Manual de Usuario - CryptoTools

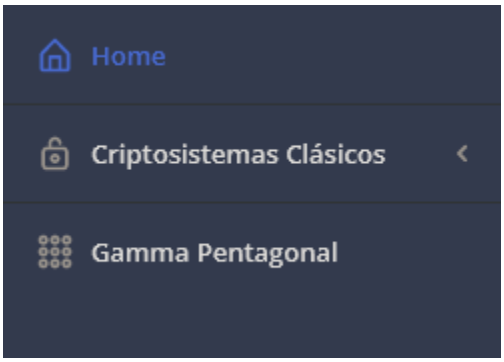
Este es el manual de usuario para la herramienta CryptoTools que hace parte de la materia Introducción a la criptografía y a la teoría de información, en su primera versión. Aquí se pueden encontrar implementados los siguientes módulos:

1. Criptosistemas clásicos
    a. Desplazamiento
    b. Afín
    c. Vigenere
    d. Sustitución
    e. Hill
    f. Permutación

🟢 Es necesario tener un mínimo conocimiento teórico sobre lo anterior descrito para poder entender y usar las herramientas proporcionadas.

Ingreso al sitio y configuración básica

Una vez se accede a la página web, en la parte izquierda se encontrará una barra con los módulos implementados y sus componentes. El usuario estará por defecto en **Home**.



En la parte superior se hallará una barra en la que el usuario podrá elegir entre varios diseños de la página. Entre ellos, oscuro (Dark), claro (Light), cósmico (Cosmic) y corporativo (Corporate).

Light (por defecto)

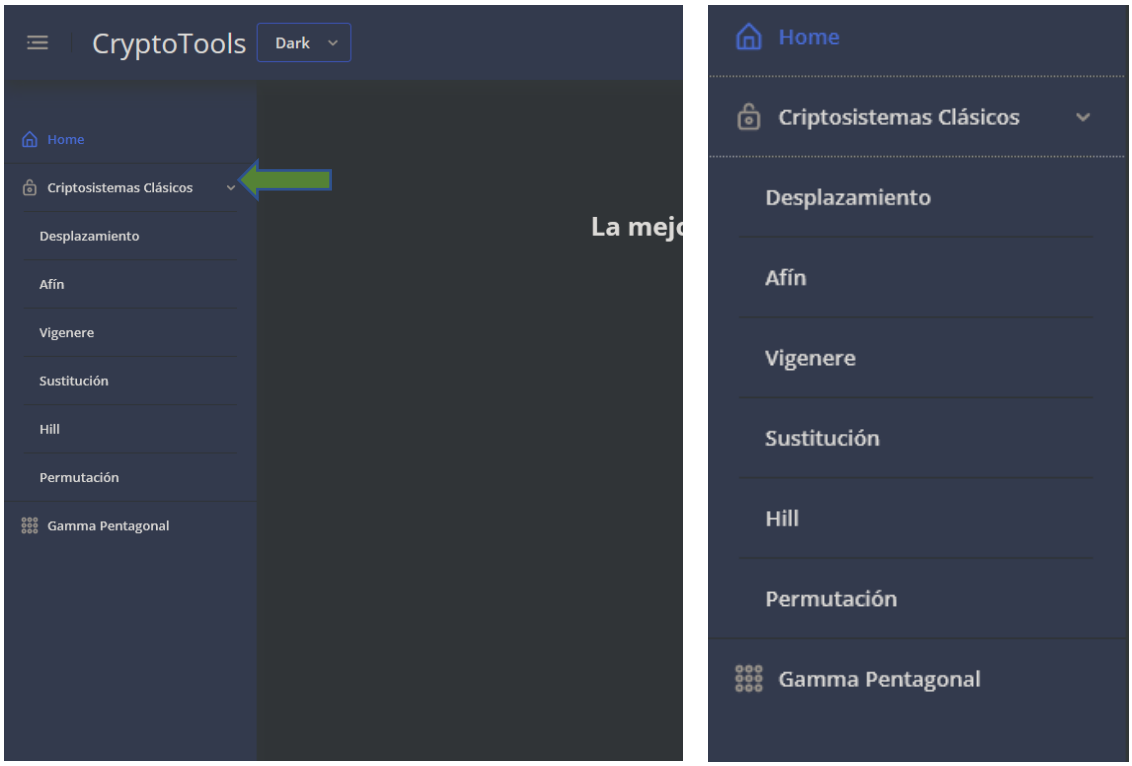
Dark

Cosmic

Corporate

Criptosistemas Clásicos.

Para acceder a los criptosistemas clásicos, se selecciona ese módulo en la barra izquierda de la página web.



