MANUAL CRIPTOMATIC

JORGE ENRIQUE CAMACHO
UNIVERSIDAD NACIONAL DE COLOMBIA
CRIPTOGRAFÍA
PROFESOR: AGUSTIN MORENO

Contenido

1. Introducción
2. Explicación
3. RSA
4. Elgamal
5. Rabin
6. Menezes – Vanstone (curva elíptica)
7. Firma digital RSA
8. Firma digital Elgamal
9. Criptografía visual

Introducción

- Criptomatic es una aplicación desarrollada durante el curso de criptografía en la Universidad Nacional de Colombia. Esta aplicación fue desarrollada con el lenguaje de programación Python y en el entorno de desarrollo Visual Studio Code para la cual se utilizaron diferentes tipos de librerías, y diferentes algoritmos criptográficos como lo son el RSA, Elgamal, Rabin, Menezes-Vanstone, Firmas digitales y criptografía visual. A través de esta presentación se explicara el uso de Criptomatic y sus diferentes funcionalidades

Explicación algoritmos de cifrado

- Los algoritmos RSA, Elgamal, Rabin y Menezes – Vanstone sirven para encriptar y desencriptar textos en plano y se basan en diferentes tipos de dificultades como son la factorización del producto de números primos muy grandes, o encontrar solución al problema del logaritmo discreto. En Criptomatic se presenta una interfaz en la cual se pueden usar estos algoritmos para ingresar datos manualmente o automáticamente y hacer su respectivo cifrado, además sirve para desencriptar mensajes guardados, sabiendo sus respectivas claves publicas y privadas.

Explicación firmas digitales

- Los algoritmos de firma digital como Elgamal y RSA sirven para firmar digitalmente un mensaje a través de los algoritmos de cifrado y poder verificar que la persona que lo ha enviado, es efectivamente la persona que creo el mensaje. La complejidad de estos algoritmos de firma también se basa en la factorización del producto de números primos o el problema del logaritmo discreto y son usados para hacer pagos por internet o verificar transacciones.

Explicación criptografía visual

- Este tipo de criptografía se utiliza para enviar mensajes a través de imágenes generando una cantidad discreta de diferentes transparencias de una imagen, en donde individualmente estas transparencias no dan ninguna información del mensaje original ya que se necesita la totalidad de ellas para sobreponerlas y que el ojo humano sea capaz de entender cual es el mensaje. En Criptomatic se utilizaron solo dos transparencias por imagen y estas imágenes son de tamaño 256 x 212 pixeles, cabe aclarar que Criptomatic encripta y desencripta imágenes.

Algoritmo RSA

Para poder encriptar y desencriptar mensajes con Criptomatic – RSA se debe:

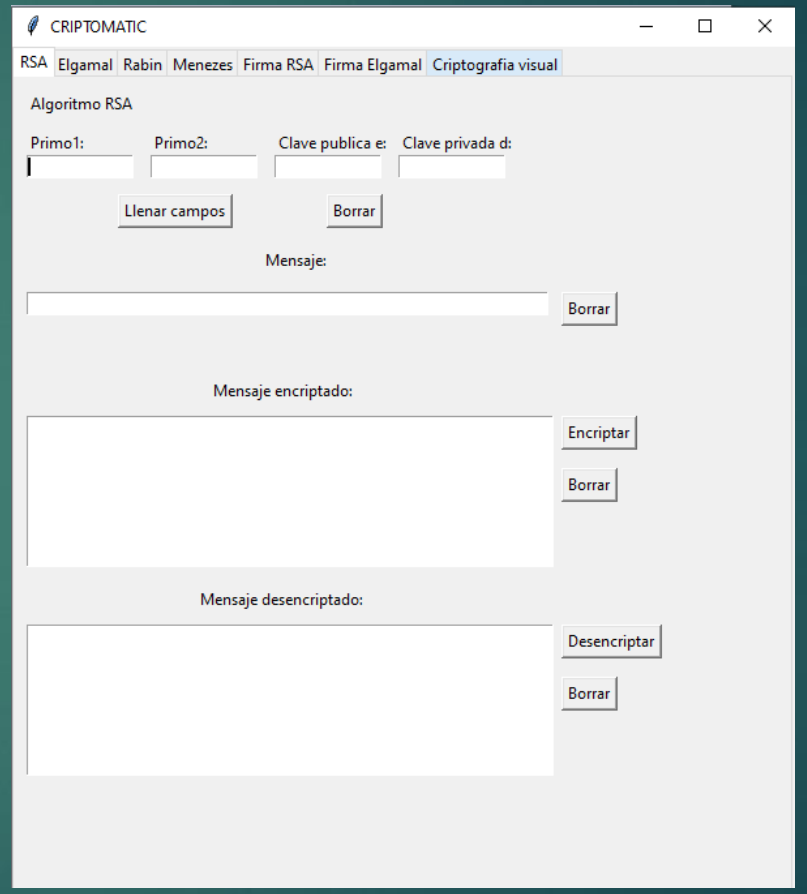
Encriptar

1. Ingresar dos números primos grandes
2. Hallar su respectiva clave publica
3. Hallar su respectiva clave privada
4. Escribir el mensaje
5. Oprimir en el botón encriptar

O llenar los campos automáticamente y seguir desde el 4 paso mencionado anteriormente

Desencriptar

1. Llenar los campos de clave publica y privada
2. Llenar el campo con el mensaje encriptado
3. Oprimir el botón desencriptar



Algoritmo Elgamal

Para poder encriptar y desencriptar mensajes con Criptomatic – Elgamal se debe:

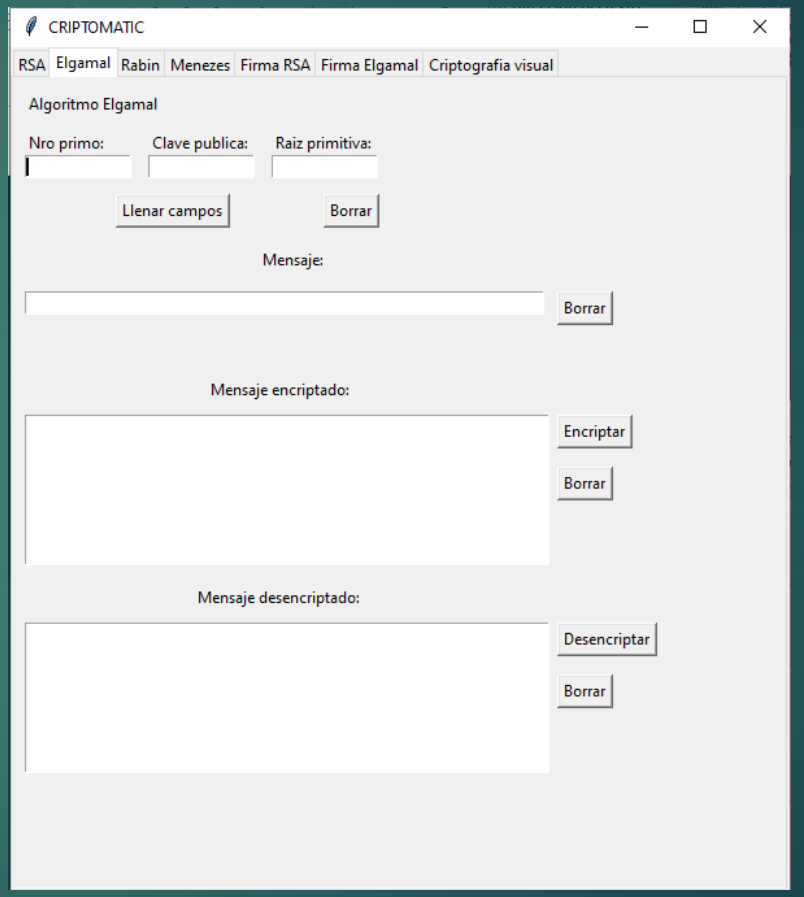
Encriptar

1. Ingresar un número primo grande
2. Hallar su respectiva clave publica
3. Hallar su respectiva raíz primitiva
4. Escribir el mensaje
5. Oprimir en el botón encriptar

