1.) $p = 7 \quad q = 11$

$n = 77$

$r = (p-1)(q-1) = 60$

2.) $e = 37 \Rightarrow \gcd(37, 60) = 1$

r	e
60	37
37	23
23	14
14	9
9	5
5	4
4	1
1	0

3.) $d \Rightarrow ed = 1 \bmod r$

$ed + rs = 1$

r	e	s	d
60	37	-8	13
37	23	5	-8
23	14	-3	5
14	9	2	-3
9	5	-1	2
5	4	1	-1
4	1	0	1
1	0	1	0

$y = x' - \left\lfloor \frac{q}{b} \right\rfloor r'$

4.) $c = m^e \pmod n \qquad m = c^d \pmod n$

$X = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$ $\Longrightarrow$ $Z = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$

$Y = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$

$l_m = \begin{cases} i_m & \text{si } i_m < j_m \\ j_m & \text{de lo contrario} \end{cases}$

$X = 1026859 68 = 2^4 3^5 7^4 11^1$

$Y = 1037337 84 = 2^3 3^7 7^2 11^2$

$Z = 2^3 3^5 7^2 11^1 = 1047816$

Algoritmo Euclid

$$GCD(a,b) = \begin{cases} GCD(b, a \% b) & \text{si } b \neq 0 \\ a & \text{si } b = 0 \end{cases}$$

GCD(10214, 2366)

a	b
10214	2366
2366	750
750	116
116	54
54	8
8	6
6	2
2	0

$m \cdot n = 1 \pmod p$

$GCD(n,p) = 1 \Rightarrow \exists\ m$

$GCD(a,b) = x \cdot a + y \cdot b$

$$xGCD(a,b) = \begin{cases} g = a,\ x = 1,\ y = 0 & \text{si } b = 0 \\ g, x', y' = xGCD(b, a \% b) & \text{si } b \neq 0 \\ g, x, y = g, y', x' - \left\lfloor \frac{a}{b} \right\rfloor y' \end{cases}$$

$xGCD(10214, 2366)$

a	b	x	y
10214	2366	-306	1321
2366	750	97	-306
750	116	-15	97
116	54	7	-15
54	8	-1	7
8	6	1	-1
6	2	0	1
2	0	1	0

$2 = 10214 \times (-306) + 2366 \times 1321$

Algoritmo RSA (

1.) p y q números primos

$n = p \cdot q$

2.) $r = (p-1)(q-1)$

$e \longrightarrow GCD(e, r) = 1$ coprimos

3.) $d \Rightarrow e \cdot d = 1 \pmod{r}$

inverso modular $ed + s \cdot r = 1$

4) (e, n) llave pública

(d, n) llave privada

Mensaje m $\quad c = m^e \pmod{n}$

$m = c^d \pmod{n}$