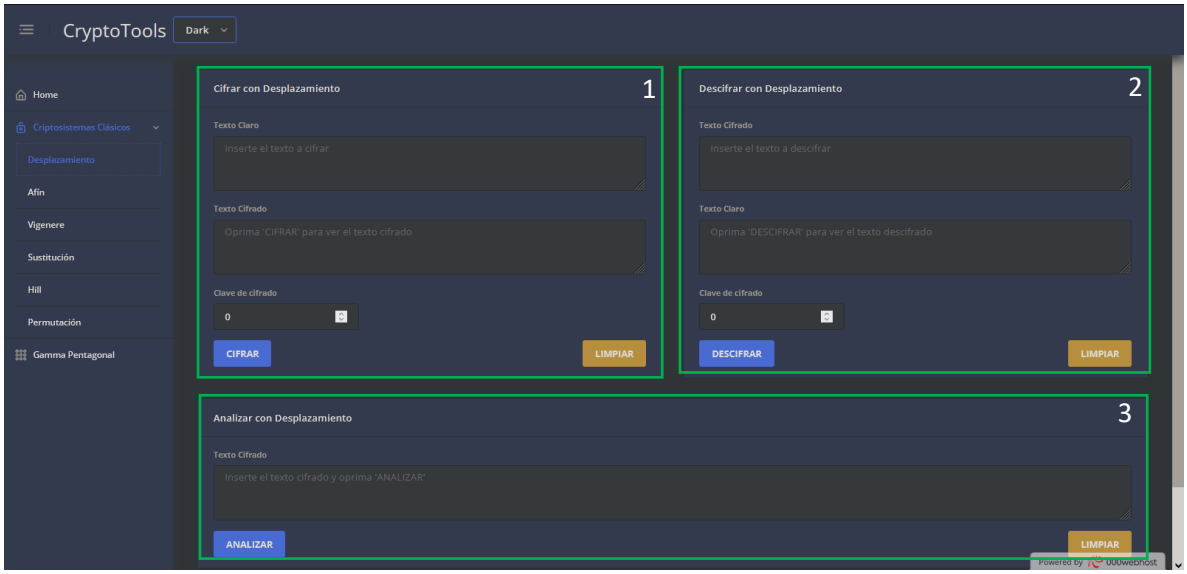
Allí, el usuario podrá hacer uso de la herramienta que considere más conveniente. Estas son:

a) Desplazamiento
b) Afín
c) Vigenere
d) Sustitución
e) Hill
f) Permutación

Cada una de ellas cuenta con al menos dos herramientas básicas, cifrado y descifrado. Para hacer uso del cifrado, cada sistema requerirá de una clave. Esta clave se utilizará para cifrar la información dada, sea texto o una imagen. Dependiendo del sistema cada clave tendrá una particularidad. Una vez se cifra un texto (imagen) el resultado es un texto (imagen) cifrada. Descifrar es la operación inversa a la de cifrar, al igual que la operación de ciframiento requiere una clave que cumple las mismas propiedades que toda clave que se usa para cifrar. Se hará una breve descripción de cada sección individualmente, su clave y su sección de criptoanálisis: una herramienta a utilizar cuando se posee un texto cifrado, pero sin conocimiento de la clave.

a) Desplazamiento

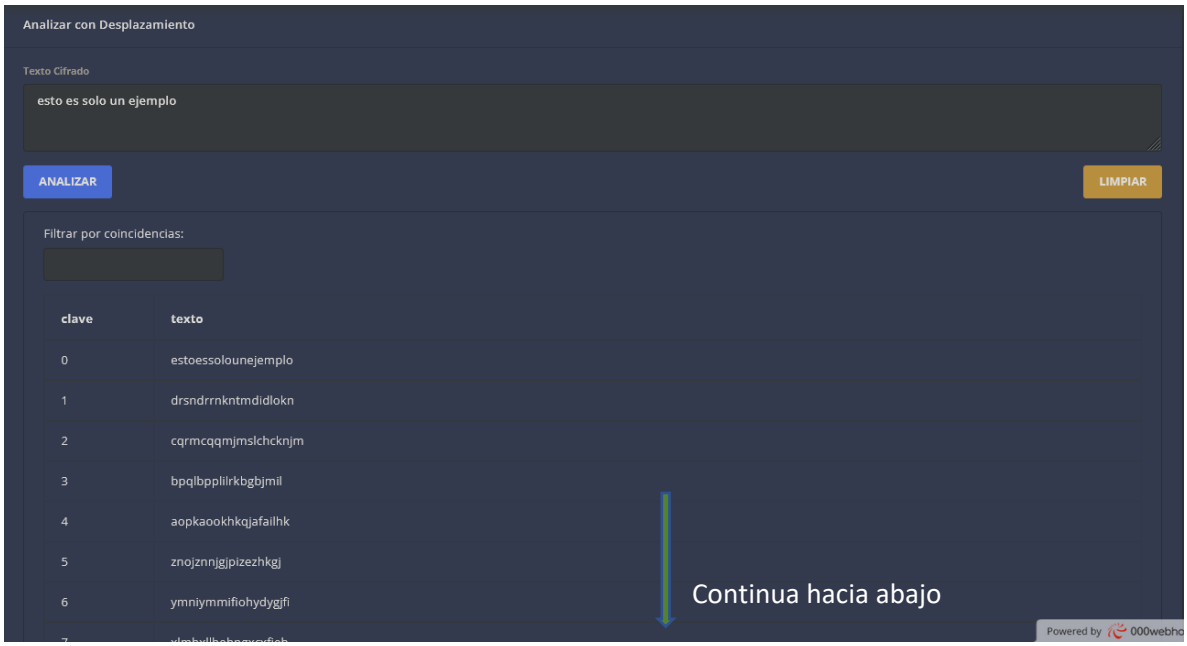
En la sección de **Desplazamiento** distinguimos tres subsecciones.



