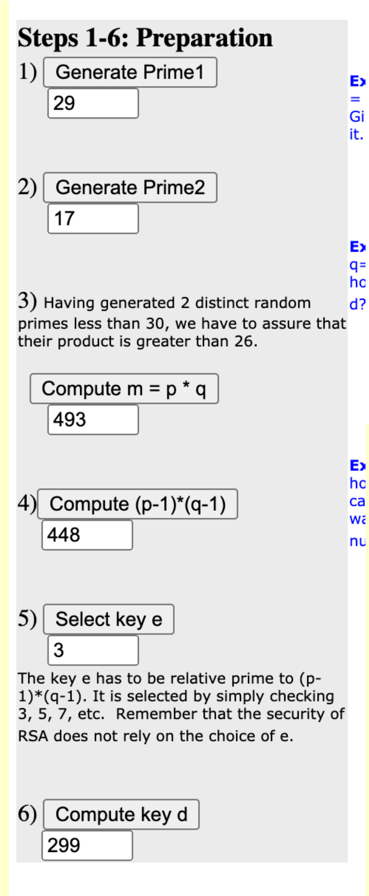
Macedo Madrigal Rodrigo
Temas Selectos de Computación
314676797

Comparativo RSA

Corrida 1:
Programa WEB:



Steps 1-6: Preparation

1) Generate Prime1
29

2) Generate Prime2
17

3) Having generated 2 distinct random primes less than 30, we have to assure that their product is greater than 26.

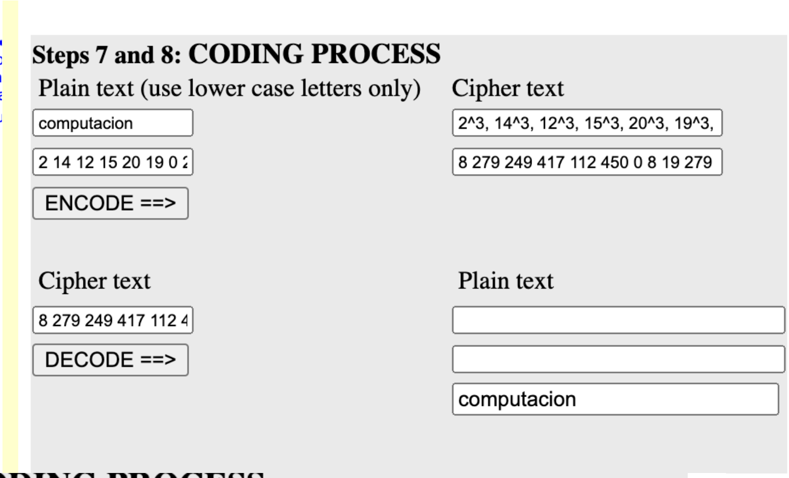
Compute m = p * q
493

4) Compute (p-1)*(q-1)
448

5) Select key e
3

The key e has to be relative prime to (p-1)*(q-1). It is selected by simply checking 3, 5, 7, etc. Remember that the security of RSA does not rely on the choice of e.

