

MANUAL DE USUARIO

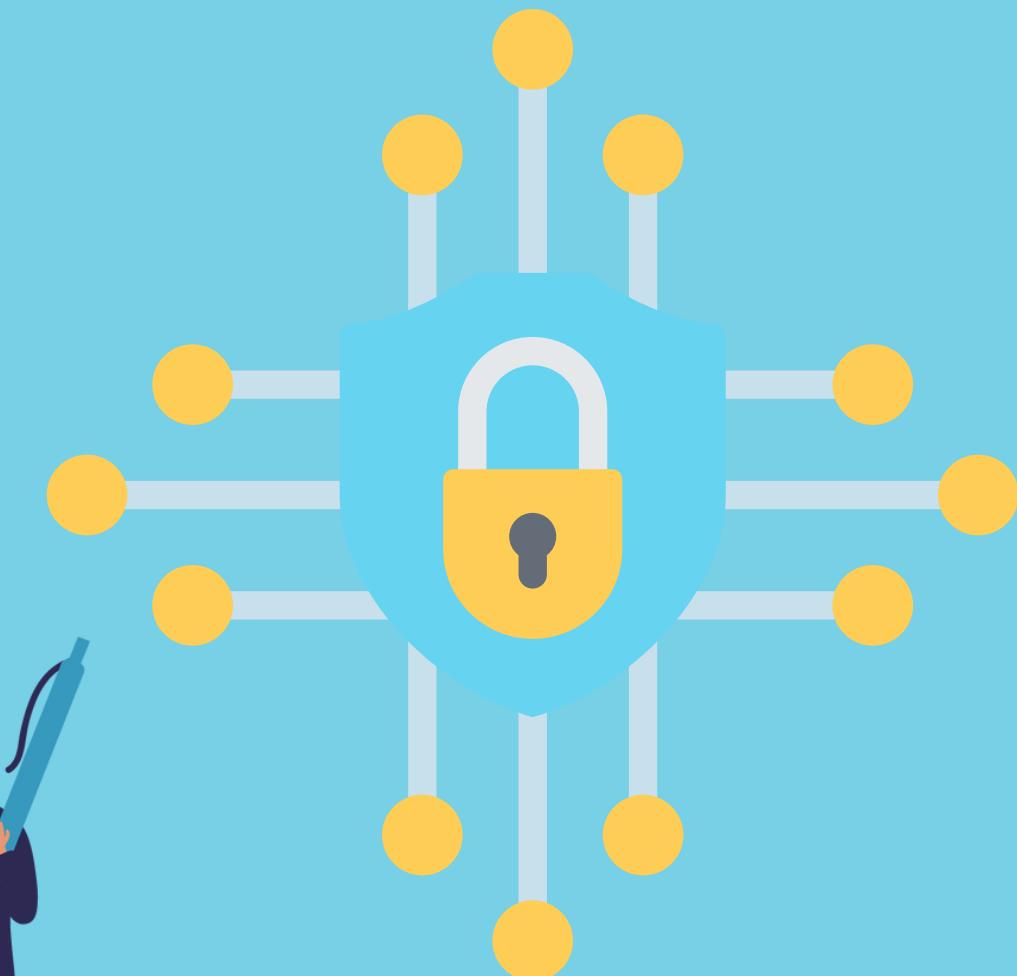
AUTOR: JOSE LUIS OBIANG ELA NANGUANG

PROFE: JUAN ARIAS MASA

ASIGNATURA: SEGURIDAD DE LA INFORMACIÓN

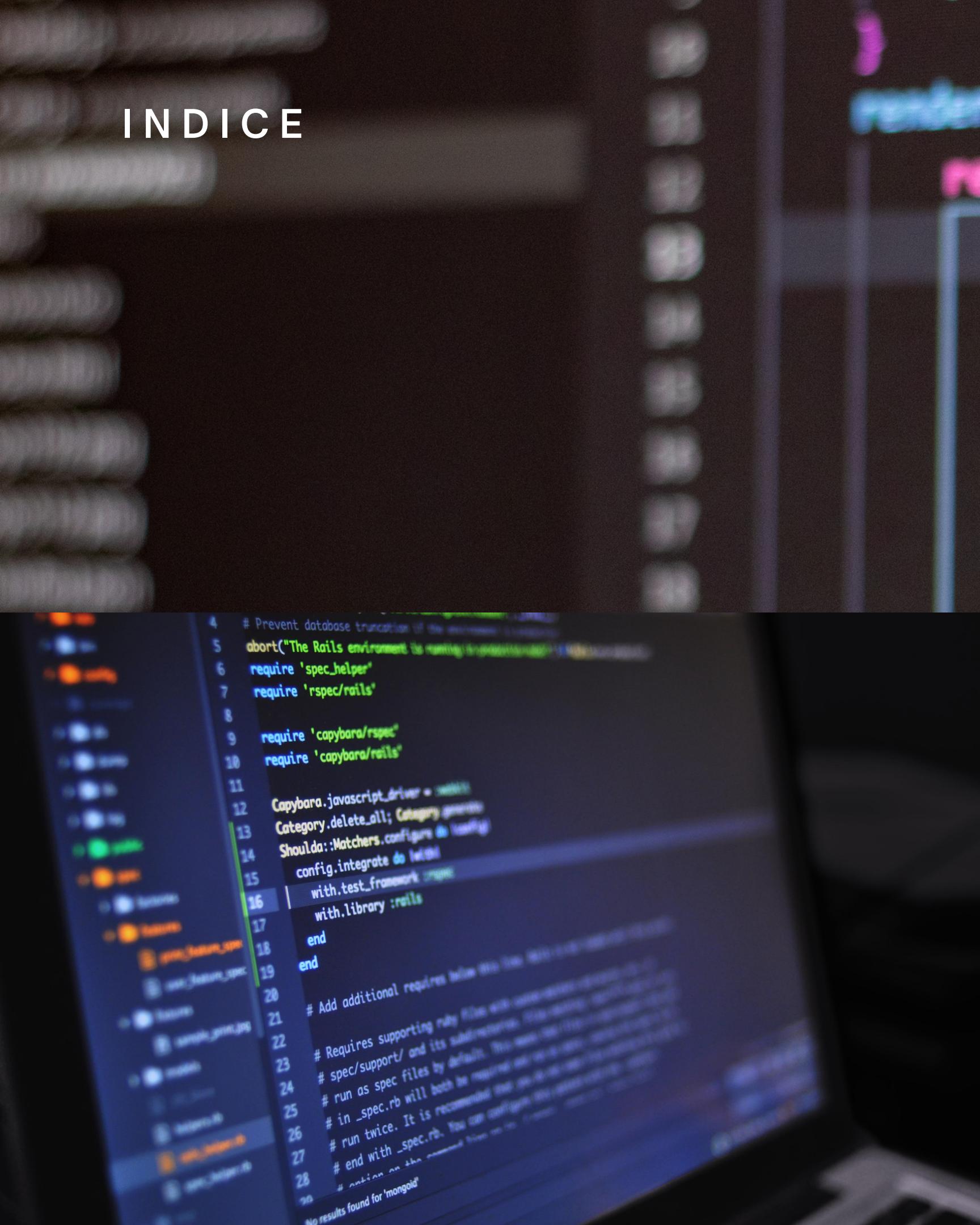


CIFRADO HILL



INDICE

1. INTRODUCCIÓN	3
2. REQUISITOS DEL SISTEMA	4
3. INSTALACIÓN Y CONFIGURACIÓN	5
4. INICIAR LA APLICACIÓN	6
5. USO BÁSICO	7
6. PREGUNTAS FRECUENTES	8
7. CONCLUSIONES	11
8. BIBLIOGRAFIA	12



```
4  # Prevent database truncation if the environment is :test
5  abort("The Rails environment is running in production mode")
6  require 'spec_helper'
7  require 'rspec/rails'
8
9  require 'capybara/rspec'
10 require 'capybara/rails'
11
12 Capybara.javascript_driver = :webkit
13 Category.delete_all; Category.create!(name: "Default")
14 Shoulda::Matchers.configure do |config|
15   config.integrate do |with|
16     with.test_framework :rspec
17     with.library :rails
18   end
19 end
20
21 # Add additional requires below this line to include more shared helpers
22
23 # Requires supporting ruby files with custom matchers and helpers
24 # in spec/support/ and its subdirectories. This directory also
25 # contains supporting files for this generator, like:
26 # - etc./config/database.yml
27 # - etc./config/initializers/filter_rails_logger.rb
28 # - etc./config/initializers/mongoid.rb