Las dos primeras subsecciones realizan las operaciones de ciframiento y desciframiento de forma respectiva. Para cifrar (descifrar) se ingresa el texto claro (cifrado) y la clave. Luego se presiona el botón de **Cifrar** (**Descifrar**) azul, en la parte baja del recuadro verde respectivo.

Restricciones sobre la clave: Debe ser un número entero entre 0 y 25, inclusivo.

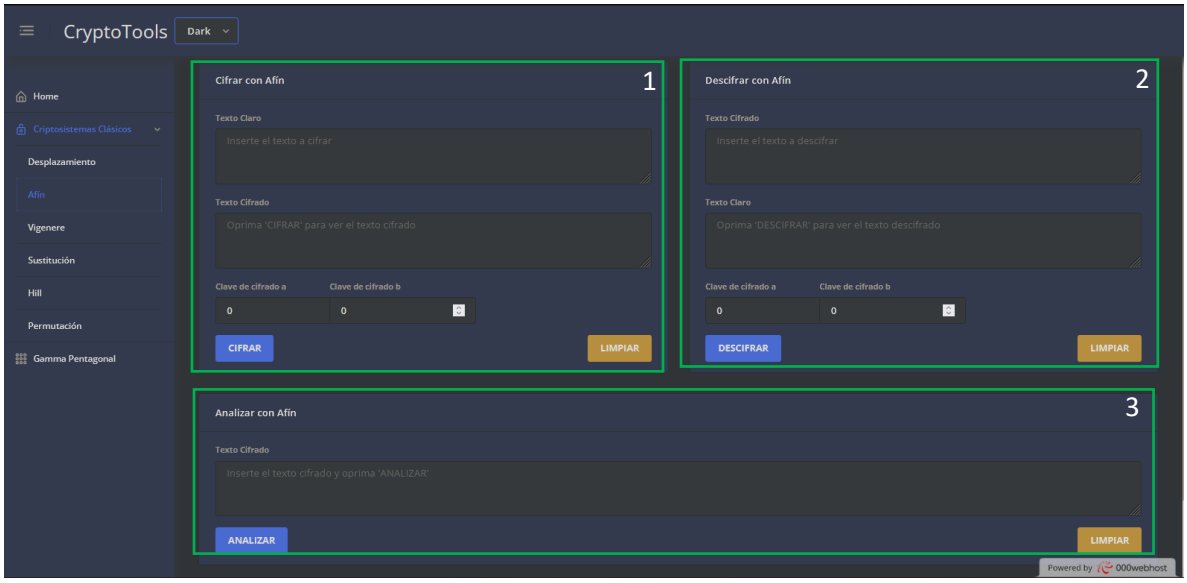
La tercera subsección realiza el criptoanálisis. Solo requiere un texto. Posterior al ingreso de este y de seleccionar el botón azul **Analizar**, se procede a descifrar ese texto con todas las posibles claves. El usuario podrá filtrar por coincidencias en un recuadro, o buscar una clave particular.



El botón amarillo de **Limpiar** en cada subsección elimina el contenido de los recuadros por si se ve necesario.

b) Afín

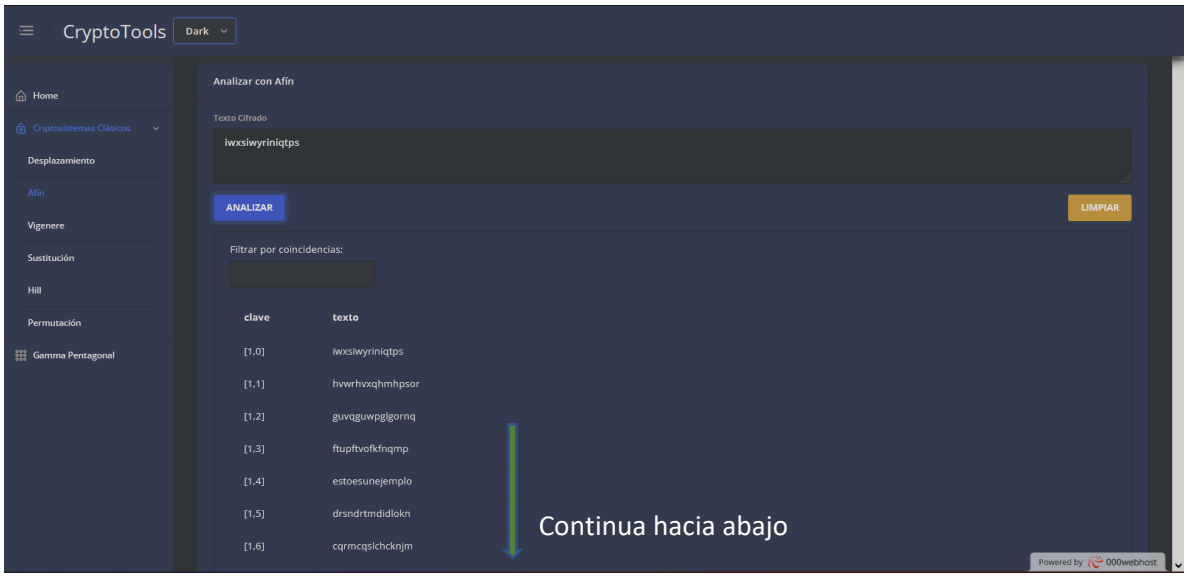
En la sección de **Afín** distinguimos tres subsecciones.



