

Manual de Usuario - CryptoTools

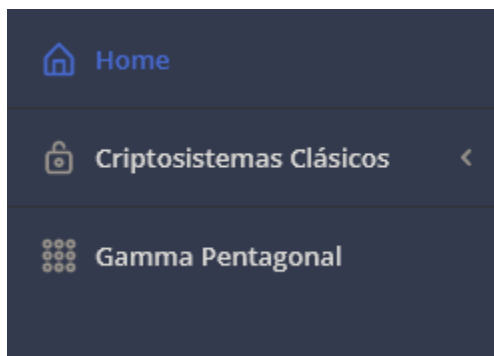
Este es el manual de usuario para la herramienta CryptoTools que hace parte de la materia Introducción a la criptografía y a la teoría de información, en su primera versión. Aquí se pueden encontrar implementados los siguientes módulos:

1. Criptosistemas clásicos
 - a. Desplazamiento
 - b. Afín
 - c. Vigenere
 - d. Sustitución
 - e. Hill
 - f. Permutación
2. Criptosistemas de bloque.
 - a. S-DES
 - b. DES
 - c. T-DES
 - d. AES
3. Gamma Pentagonal.

● 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

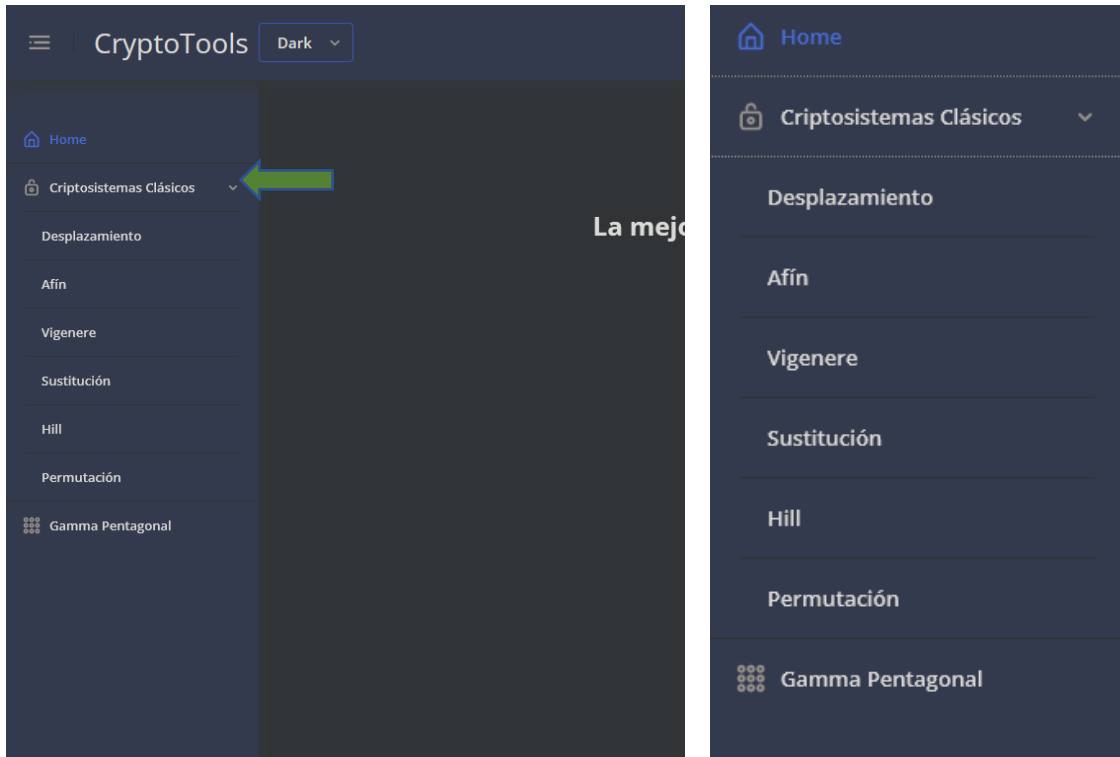


Corporate



1. 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.

The screenshot displays the CryptoTools web application interface. On the left is a dark sidebar with a menu containing 'Home', 'Criptosistemas Clásicos' (expanded), 'Desplazamiento', 'Afin', 'Vigenere', 'Sustitución', 'Hill', 'Permutación', and 'Gamma Pentagonal'. The main area has a dark background with three sub-sections highlighted by green boxes and numbered 1, 2, and 3. Sub-section 1, 'Cifrar con Desplazamiento', includes a 'Texto Claro' input field with the placeholder 'Inserte el texto a cifrar', a 'Texto Cifrado' output field with the placeholder 'Oprima "CIFRAR" para ver el texto cifrado', a 'Clave de cifrado' input field with a value of '0' and a range indicator from 0 to 25, and 'CIFRAR' and 'LIMPIAR' buttons. Sub-section 2, 'Descifrar con Desplazamiento', includes a 'Texto Cifrado' input field with the placeholder 'Inserte el texto a descifrar', a 'Texto Claro' output field with the placeholder 'Oprima "DESCIFRAR" para ver el texto descifrado', a 'Clave de cifrado' input field with a value of '0' and a range indicator from 0 to 25, and 'DESCIFRAR' and 'LIMPIAR' buttons. Sub-section 3, 'Analizar con Desplazamiento', includes a 'Texto Cifrado' input field with the placeholder 'Inserte el texto cifrado y oprima "ANALIZAR"', and an 'ANALIZAR' button. A 'LIMPIAR' button is also present at the bottom right of this section. The interface is powered by 'uUuWebTools'.

