

# **Criptografía y Seguridad**

## **Secuencia de Pantallas para la Opción de RSA**

### **Grupo 032**

**Maestro Angel Salvador Pérez Blanco**

**Roberto Treviño Cervantes**

**#1915003**

Presentado el 30 de Octubre de 2023

## Secuencia de Pantallas

1. Seleccionar la opción "b) RSA"

```
*** PIA Criptografia ***

#=> El conjunto de caracteres empleado es el conjunto ASCII con 52 elementos.
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's',
 't', 'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L',
 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

a) Cifrado de César
> b) RSA
c) Información del Programa
d) Imprimir código fuente
e) Salir
```

2. Introducir un número primo para la llave de cifrado

```
*** PIA Criptografia ***

#=> El conjunto de caracteres empleado es el conjunto ASCII con 52 elementos.
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's',
 't', 'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L',
 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

+++ Menu RSA +++
Introduce un número primo, p = 7
```

3. Introducir otro número primo para la llave de cifrado

```
*** PIA Criptografia ***

#=> El conjunto de caracteres empleado es el conjunto ASCII con 52 elementos.
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's',
 't', 'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L',
 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

+++ Menu RSA +++
Introduce un número primo, p = 7
Introduce otro número primo, q = 11
```

4. Recibir la llave pública y privada

```
*** PIA Criptografia ***

#=> El conjunto de caracteres empleado es el conjunto ASCII con 52 elementos.
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's',
 't', 'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L',
 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

+++ Menu RSA +++
Introduce un número primo, p = 7
Introduce otro número primo, q = 11
#=> Llave pública: (7, 77)
#=> Llave privada: (43, 77)
```

5. Para encriptar, seleccionar la opción "a) Encriptar"

```

*** PIA Criptografia ***

#=> El conjunto de caracteres empleado es el conjunto ASCII con 52 elementos.
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's',
 't', 'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L',
 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

+++ Menu RSA +++
Introduce un número primo, p = 7
Introduce otro número primo, q = 11
#=> Llave pública: (7, 77)
#=> Llave privada: (43, 77)
> a) Encriptar
  b) Desencriptar
  d) Regresar

```

6. Introducir el texto plano:

```

*** PIA Criptografia ***

#=> El conjunto de caracteres empleado es el conjunto ASCII con 52 elementos.
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's',
 't', 'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L',
 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

+++ Menu RSA +++
Introduce un número primo, p = 7
Introduce otro número primo, q = 11
#=> Llave pública: (7, 77)
#=> Llave privada: (43, 77)
Introduce el texto a encriptar: text

```

7. Recibir el texto cifrado

```

*** PIA Criptografia ***

#=> El conjunto de caracteres empleado es el conjunto ASCII con 52 elementos.
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's',
 't', 'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L',
 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

+++ Menu RSA +++
Introduce un número primo, p = 7
Introduce otro número primo, q = 11
#=> Llave pública: (7, 77)
#=> Llave privada: (43, 77)
Introduce el texto a encriptar: text
#=> El texto cifrado es: <<68602368>>

```

8. Para desencriptar, seleccionar la opción “b) Desencriptar”

```

*** PIA Criptografia ***

#=> El conjunto de caracteres empleado es el conjunto ASCII con 52 elementos.
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's',
 't', 'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L',
 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

+++ Menu RSA +++
Introduce un número primo, p = 7
Introduce otro número primo, q = 11
#=> Llave pública: (7, 77)
#=> Llave privada: (43, 77)
Introduce el texto a encriptar: text
#=> El texto cifrado es: <<68602368>>

a) Encriptar
> b) Desencriptar
d) Regresar

```

## 9. Introducir el mensaje original

```

*** PIA Criptografia ***

#=> El conjunto de caracteres empleado es el conjunto ASCII con 52 elementos.
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's',
 't', 'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L',
 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

+++ Menu RSA +++
Introduce un número primo, p = 7
Introduce otro número primo, q = 11
#=> Llave pública: (7, 77)
#=> Llave privada: (43, 77)
Introduce el texto a encriptar: text
#=> El texto cifrado es: <<68602368>>

Introduce el texto a desencriptar: 68602368

```

## 10. Recibir el mensaje original