Las dos primeras subsecciones realizan las operaciones de cifrамiento y descifrамiento de forma respectiva. Para cifrar (descifrar) se ingresa el texto claro (cifrado) y la clave. Luego se presiona el botón de **Cifrar** (**Descifrar**) azul, en la parte baja del recuadro verde respectivo.

Restricciones sobre la clave: La clave de cifrado **a** y **b** deben ser números enteros entre 0 y 25, inclusivo. Adicionalmente, la clave de cifrado **a** debe ser primo relativo con el número 26, el tamaño del alfabeto inglés.

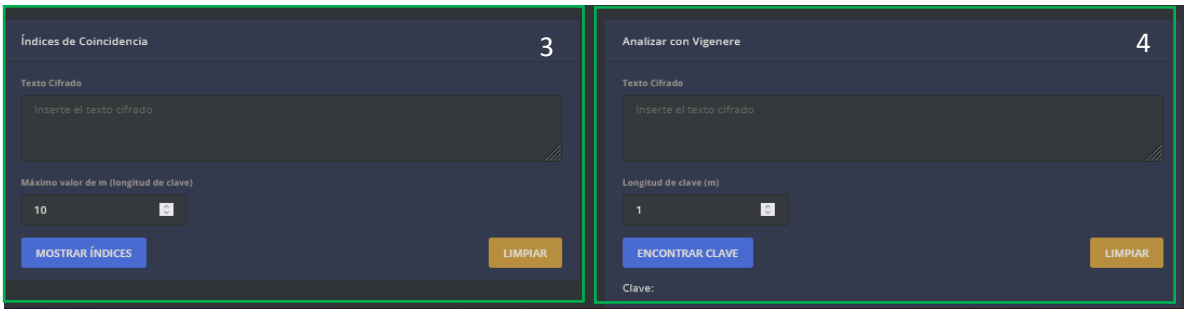
La tercera subsección realiza el criptoanálisis. Solo requiere un texto. Posterior al ingreso de este y de seleccionar el botón azul **Analizar**, se procede a descifrar ese texto con todas las posibles claves. El usuario podrá filtrar por coincidencias en un recuadro, o buscar una clave particular.



El botón amarillo de **Limpiar** en cada subsección elimina el contenido de los recuadros por si se ve necesario.

c) Vigenere

En la sección de **Vigenere** distinguimos cuatro subsecciones.

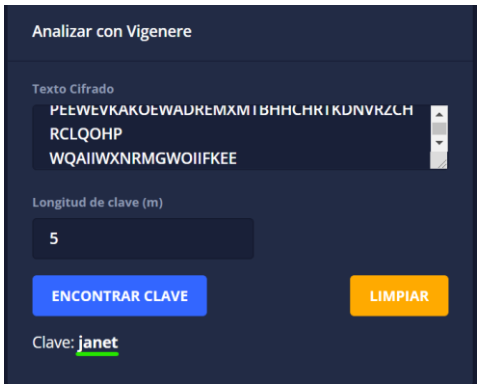


Las dos primeras subsecciones realizan las operaciones de ciframiento y desciframiento de forma respectiva. Para cifrar (descifrar) se ingresa el texto claro (cifrado) y la clave. Luego se presiona el botón de **Cifrar** (**Descifrar**) azul, en la parte baja del recuadro verde respectivo.

Restricciones sobre la clave: La clave debe ser una palabra no vacía escrita en el alfabeto inglés.

Las dos subsecciones restantes realizan el criptoanálisis. La subsección tres retorna, dado un texto cifrado y número positivo m, la tabla de los índices de coincidencia de 1 hasta m al presionar el botón **Mostrar índices**. La idea es escoger el número que haga que los índices de coincidencia de la fila sean cercanos a 0.065, así, el número elegido será probablemente la longitud de la clave del cifrado. El usuario podrá filtrar por coincidencias en un recuadro, o buscar un número de índices de coincidencia particular.