29 # - etc./config/initializers/mongoid_logging.rb
30
31 # run as spec/ and its subdirectories. This directory also
32 # contains supporting files for this generator, like:
33 # - etc./config/database.yml
34 # - etc./config/initializers/filter_rails_logger.rb
35 # - etc./config/initializers/mongoid.rb
36 # - etc./config/initializers/mongoid_logging.rb
37
38 # run twice. It is recommended you use a command like the one below
39 # in your .rspec file. This will run the default + --color=auto + --format
40 # options from rspec, as well as --color=never + --format=html
41 # from this generator's configuration
42 # --tag ^:unit --tag ^:integration --tag ^:system --tag ^:request
43 # --tag ^:pending --tag ^:x --tag ^:wip --tag ^:features --tag ^:e2e
44 # --tag ^:cucumber --tag ^:scenarios --tag ^:examples
45
46 # Note: If you are running 'rake spec' without the --tag
47 # option it will run all of the above specs. To run
48 # only 'unit' specs, you must explicitly add the --tag
49 # :unit option.
```



1. INTRODUCCIÓN

Bienvenido al manual de usuario de la aplicación de cifrado AES y CBC. Esta herramienta está diseñada para cifrar y descifrar texto en claro. Esta guía le orientará sobre cómo utilizar la aplicación de manera eficiente.





2. REQUISITOS DEL SISTEMA

Sistema Operativo

