



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

The screenshot shows a web application window titled "CRIPTOMATIC". It has a navigation bar with tabs: "RSA", "Elgamal", "Rabin", "Menezes", "Firma RSA", "Firma Elgamal", and "Criptografia visual". The "RSA" tab is selected. The main content area is titled "Algoritmo RSA". It contains four input fields: "Primo1:", "Primo2:", "Clave publica e:", and "Clave privada d:". Below these fields are two buttons: "Llenar campos" and "Borrar". Below the key fields is a "Mensaje:" label and a text input field with a "Borrar" button. Below that is a "Mensaje encriptado:" label and a larger text area with "Encriptar" and "Borrar" buttons. At the bottom is a "Mensaje desencriptado:" label and another large text area with "Desencriptar" and "Borrar" buttons.

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

The screenshot shows the CRIPTOMATIC web application interface. At the top, there is a navigation bar with tabs for RSA, Elgamal (selected), Rabin, Menezes, Firma RSA, Firma Elgamal, and Criptografía visual. Below the navigation bar, the title "Algoritmo Elgamal" is displayed. The interface is divided into three main sections: 1. Key Generation: It contains three input fields labeled "Nro primo:", "Clave publica:", and "Raiz primitiva:". Below these fields are two buttons: "Llenar campos" and "Borrar". 2. Encryption: It features a large text input field labeled "Mensaje:". To the right of this field is a "Borrar" button. Below the input field is a section labeled "Mensaje encriptado:" which contains a large text area. To the right of this area are two buttons: "Encriptar" and "Borrar". 3. Decryption: It features a large text input field labeled "Mensaje desencriptado:". To the right of this field is a "Borrar" button. Below the input field is a section labeled "Mensaje desencriptado:" which contains a large text area. To the right of this area are two buttons: "Desencriptar" and "Borrar".

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

The screenshot shows the 'CRIPTOMATIC' web application interface. The 'Rabin' tab is selected in the top navigation bar. The main section is titled 'Algoritmo Rabin'. It contains three input fields for 'Primo1:', 'Primo2:', and 'Clave privada:'. Below these fields are two buttons: 'Llenar campos' and 'Borrar'. A 'Mensaje:' input field is located below the prime fields, with a 'Borrar' button to its right. The 'Mensaje encriptado:' section features a large text area for the encrypted message, with 'Encriptar' and 'Borrar' buttons to its right. The 'Mensaje desencriptado:' section features a large text area for the decrypted message, with 'Desencriptar' and 'Borrar' buttons to its right.

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 Secp256k1 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

The screenshot shows the CRIPTOMATIC application window. The 'Menezes' tab is selected in the top navigation bar. The interface displays the following elements:

- Algorithm and Curve:** 'Algoritmo Menezes-Vanstone' and 'Curva secp256k1' are shown. There are 'Llenar campos' and 'Borrar' buttons next to the curve name.
- Key Fields:** 'Clave publica:' and 'Clave privada:' labels with corresponding input text boxes.
- Message Field:** A 'Mensaje:' label with an input text box and a 'Borrar' button.
- Encryption Section:** A 'Mensaje encriptado:' label with a large text area for the encrypted message. To the right are 'Encriptar' and 'Borrar' buttons.
- Decryption Section:** A 'Mensaje desencriptado:' label with a large text area for the decrypted message. To the right are 'Desencriptar' and 'Borrar' buttons.

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

The screenshot shows the 'CRIPTOMATIC' web application interface. At the top, there are tabs for 'RSA', 'Elgamal', 'Rabin', 'Menezes', 'Firma RSA' (which is selected), 'Firma Elgamal', and 'Criptografia visual'. Below the tabs, the 'Firma RSA' section contains input fields for 'Primo1:', 'Primo2:', 'Clave publica e:', and 'Clave privada d: n:'. There are 'Llenar campos' and 'Borrar' buttons below these fields. A 'Mensaje:' input field with a 'Borrar' button is located below the key fields. Further down, there are two large text areas labeled 'Hash del mensaje:' and 'Firma:', each with its own 'Firmar' and 'Borrar' buttons. At the bottom, there is a 'Mensaje Verificado:' input field with 'verificar' and 'Borrar' buttons. The interface is clean and uses a light gray color scheme.

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

The screenshot shows the 'CRIPTOMATIC' web application interface. The 'Firma Elgamal' tab is selected. The interface includes input fields for 'P publico:', 'G publico:', 'Y publico:', and 'Clave privada:'. Below these is a 'Llenar campos' button and a 'Borrar' button. A 'Mensaje:' input field is followed by a 'Borrar' button. Below the message field are two large input fields labeled 'r:' and 's:'. To the right of these are 'Firmar' and 'Borrar' buttons. At the bottom, there is a 'Mensaje Verificado:' input field with 'verificar' and 'Borrar' buttons to its right.

Criptografía visual

Para poder encriptar imágenes:

Encriptar

1. Seleccionar una imagen
2. Generar transparencias

Desencriptar

1. Importar transparencia 1
2. Importar transparencia 2
3. Unir transparencias