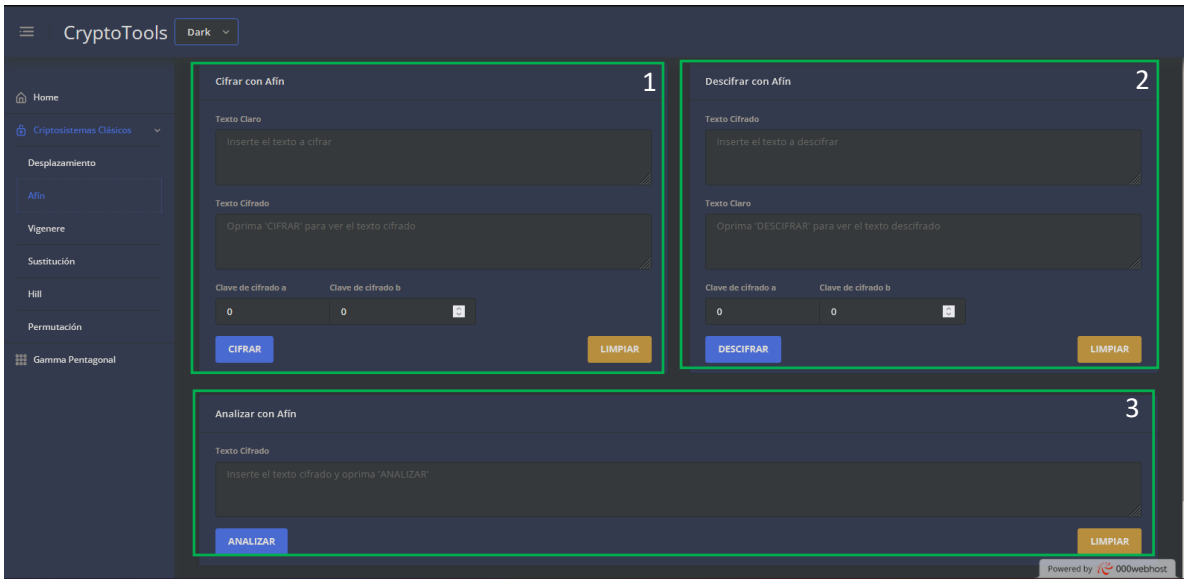
Para la subsección cuatro, solo requiere un texto cifrado en inglés y una conjetura de la longitud de la clave. Posterior al ingreso de estos y de seleccionar el botón azul **Analizar**, se procede a retornar la posible clave de cifrado de Vigenere usando el algoritmo basado en las probabilidades de aparición de las letras en el idioma inglés.



Finalmente, los botones amarillos de **Limpiar** eliminan en cada subsección el contenido de los recuadros de ingreso de texto por si se ve que es necesario.

d) Sustitución

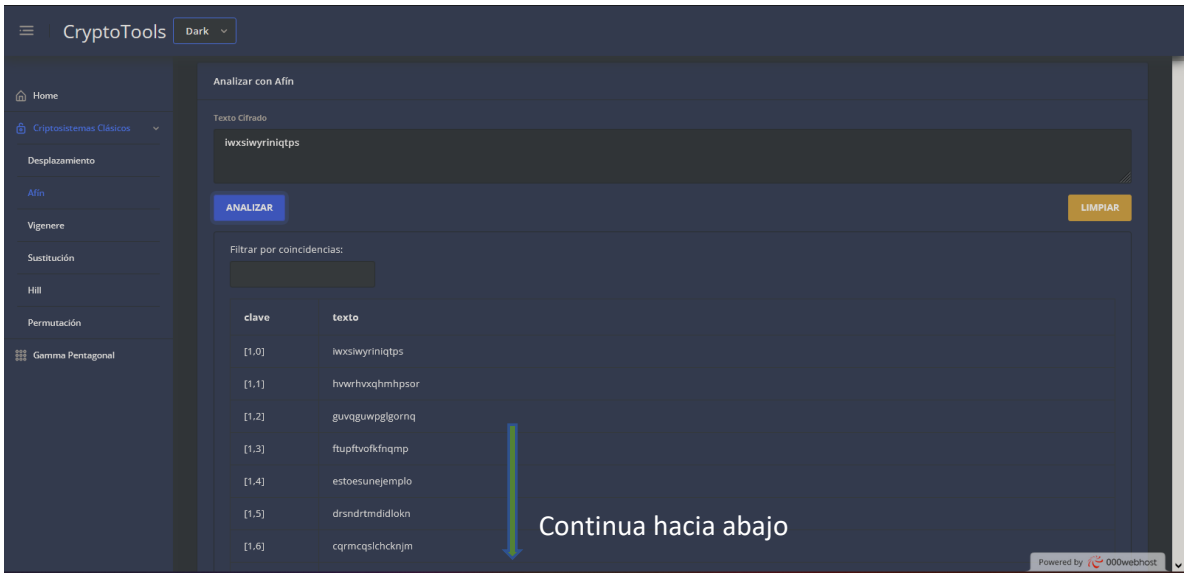
En la sección de **Sustitución** distinguimos tres subsecciones.



