RSA ejercicio simple

Planteamiento

Vamos a utilizar la siguiente tabla para el reemplazo de letras por sus correspondientes valores numéricos.

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

Hay que leer dos variables p y q, para armar la siguiente operación:

$$F(c) = (p*k+q) \bmod 27$$

Donde **c** es valor para el carácter cifrado y **k** el valor según la tabla del mensaje a cifrar

Por ejemplo, si el mensaje a cifrar fuera: UNION

U	N	I	O	N
21	13	8	15	13

Cada valor hallado de cada carácter corresponde a un valor k_i que nos permitirá encontrar el respectivo carácter cifrado C_i

Para el caso, consideremos el hecho de que p=17 y q=27

Por tanto: % //

U = 21 => (p*21+q) mod 27 => C_1= (17*21+27) mod 27 = 6 Y_1=14

N = 13 => (p*13+q) mod 27 => C_2= (17*13+27) mod 27 = 5 Y_2=9

I = 8 => (p*8+q) mod 27 => C_3= (17*8+27) mod 27 = 1 Y_3=6

O = 15 => (p*15+q) mod 27 => C_4= (17*15+27) mod 27 = 12 Y_4=10

N = 13 => (p*13+q) mod 27 => C_5= (17*13+27) mod 27 = 5 Y_5=9

$C_1C_2C_3C_4C_5$ = 6 5 1 12 5 = G F B M F

$Y_1Y_2Y_3Y_4Y_5$ = 14 9 6 10 9 = Ñ J G K J

Mensaje Cifrado: $C_1Y_1C_2Y_2C_3Y_3C_4Y_4C_5Y_5$ = G Ñ F J B G M K F J

Mensaje original: UNION

Mensaje cifrado: GÑFJBGMKFJ