a → b
c → x
s → p

casa
xbpb

a b c d e ... z
0 1 2 3 4 25

casa
3

j d

Encriptar
Mensaje -> Codificación

(3+3) mod 26
6 mod 26
6

c → j
a → d

(0+3) mod 26
3 mod 26
3

STOP clave publica (2537,13) --> n = p*q 2537 = 43*59

A=00 B=01 C=02 D=03 E=04 F=05 G=06 H=07 I=08 J=09
K=10 L=11 M=12 N=13 O=14 P=15 Q=16 R=17 S=18 T=19
U=20 V=21 W=22 X=23 Y=24 Z=25

S T O P
18 19 14 15

n = 2537 max 4 numeros 25 25

2525 < 2537 ✓

Vamos hacer modulo con 2537, el problema es que si tenemos un numero mas grande, van a haber dos valores que dan el mismo codificado (pierde información)

$m_1 = 1819$ $m_2 = 1415$

$e = 13$

$C_1 = 1819^{13} \bmod 2537$

$C_2 = 1415^{13} \bmod 2537$

$C_1 = 2081$
$C_2 = 2182$

2081 2182

Teorema

Si p es primo y a no es divisible por p entonces:

$$a^{p-1} \equiv 1 \,(\mathit{mod}\, p).$$

Además,

$$a^{p} \equiv a \,(\mathit{mod}\, p).$$

Calculamos el d

d inverso e mod phi(n)
d inverso e mod (p-1)*(q-1)
d inverso 13 mod 2436

$d = 937$ (n, e) → p, q

$2081^{937} \bmod 2537 = 1819$
$2182^{937} \bmod 2537 = 1915$

Cifre el mensaje UPLOAD empleando el sistema de cifrado RSA con p = 53, q = 61 y e = 17.

A=00 B=01 C=02 D=03 E=04 F=05 G=06 H=07 I=08 J=09
K=10 L=11 M=12 N=13 O=14 P=15 Q=16 R=17 S=18 T=19
U=20 V=21 W=22 X=23 Y=24 Z=25

U P L O A D
20 15 11 14 00 03

Z Z
25 25

$n = 53 * 61$

3233

$2525 < 3233$

$m1 = 2015$ $m2 = 1114$

$m3 = 0003$

$C1 = 2015^{17} \bmod 3233 = 2545$
$C2 = 1114^{17} \bmod 3233 = 2757$
$C2 = 0003^{17} \bmod 3233 = 1211$

$e \bmod \phi(n)$

$17 \bmod (52 * 60)$ $17 \bmod 3120$

$y = 2783$

$m_1 = 2545^{2783} \bmod 3233$

$m_2 = 2787^{2783} \bmod 3233$

$m_3 = 1211^{2783} \bmod 3233$