6) Compute key d
299



Steps 7 and 8: CODING PROCESS

Plain text (use lower case letters only)
computacion
2 14 12 15 20 19 0 2

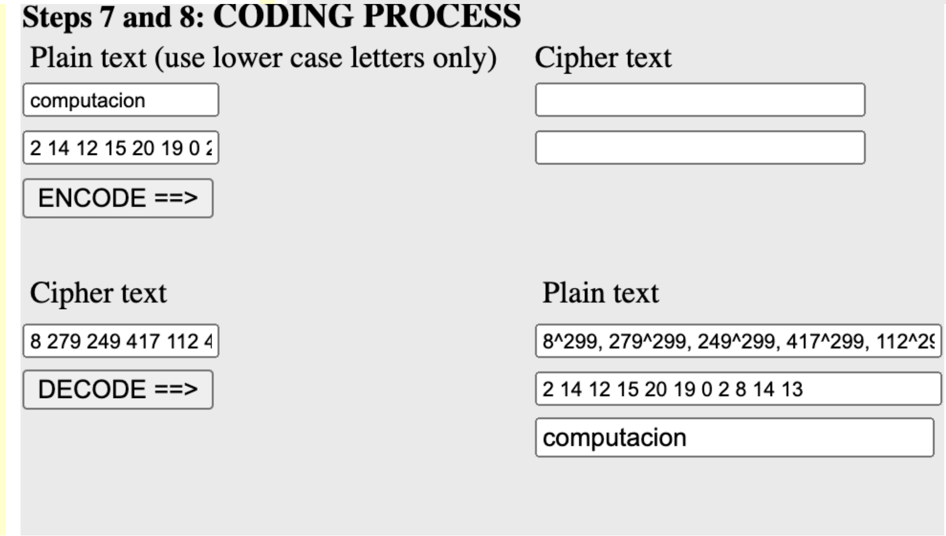
Cipher text
2^3, 14^3, 12^3, 15^3, 20^3, 19^3,
8 279 249 417 112 450 0 8 19 279

ENCODE ==>

Cipher text
8 279 249 417 112 4

DECODE ==>

Plain text
computacion



Steps 7 and 8: CODING PROCESS

Plain text (use lower case letters only)
computacion
2 14 12 15 20 19 0 2

ENCODE ==>

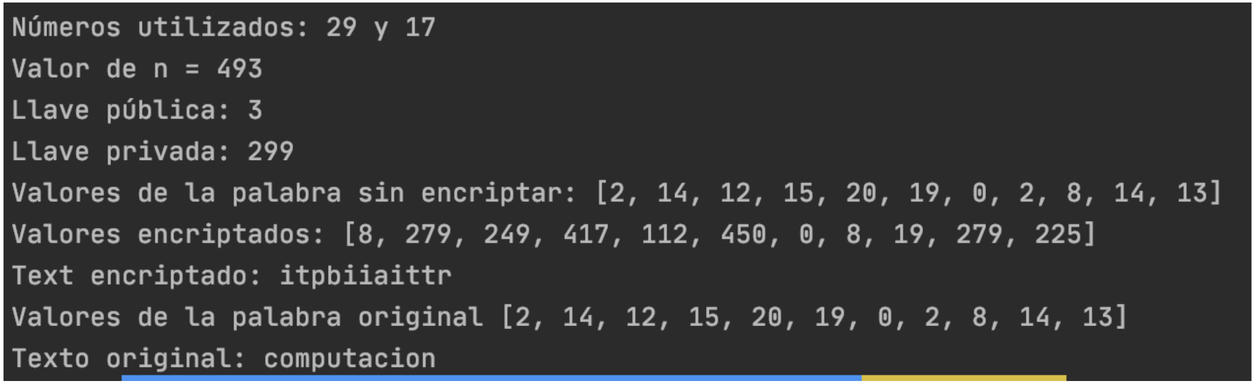
Cipher text

Cipher text
8 279 249 417 112 4

DECODE ==>

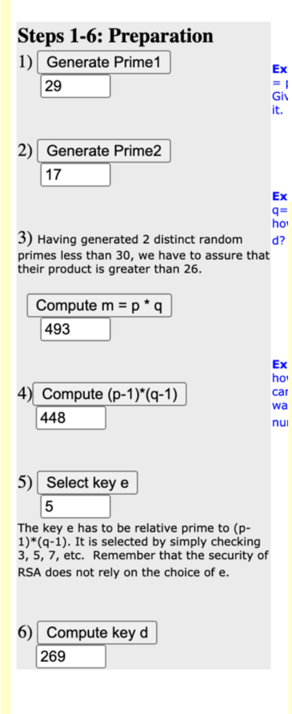
Plain text
8^299, 279^299, 249^299, 417^299, 112^2
2 14 12 15 20 19 0 2 8 14 13
computacion

