qquad \text{mód} \qquad n$$

   para todo $a \in \mathbb{Z}$ con $m.c.d.(a, n) = 1$.

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: Cesar_Ruiz@mat.ucm.es