- Windows: Windows 10 (8/7/Vista opcional pero podría requerir configuraciones adicionales).
- macOS: macOS 10.12 Sierra o superior.
- Linux: Distribuciones modernas como Ubuntu 20.04, Fedora 32, Debian 10 o similares.

Software

Java Runtime Environment (JRE) versión 18.0.2.1: Esencial para ejecutar programas Java. En algunos casos, es posible que necesite el Java Development Kit (JDK) V.18 si está previsto compilar código fuente.

- Nota: Si bien Java es conocido por su compatibilidad hacia atrás ("backward compatibility"), es recomendable usar la versión exacta (18.0.2.1) para evitar problemas de incompatibilidad o comportamientos inesperados.

Hardware

- Procesador: CPU moderna de al menos 1 GHz. Se recomiendan CPUs de 64 bits para un mejor rendimiento.
- Memoria RAM: Mínimo de 2 GB. Se recomiendan 4 GB o más para aplicaciones más exigentes.
- Espacio en disco: Mínimo de 200 MB para la instalación del JRE/JDK. Se debe tener en cuenta el espacio adicional para el programa en sí y cualquier archivo o base de datos asociado.
- Tarjeta gráfica: Cualquier tarjeta gráfica moderna para aplicaciones que utilicen GUIs avanzadas o renderizado.
- Conexión a Internet: Necesaria para descargar actualizaciones, conectarse a bases de datos remotas o acceder a servicios en la nube, si es que el programa lo requiere.