O llenar los campos automáticamente y seguir desde el 4 paso mencionado anteriormente

Desencriptar

1. Llenar los campos de clave publica y privada
2. Llenar el campo con el mensaje encriptado
3. Oprimir el botón desencriptar



Algoritmo Rabin

Para poder encriptar y desencriptar mensajes con Criptomatic – Rabin se debe:

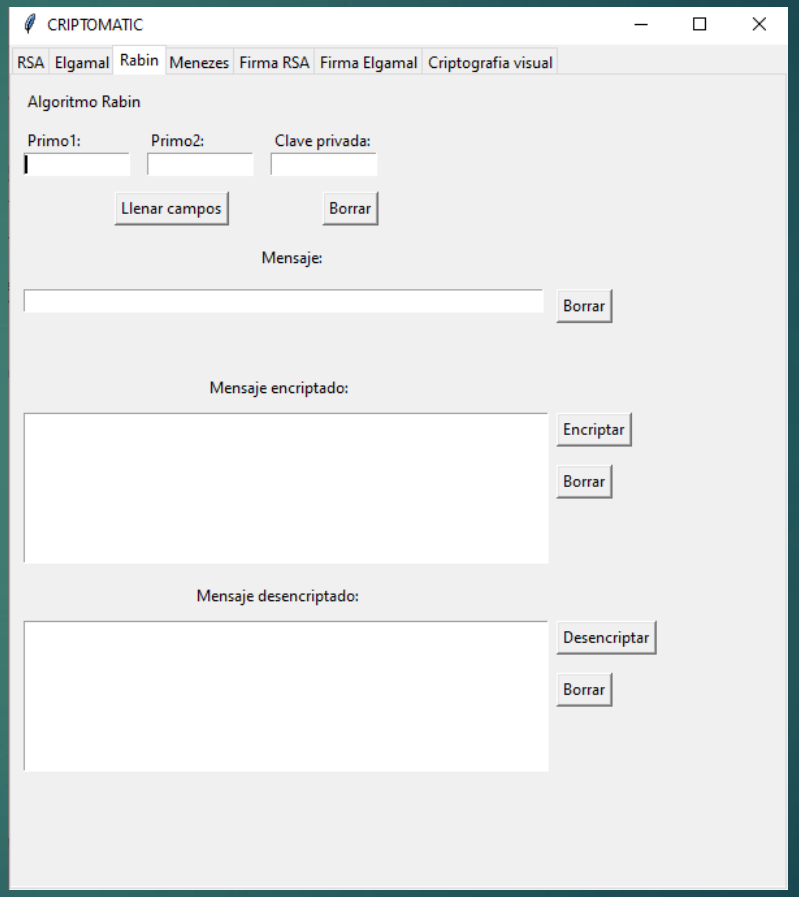
Encriptar

1. Ingresar dos números primos grandes
2. Hallar su respectiva clave privada
3. Escribir el mensaje
4. Oprimir en el botón encriptar

O llenar los campos automáticamente y seguir desde el 3 paso mencionado anteriormente

Desencriptar

1. Llenar los campos de clave publica y privada
2. Llenar el campo con el mensaje encriptado
3. Oprimir el botón desencriptar



Algoritmo Menezes – Vanstone (Curva elíptica)

Para poder encriptar y desencriptar mensajes con Criptomatic – Curva elíptica se debe:

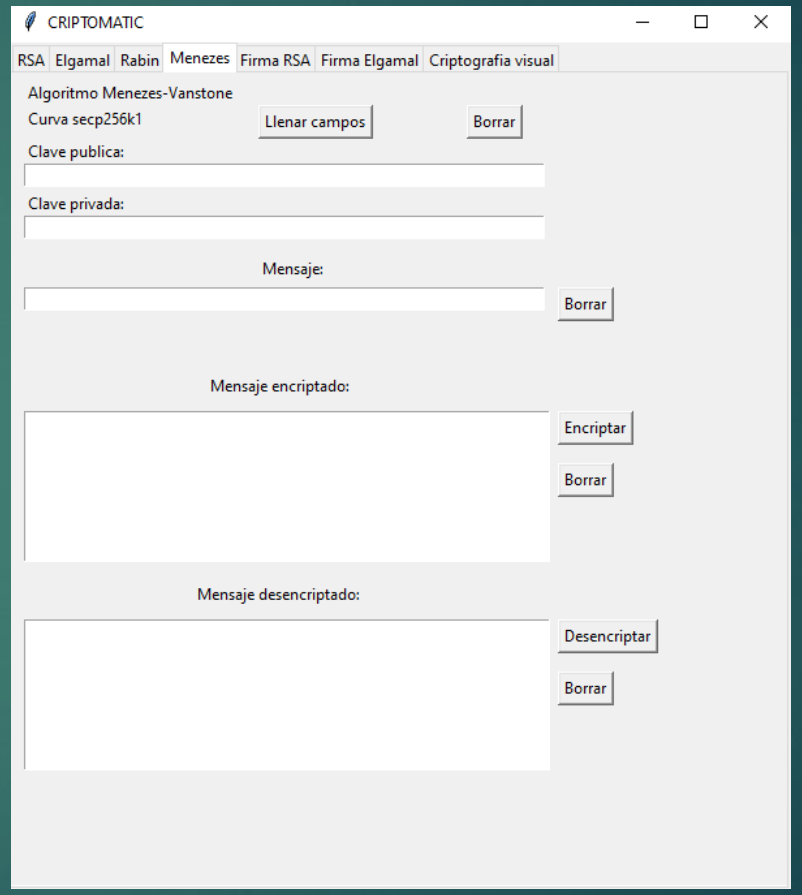
Encriptar

1. Oprimir el botón llenar campos
2. Escribir el mensaje
3. Oprimir en el botón encriptar

Este algoritmo usa la curva elíptica Secp256k y cifra los mensajes basándose en los puntos que genera dicha curva

Desencriptar

1. Llenar los campos de clave publica y privada
2. Llenar el campo con el mensaje encriptado
3. Oprimir el botón desencriptar



Firma Digital RSA

Para poder firmar mensajes con Criptomatic – Firma digital RSA se debe:

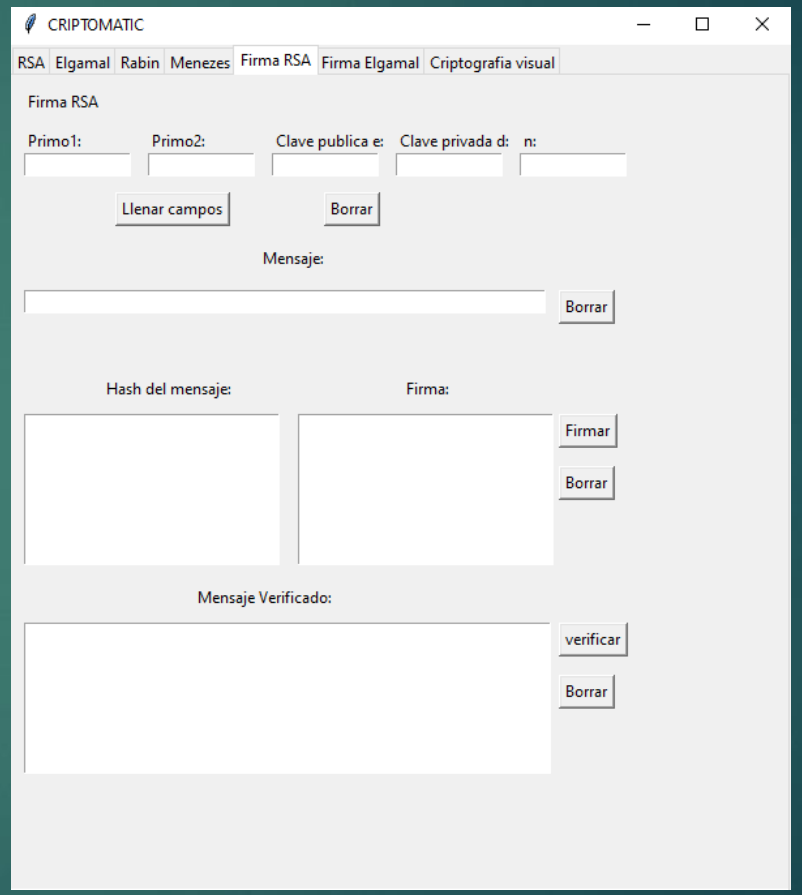
Firmar

1. Ingresar dos números primos grandes
2. Hallar su respectiva clave publica
3. Hallar su respectiva clave privada
4. Calcular el producto de los dos primos anteriores
5. Ingresar el mensaje a firmar
6. Oprimir en el botón firmar

O llenar los campos automáticamente y seguir desde el 5 paso mencionado anteriormente

Verificar

1. Llenar los campos de clave publica y privada
2. Llenar los campos mensaje, hash y firma
3. Oprimir el botón verificar



Firma Digital Elgamal

Para poder firmar mensajes con Criptomatic – Firma digital Elgamal se debe:

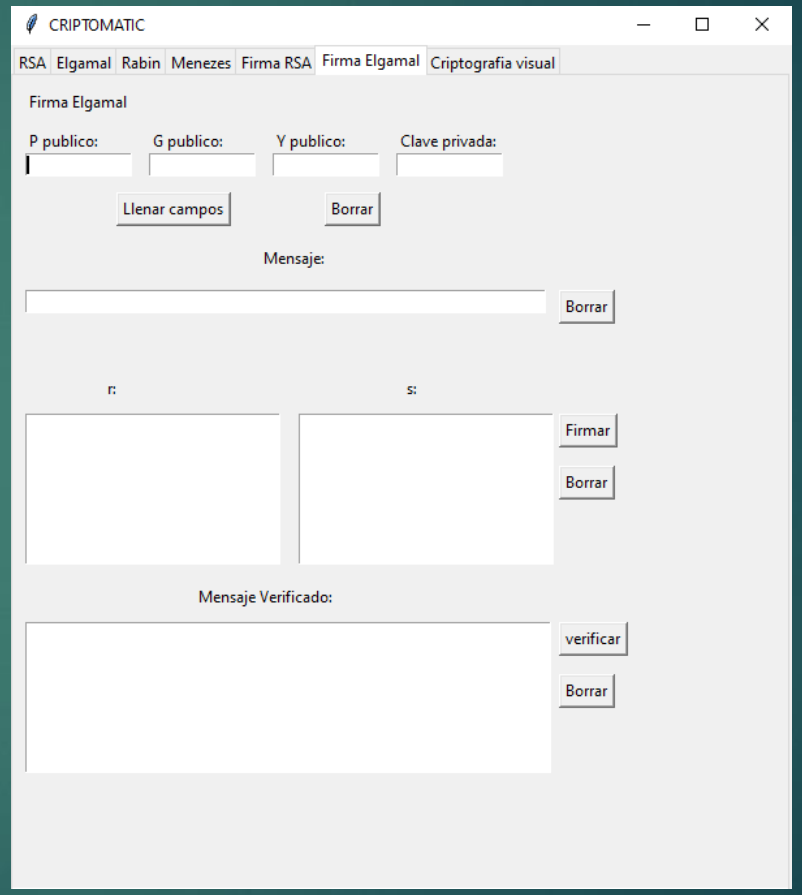
Firmar

1. Ingresar un número primo grande
2. Hallar sus respectivos valores G y Y públicos
3. Hallar su respectiva clave privada
4. Ingresar el mensaje a firmar
5. Oprimir en el botón firmar

O llenar los campos automáticamente y seguir desde el 4 paso mencionado anteriormente

Verificar

1. Llenar los campos de clave publica y privada
2. Llenar los campos mensaje, r y s
3. Oprimir el botón verificar



Criptografía visual

Para poder encriptar imágenes:

Encriptar

1. Seleccionar una imagen
2. Generar transparencias

Desencriptar

1. Importar trasparencia 1
2. Importar trasparencia 2
3. Unir transparencias