Corrida programa propio:



```
Números utilizados: 29 y 17
Valor de n = 493
Llave pública: 3
Llave privada: 299
Valores de la palabra sin encriptar: [2, 14, 12, 15, 20, 19, 0, 2, 8, 14, 13]
Valores encriptados: [8, 279, 249, 417, 112, 450, 0, 8, 19, 279, 225]
Text encriptado: itpbiiaittr
Valores de la palabra original [2, 14, 12, 15, 20, 19, 0, 2, 8, 14, 13]
Texto original: computacion
```

Corrida 2:
Programa WEB:



Steps 1-6: Preparation

1) Generate Prime1
29

2) Generate Prime2
17

3) Having generated 2 distinct random primes less than 30, we have to assure that their product is greater than 26.

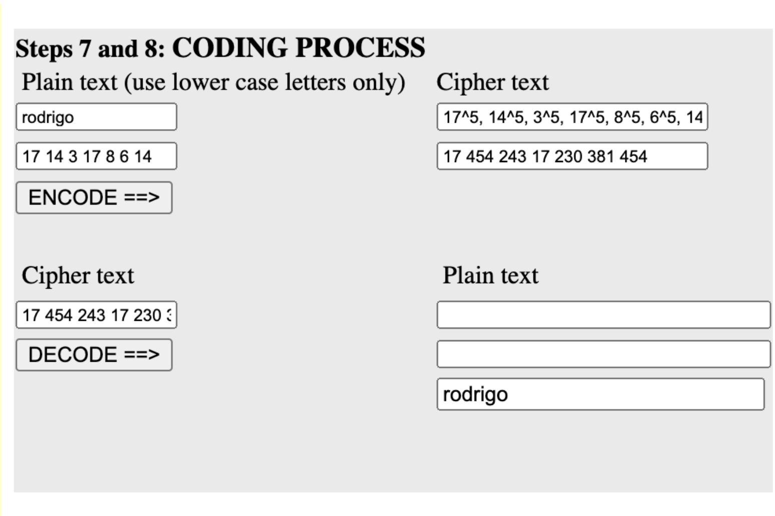
Compute m = p * q
493

4) Compute (p-1)*(q-1)
448

5) Select key e
5

The key e has to be relative prime to (p-1)*(q-1). It is selected by simply checking 3, 5, 7, etc. Remember that the security of RSA does not rely on the choice of e.