3. Instalación y configuración

NOTA: SOLO PARA WINDOWS

Preparación

Ubicación del Programa

Instalación

- Antes de comenzar la instalación, **asegúrese de haber cumplido con todos los Requisitos del sistema.**
- La ubicación de la carpeta de instalación es independiente del lugar.
- El programa cifra y descifra el contenido del fichero de entrada, denominada `quijote1.txt` ubicada en la carpeta ...\\ejecutable\\
- El programa de ejecución se encontrará en la carpeta ...\\ejecutable\\, se llama `probar.bat`, **el cual ejecutaremos pero no sin antes leer la siguiente página.**



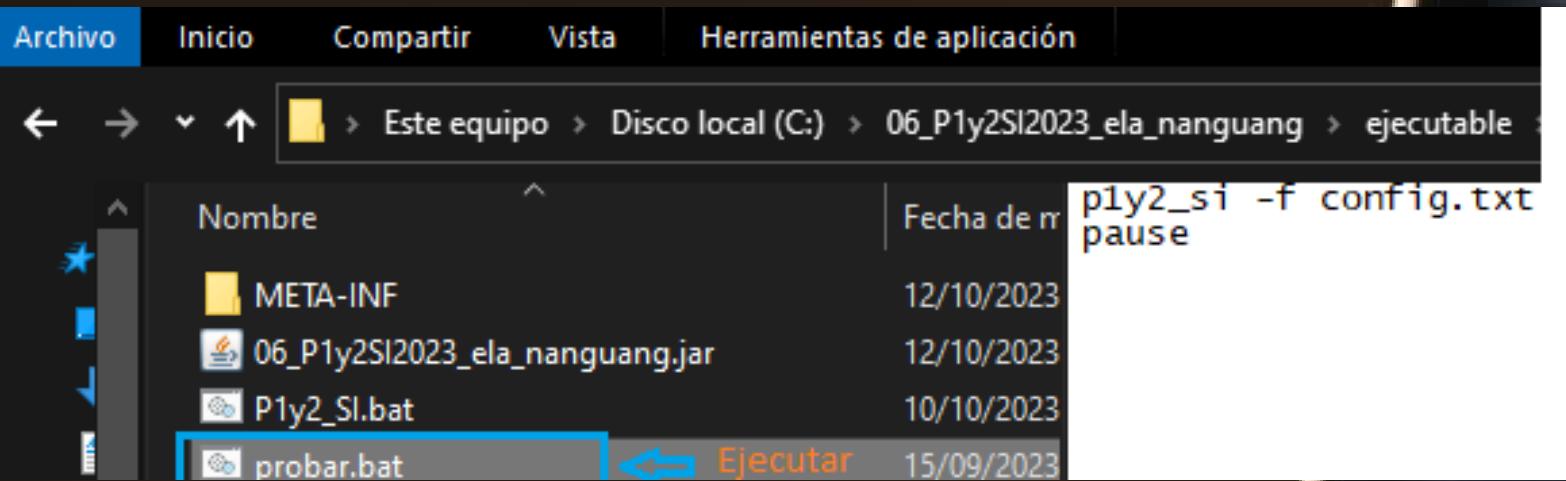
4. INICIAR APLICACIÓN

Para que se ejecute la aplicación tenemos que haber cumplido los requisitos del sistema y la conocer dónde se ha ubicado la carpeta de instalación.

Al cumplir dichas condiciones, para la ejecución de la aplicación debemos seguir los siguientes pasos:

- Primero **abrimos el archivo** `quijotel.txt` ubicada en la carpeta ...\\ejecutable\\, luego **sobreescrivimos en su contenido el texto que queremos cifrar y que contenga los caracteres del abecedario incluido la ñ. Evite símbolos, espacios y caracteres especiales.**
- **Guardamos el fichero modificado** con el texto en claro que hayamos añadido.
- Nos **Ubicamos en la misma carpeta** ...\\ejecutable\\ y finalmente ejecutamos el programa **haciendo doble click sobre el archivo** `probar.bat`.
- Para ver todos los registros de los textos en claro y sus correspondientes cifrados, nos **ubicamos nuevamente en la la misma carpeta** ...\\ejecutable\\, la cual veremos que se ha creado el archivo `logs.txt`, el cual **abrimos para visualizar los textos en claro con sus correspondientes criptogramas.**