Las dos primeras subsecciones realizan las operaciones de ciframiento y desciframiento de forma respectiva. Para cifrar (descifrar) se ingresa el texto claro (cifrado) y la clave. Luego se presiona el botón de **Cifrar** (**Descifrar**) azul, en la parte baja del recuadro verde respectivo.

Restricciones sobre la clave: La clave de cifrado **a** y **b** deben ser números enteros entre 0 y 25, inclusivo. Adicionalmente, la clave de cifrado **a** debe ser primo relativo con el número 26, el tamaño del alfabeto inglés.

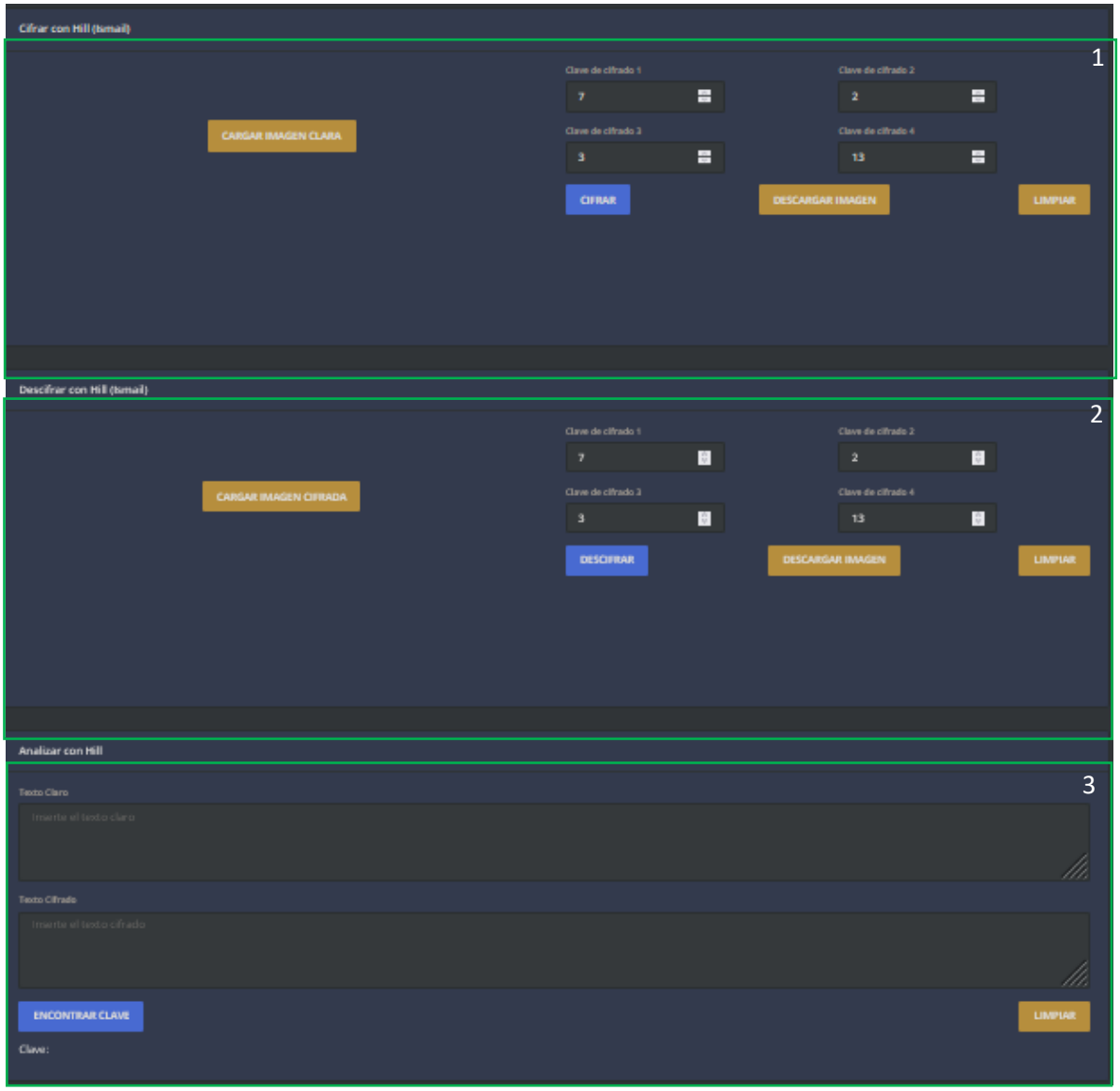
La tercera subsección realiza el criptoanálisis. Solo requiere un texto. Posterior al ingreso de este y de seleccionar el botón azul **Analizar**, se procede a descifrar ese texto con todas las posibles claves. El usuario podrá filtrar por coincidencias en un recuadro, o buscar una clave particular.