6) Compute key d
269



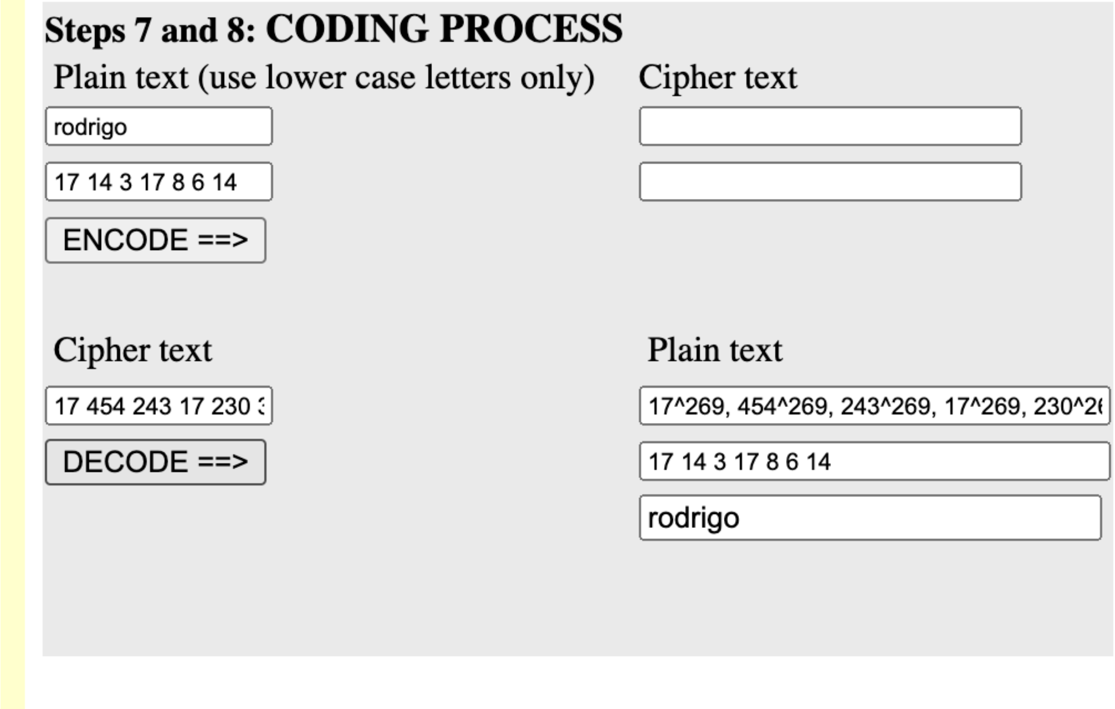
Steps 7 and 8: CODING PROCESS

Plain text (use lower case letters only)
rodrigo
17 14 3 17 8 6 14
ENCODE ==>

Cipher text
17^5, 14^5, 3^5, 17^5, 8^5, 6^5, 14
17 454 243 17 230 381 454

Cipher text
17 454 243 17 230 3
DECODE ==>

Plain text
rodrigo



Steps 7 and 8: CODING PROCESS

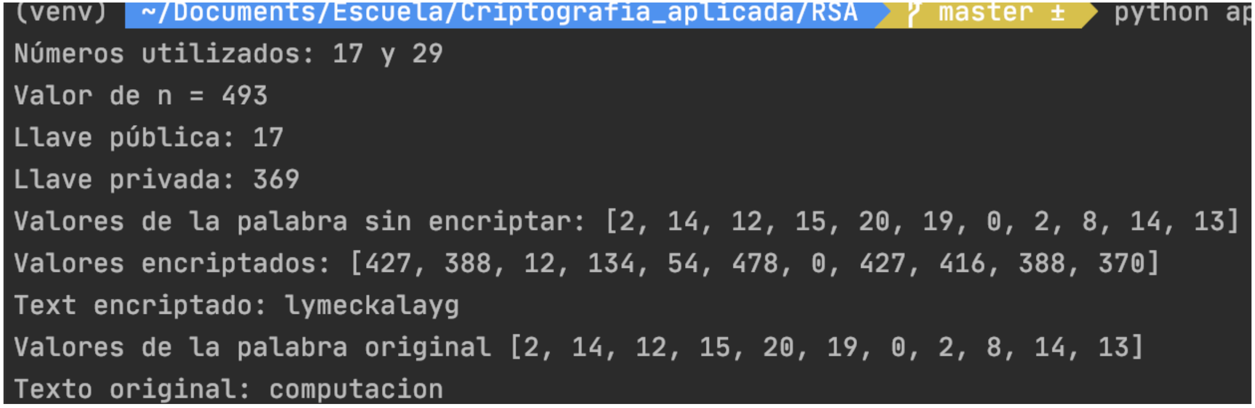
Plain text (use lower case letters only)
rodrigo
17 14 3 17 8 6 14
ENCODE ==>

Cipher text

Cipher text
17 454 243 17 230 3
DECODE ==>

Plain text
17^269, 454^269, 243^269, 17^269, 230^26
17 14 3 17 8 6 14
rodrigo

Corrida programa propio:



```
(venv)  ~/Documents/Escuela/Criptografia_aplicada/RSA   master ±  python ap
Números utilizados: 17 y 29
Valor de n = 493
Llave pública: 17
Llave privada: 369
Valores de la palabra sin encriptar: [2, 14, 12, 15, 20, 19, 0, 2, 8, 14, 13]
Valores encriptados: [427, 388, 12, 134, 54, 478, 0, 427, 416, 388, 370]
Text encriptado: lymeckalayg
Valores de la palabra original [2, 14, 12, 15, 20, 19, 0, 2, 8, 14, 13]
Texto original: computacion
```