RSA

Creación de claves en el sistema RSA

RSA - Claves

Pero antes….

RSA - Claves

Se buscan dos primos lo suficientemente grandes: p y q, con $p \neq q$

En la realidad estos números tienen centenares de dígitos.

En nuestro ejemplo serán:

$p = 11$ y $q = 23$

RSA - Claves

A partir de estos números se obtiene:

$$n = p * q$$

$$\emptyset = (p - 1) * (q - 1)$$

En nuestro ejemplo:

$$n = 11 * 23 = 253$$

$$\emptyset = (p - 1) * (q - 1) = 220$$

donde: $(p - 1) = 10$ y $(q - 1) 22$

RSA - Claves

Se busca un número 'e' (impar) tal que no tenga múltiplos comunes con ∅.

Para esto se selecciona de forma aleatoria un entero 'e', tal que $1 < e < \emptyset$, MCD(∅, e) = 1.

En nuestra ejemplo:

e = 3

MCD (220, 3) = 1

RSA - Claves

Se calcula el exponente privado de RSA

$d = inv (e, \emptyset)$

$d = inv (3, 220) = 147$

Ver ejercicios del práctico.

Y hacer este también como ejercicio.

RSA - Claves

Clave pública:

$$(e,n) = (3,253)$$

Clave privada:

$$(d,n) = (147,253)$$

RSA - Claves

Cifrado:

$$C = M^e \bmod n$$

Descifrado:

$$C^d \bmod n = M$$

RSA - Claves

Asignemos a cada letra un número:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Con las claves del ejemplo vamos a cifrar el mensaje M:

S	E	G	U	R	I	D	A	D
18	4	6	20	17	8	3	0	3

RSA - Claves

Cifrado con Clave Pública: (3,253)

M = 18 4 6 20 17 8 3 0 3

$18^3 = 5832 \bmod 253 = 13$

$4^3 = 64 \bmod 253 = 64$

$6^3 = 216 \bmod 253 = 216$

$20^3 = 8000 \bmod 253 = 157$

$17^3 = 4913 \bmod 253 = 106$

$8^3 = 512 \bmod 253 = 6$

$3^3 = 27 \bmod 253 = 27$

$0^3 = 0 \bmod 253 = 0$

$3^3 = 27 \bmod 253 = 27$

C = 13 64 216 157 106 6 27 0 27

RSA - Claves

Descifrado con Clave Privada: (147,253)

C = 13 64 216 157 106 6 27 0 27

$13^{147} \mod 253 = 18$

$64^{147} \mod 253 = 4$

$216^{147} \mod 253 = 6$

$157^{147} \mod 253 = 20$

$106^{147} \mod 253 = 17$

$6^{147} \mod 253 = 8$

$27^{147} \mod 253 = 3$

$0^{147} \mod 253 = 0$

$27^{147} \mod 253 = 3$

S	E	G	U	R	I	D	A	D
18	4	6	20	17	8	3	0	3

M = 18 4 6 20 17 8 3 0 3

RSA - Claves

FIN