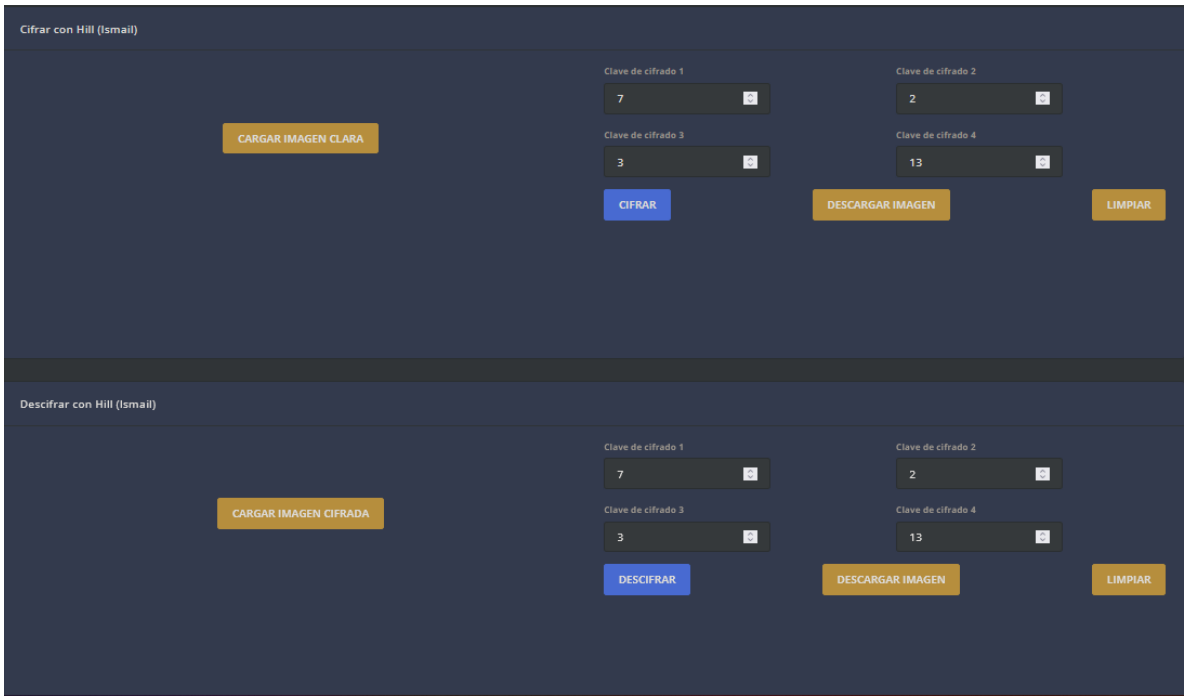
El botón amarillo de **Limpiar** en cada subsección elimina el contenido de los recuadros por si se ve necesario.

e) Hill

En la sección de **Hill** distinguimos tres subsecciones.



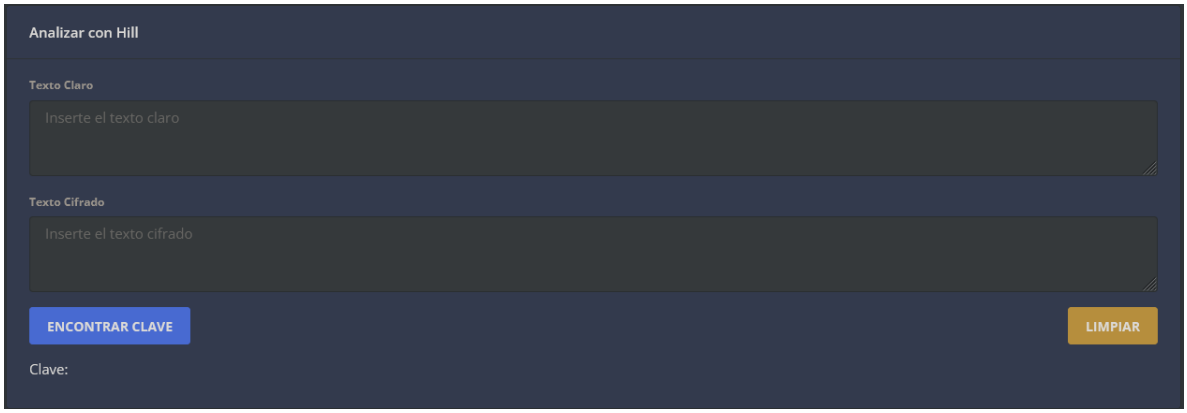
Las dos primeras subsecciones realizan las operaciones de ciframiento y desciframiento de forma respectiva, a diferencia del resto de secciones, el ciframiento aquí se realiza sobre una imagen. Para cifrar (descifrar) se ingresa la imagen clara (cifrada) y la clave. Luego se presiona el botón de **Cifrar** (**Descifrar**) azul, en la parte baja de donde se ingresa la clave. En estas dos subsecciones en la parte inferior central se encuentra el botón de para descargar la imagen cifrada(clara).



Restricciones sobre la clave: La clave está compuesta de cuatro números, que forman una matriz.

$$\begin{bmatrix} Clave\ de\ cifrado\ 1 & Clave\ de\ cifrado\ 2 \\ Clave\ de\ cifrado\ 3 & Clave\ de\ cifrado\ 4 \end{bmatrix}$$

Se recomienda que esta matriz sea invertible para poder descifrar la imagen ingresada y que no sea la matriz identidad para que el cifrado sea apropiado. Una buena clave es la que viene por defecto.