5. Uso Básico {



```

Comentario
Linea vacia
Comentario
Bandera
La traza esta encendida
Comentario
Comando
Leyendo fichero clave
1 2 3 0 4 5 1 0 6
Multiplo: 3
1 2 3 0 4 5 1 0 6
Total tokens a leer: 9
Mostrando matriz clave:
1 2 3
0 4 5
1 0 6
Linea vacia
Comentario
Comentario
Comando
Leyendo fichero de entrada
El texto claro sin formatear tiene: 12 caracteres
Texto en claro Formateado: NUEVOEJEMPLO
Linea vacia
Comentario
Comando
Fichero de salida
Existe el fichero de salida quijoteOutput.txt
Linea vacia
Comentario
Comando
Linea vacia
Comentario
Bandera
Codificando
12
Mostrando valores numericos de la matriz de texto:
13 22 9 16
21 15 4 11
4 4 12 15
Mostrando la matriz de texto cifrado:

```

```

Mostrando la matriz de texto cifrado:
Total de filas: 3
Total de columnas: 4
13 10 26 2
23 26 22 11
10 19 0 25
Bandera
La traza esta encendida
Comentario
Comando
Se produce la ejecucion del cifrado
CRIPTOGRAMA: NWKKZSZVACLY
Linea vacia
Comentario
Bandera
Decodificacion

Paso 1: Determinante de la matriz clave → 22
Mostrando la matriz inversa modulo 27 de la matriz clave:

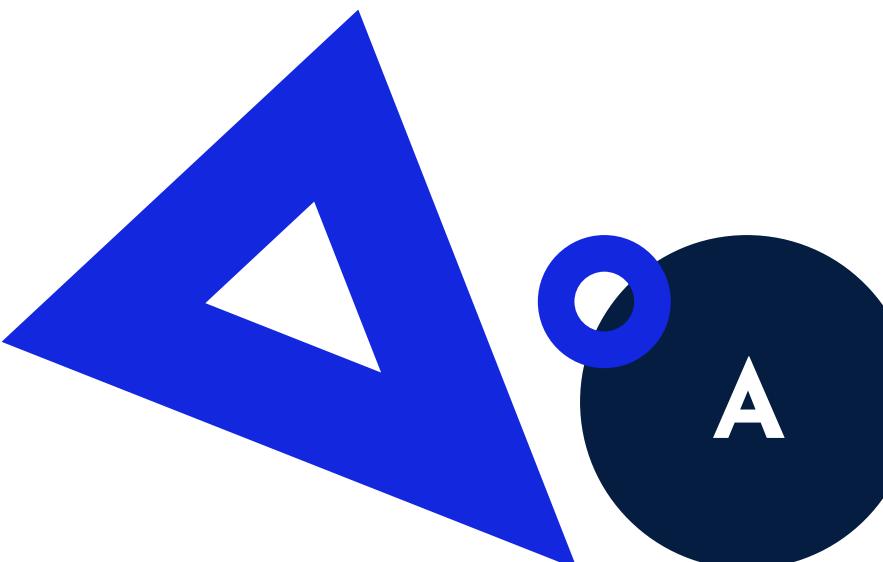
6 24 22
26 21 1
17 5 10

Mostrando matriz producto de inversa x matriz cifrado

13 22 9 16
21 15 4 11
4 4 12 15

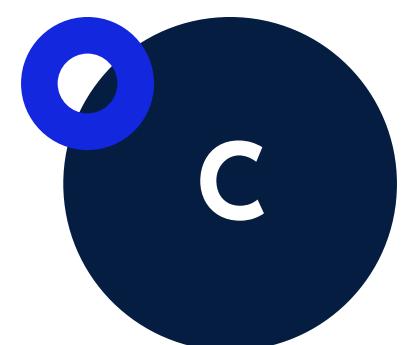
Comentario
Comando
Se produce la ejecucion del de
Texto Descifrado: NUEVOEJEMPLO
}
```

6. PREGUNTAS FRECUENTES: CIFRADO HILL



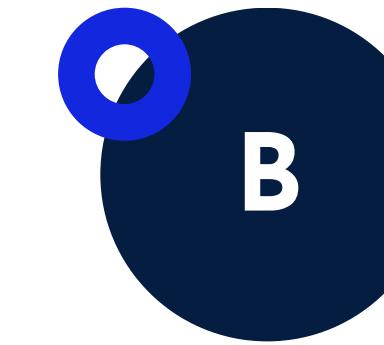
¿Qué es el cifrado Hill?

