Ejemplo: algoritmo RSA

1. *Generación de claves*

$p = 101$, $q = 113 \Rightarrow n = 11413$ y $\varphi(n) = 100 \times 112 = 11200$.

Elegimos d (exponente de desencriptación) que tiene que cumplir con la siguiente condición: $\gcd(\varphi(n), d) = 1$. Un posible d es 6597.

Por último, calculamos el inverso modular del exponente d utilizando el algoritmo de Euclides. Es decir, $e \times d = 1 \bmod \varphi(n)$

Haciendo las cuentas obtenemos: $e = 3533$

Clave Pública = (e,n) / Clave Privada (d,n)

2. *Encriptación ($E_k(m) = m^e \bmod n$)*

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

M = OPERACION = 15165181391514 … Ahora debemos dividir el mensaje plano en bloques de tamaño máximo n -1

$m_1 = 1516 \quad \rightarrow c_1 = 1516^{3533} \bmod 11413 = 5556$
$m_2 = 5181 \quad \rightarrow c_2 = 5187^{3533} \bmod 11413 = 7771$
$m_3 = 3915 \quad \rightarrow c_3 = 3915^{3533} \bmod 11413 = 1434$
$m_4 = 14 \quad \rightarrow c_4 = 14^{3533} \bmod 11413 = 7289$

3. *Desencriptación ($D_k(c) = c^d \bmod n$)*

$c_1 = 5556 \quad \rightarrow m_1 = 5556^{6597} \bmod 11413 = 1516$
$c_2 = 7771 \quad \rightarrow m_2 = 7771^{6597} \bmod 11413 = 5181$
$c_3 = 1434 \quad \rightarrow m_3 = 1434^{6597} \bmod 11413 = 3915$
$c_4 = 7289 \quad \rightarrow m_4 = 7289^{6597} \bmod 11413 = 14$