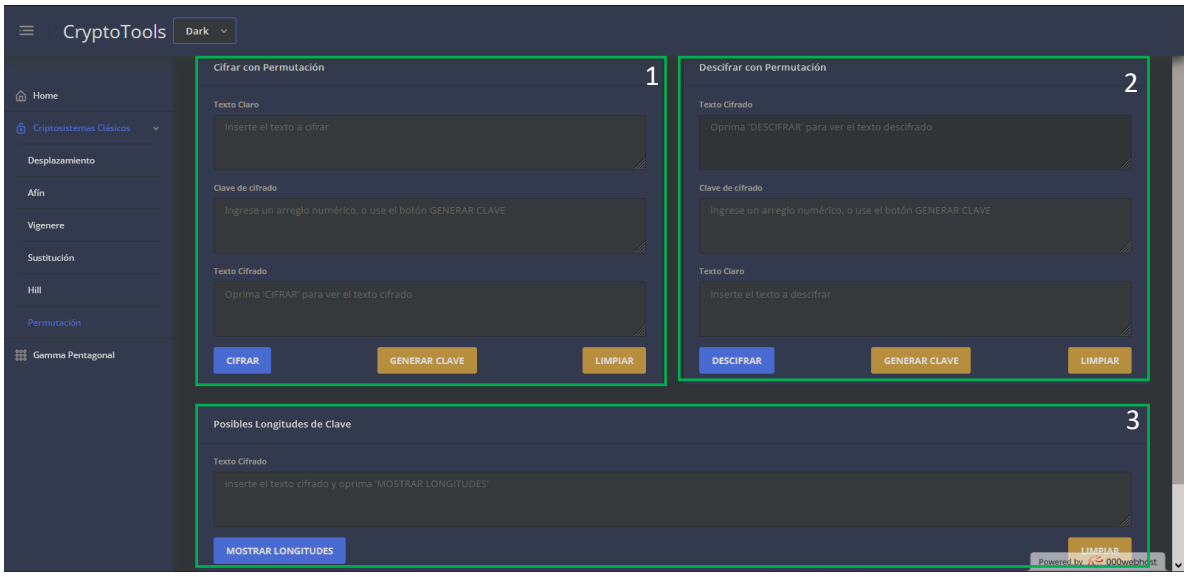


La tercera subsección realiza el criptoanálisis. Requiere un texto claro y el texto que se obtiene al cifrarlo. Posterior al ingreso de ambos textos y de seleccionar el botón azul **Encontrar Clave**, el usuario verá la clave que se usó para cifrar al texto claro. Para el criptoanálisis, se presupone que para la clave utilizada se usó una matriz del tamaño igual al que se usa para cifrar y descifrar.

El botón amarillo de **Limpiar** en cada subsección elimina el contenido de los recuadros por si se ve necesario.

f) Permutación

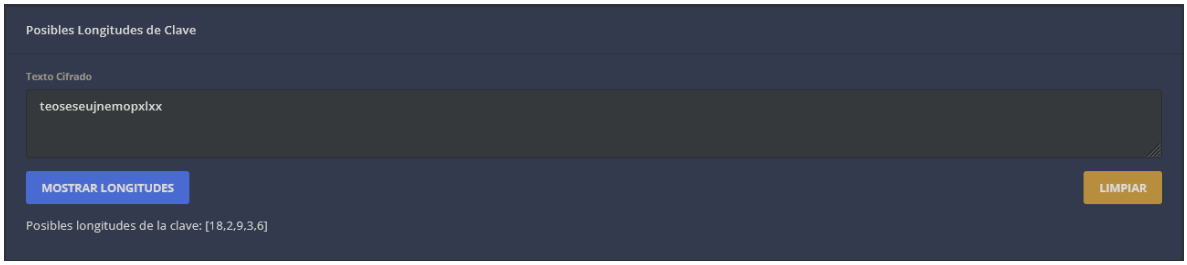
En la sección de **Permutación** distinguimos tres subsecciones.



Las dos primeras subsecciones realizan las operaciones de ciframiento y desciframiento de forma respectiva. Para cifrar (descifrar) se ingresa el texto claro (cifrado) y la clave. Luego se presiona el botón de **Cifrar** (**Descifrar**) azul, en la parte baja del recuadro verde respectivo. En estas dos subsecciones en la parte inferior central se encuentra el botón de generar clave.

Restricciones sobre la clave: Una permutación sobre el conjunto {1, 2, ..., m}.

La tercera subsección realiza el criptoanálisis. Solo requiere un texto. Posterior al ingreso de este y de seleccionar el botón azul **Mostrar Longitudes**, el usuario verá las posibles longitudes de la clave. Es decir, el valor de m.



El botón amarillo de **Limpiar** en cada subsección elimina el contenido de los recuadros por si se ve necesario.