Es un método de cifrado simétrico que utiliza operaciones matriciales para transformar texto en claro en texto cifrado y viceversa.



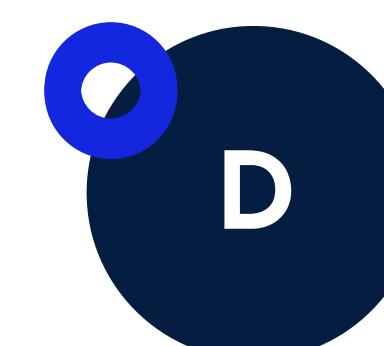
¿Puedo cifrar cualquier tipo de archivo o solo texto?

Esta versión del programa está diseñada principalmente para trabajar con texto.



¿Dónde se encuentra el archivo clave y cómo elijo otra clave para el cifrado?

El archivo de clave se encuentra en ...\\ejecutable y se llama **clave.txt**.

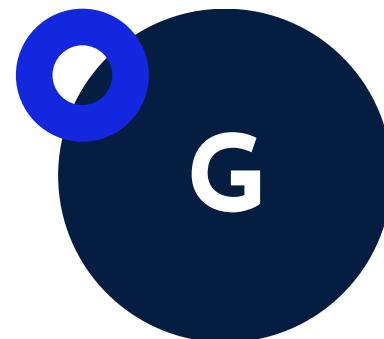
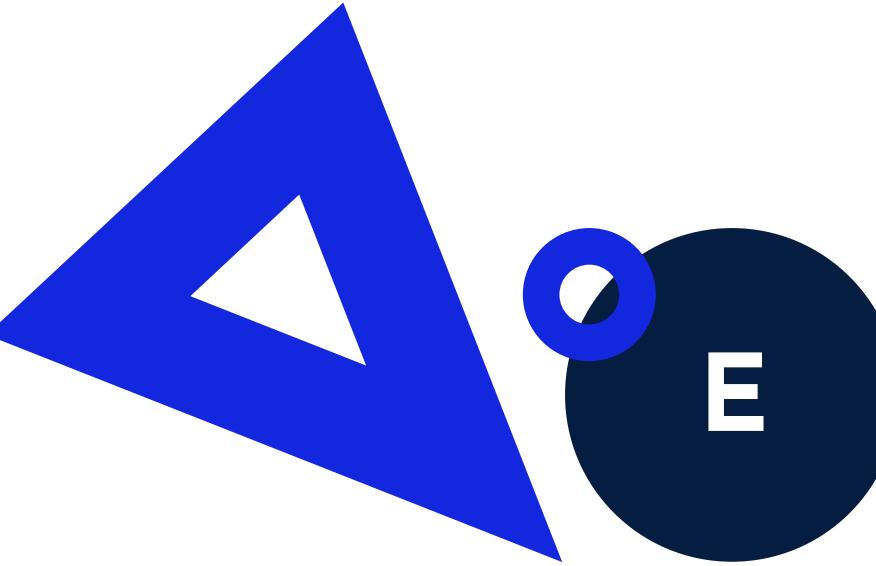


¿Qué sucede si pierdo mi archivo de clave?

Sin el archivo de clave correcto, no podrás descifrar correctamente el texto. Es esencial mantener el archivo de clave seguro, al igual que el fichero **config.txt** y el fichero de entrada **quijote1.txt**, las cuales recomendaría hacer copias de respaldo.

PREGUNTAS FRECUENTES:

CIFRADO HILL

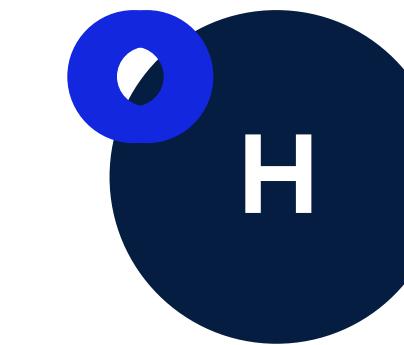


¿Es seguro el cifrado Hill comparado con otros métodos de cifrado?

