R.S.A.

Vamos a decribir brevemente el algoritmo R.S.A.

1. Se toman dos púmeros **primos** p y q "grandes" y del mismo orden de cifras. Se considera
$$n = pq.$$
2. Se selecciona $d \in \mathbb{Z}^*_{\phi(n)}$ de forma aleatoria. ($\phi(n) = (p-1)(q-1)$ y tiene que ocurrir que $m.c.d.(d, \phi(n)) = 1$).
3. Se determina
$$e \in \mathbb{Z}^*_{\phi(n)} \qquad \text{de modo que} \qquad ed \equiv 1 \text{ mód } \phi(n).$$
Observemos que si $m.c.d.(d, \phi(n)) = 1$, entonces el lema de Bezout (y por tanto el algoritmo de Euclides) nos dicen como calcular $e, v, \in \mathbb{Z}$ de modo que
$$1 = ed + v\phi(n).$$
4. Se hacen públicos e y n (**claves públicas**) y se ocultan d, p y q. Observemos que conocido n no es fácil calcular $\phi(n)$. Para ello hay que descomponerlo en factores primos. Y sin conocer $\phi(n)$ no se puede deducir d a partir de e.
5. El **mensaje** que se quiere enviar es $\mathbf{m}$ con $1 < \mathbf{m} \leq n-1$ y con $\mathbf{m} \in \mathbb{Z}^*_n$.
6. La **cifra C** es
$$\mathbf{C(m)} \equiv m^e \text{ mód } n.$$
7. El descifrado **D** es
$$\mathbf{D}(k) \equiv k^d \text{ mód } n.$$
y así
$$\mathbf{D(C(m))} \equiv m^{de} \text{ mód } n.$$

Teorema 1. *En las condiciones anteriores*
$$\boldsymbol{D(C(m))} = m^{de} \equiv m \text{ mód } n.$$

Demostración: Recordemos que

- $ed \equiv 1$ mód. $\phi(n)$.
- $m \in \mathbb{Z}^*_n$.
- $m^{\phi(n)} \equiv 1$ mód. n.

Entonces se tiene que

$$\mathbf{D(C(m))} = m^{de} = m^{1+k\phi(n)} = m(m^{\phi(n)})^k \equiv m \text{ mód } n \ \square$$

Ejemplo 1. *Tomemos los números primos* 3 *y* 11*, consideremos* $n = 3 \times 11 = 33$*, luego*

$$\phi(33) = (3-1) \times (11-1) = 20.$$

Consideremos $d = 7$*. Como m.c.d.*$(7, 20) = 1$*, el algoritmo de Euclides nos permite calcular el inverso de* 7 *en* $(\mathbb{Z}_{20}\backslash\{0\}, \times)$.

i	0	1	2	3	4	
r_i	20	7	6	1	0	
q_i		2	1	1		
α_i	1	0	1	-1		
β_i	0	1	-2	3		

Así $3 \times 7 + (-1) \times 20 = 21 \equiv 1$ mód. $20 = \phi(33)$. Luego hemos construido las claves públicas: 33 y 3.

Si trabajamos en $(\mathbb{Z}_{33}^*\backslash\{1\}, \times)$, solo podemos enviar mensajes con 19 carácteres distintos ($|\mathbb{Z}_{33}^*\backslash\{1\}| = \phi(33) - 1 = 19$).

Supongamos que los carácteres que utilizamos son

A	B	C	D	E	F	G	H	I	J	K	L	M	N
2	4	5	7	8	10	13	14	16	17	19	20	23	25
Ñ	O	P	Q	R									
26	28	29	31	32									

Ahora queremos transmitir en secreto el mensaje: ALGEBRA. Para ello usamos las claves públicas 3 y 11. Así

$$\begin{array}{lllllllll}
\text{A} \to 2, & C(2) & = & 2^3 & \equiv & 8 \text{ mód } 33; & \to & E \\
\text{L} \to 20, & C(20) & = & 20^3 = 10^3 \times 2^3 & \equiv & 10 \times 8 \equiv 14 \text{ mód } 33; & \to & H \\
\text{G} \to 13, & C(13) & = & 13^3 \equiv (-20)^3 & \equiv & 19 \text{ mód } 33; & \to & K \\
\text{E} \to 8, & C(8) & = & 8^3 \equiv 31 \times 8 & \equiv & 17 \text{ mód } 33; & \to & J \\
\text{B} \to 4, & C(4) & = & 4^3 & \equiv & 31 \text{ mód } 33; & \to & Q \\
\text{R} \to 32, & C(32) & = & 32^3 \equiv (-1)^3 & \equiv & 32 \text{ mód } 33; & \to & R \\
\text{A} \to 2, & C(2) & = & 2^3 & \equiv & 8 \text{ mód } 33; & \to & E
\end{array}$$

ALGEBRA se transforma en EHKJQRE que es el mensaje que se transmite. El receptor del mensaje, como conoce $d = 7$, es capaz de reconstruir el mensaje original. Veámoslo para el primer carácter. Tengamos en cuenta que $8^2 = 64 \equiv 31 \equiv (-2)$ mód 33.

$$\text{E} \to 8, \quad D(8) = 8^7 \equiv (-2)^3 \times 8 \equiv 2 \text{ mód } 33; \to A.$$

Referencias

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