El cifrado Hill es relativamente seguro para textos cortos, pero existen métodos más modernos y robustos para la mayoría de las aplicaciones prácticas. Su seguridad depende en gran medida de la elección de la matriz clave y del tamaño del alfabeto utilizado.

Encuentro errores al intentar cifrar o descifrar. ¿Qué podría estar mal?

Asegúrate de que exista el archivo clave **clave.txt**, **quijsote1.txt** y **config.txt** en la misma ubicación de la carpeta ...\\ejecutable.



¿Necesito algún conocimiento previo en matemáticas para usar este programa?

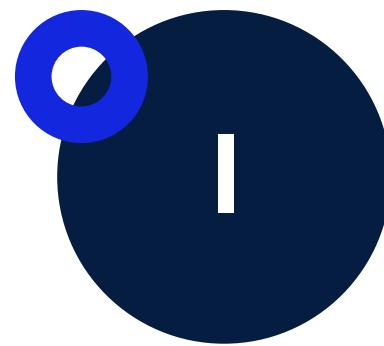
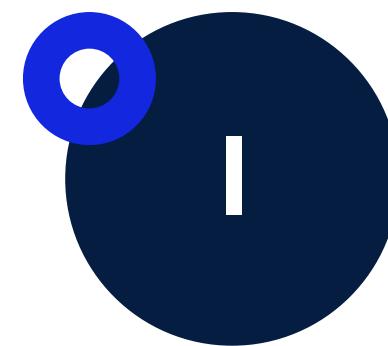
No, el programa se encarga de todos los cálculos matriciales por ti. Solo necesitas proporcionar el texto y la clave adecuada.

¿Dónde se almacenan los registros de cifrado?

Todos los registros de cifrado se almacenan en el archivo "**logs.txt**" ubicado en la misma carpeta que el resto de archivos que he mencionado anteriormente, dicho fichero contiene los textos en claro junto con los criptogramas.

PREGUNTAS FRECUENTES:

CIFRADO HILL



¿El programa soporta otros métodos de cifrado además del Hill?

Este programa está diseñado específicamente para el cifrado Hill. Si estás interesado en otros métodos de cifrado, consulta [otras herramientas disponibles](#).



Jose Luis
Obiang Ela
Nanguang

7. CONCLUSIONES

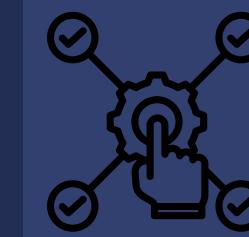
Seguridad

En la era digital actual, la seguridad y privacidad de la información es esencial. Herramientas como el programa de cifrado Hill brindan un nivel adicional de protección para los datos, asegurando que solo aquellos con la clave adecuada puedan acceder al contenido original.



Usabilidad

A pesar de los complejos cálculos matemáticos que implica el cifrado Hill, el programa ha sido diseñado para que cualquier usuario, sin conocimientos avanzados, pueda cifrar y descifrar sus textos de manera sencilla.



Responsabilidad del usuario

Si bien el programa proporciona las herramientas para cifrar y descifrar información, es responsabilidad del usuario manejar y almacenar sus claves de manera segura. La pérdida de la clave resulta en la imposibilidad de descifrar el contenido cifrado.



Continuo avance de la tecnología

Es importante recordar que, con el paso del tiempo, los métodos de cifrado pueden volverse obsoletos o vulnerables. Por lo tanto, siempre es recomendable estar al tanto de los avances en criptografía y actualizar las herramientas y métodos utilizados regularmente.



8 . BIBLIOGRAFÍA



**Calculadora
Online para las
pruebas**

[planetcalc](#)

**Funciones para
cálculo de
matrices**

[youCode](#)

Colores ANSI

[w3schools](#)

**Inversa Modular
de una matriz**

Apuntes del profe de SEI y apuntes
del profe de AMA



**MUCHAS
GRACIAS**