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.

Analizar con Desplazamiento

Texto Cifrado

esto es solo un ejemplo

ANALIZAR LIMPIAR

Filtrar por coincidencias:

clave	texto
0	estoessolonejemplo
1	drsndrrnkntmdidlokn
2	cqrmcqmqjmslchcknjm
3	bpqibppllrkbgbjmil
4	aopkaookhkqajafailhk
5	znojznnjgipizezhkgj
6	ymniymmfiohydygfi

Continúa hacia abajo

Powered by 000webhost

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.

CryptoTools Dark

Home

Criptosistemas Clásicos

Desplazamiento

Afín

Vigenere

Sustitución

Hill

Permutación

Gamma Pentagonal

1

Cifrar con Afín

Texto Claro

Inserte el texto a cifrar

Texto Cifrado

Oprima 'CIFRAR' para ver el texto cifrado

Clave de cifrado a Clave de cifrado b

0 0

CIFRAR LIMPIAR

2

Descifrar con Afín

Texto Cifrado

Inserte el texto a descifrar

Texto Claro

Oprima 'DESCIFRAR' para ver el texto descifrado

Clave de cifrado a Clave de cifrado b

0 0

DESCIFRAR LIMPIAR

3

Analizar con Afín

Texto Cifrado

Inserte el texto cifrado y oprima 'ANALIZAR'

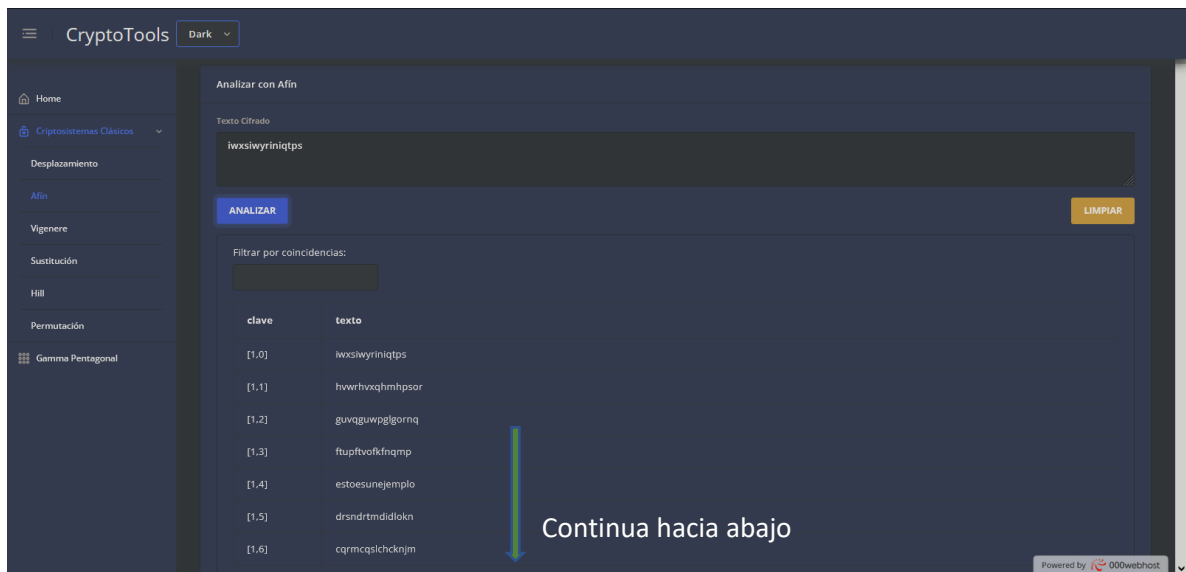
ANALIZAR LIMPIAR

Powered by 000webhost

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.

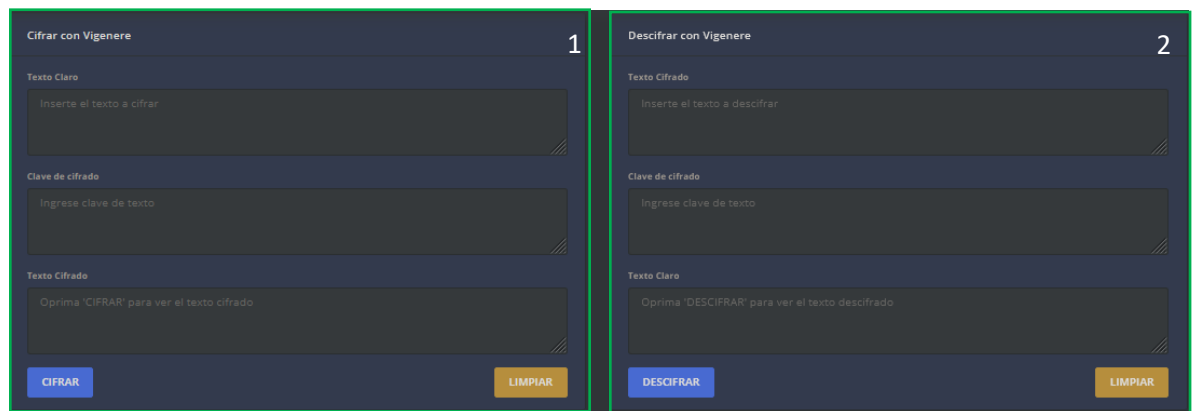
La tercera subsección realiza el criptoanálisis. Solo requiere un texto. Posterior al ingreso de este y de seleccionar el botón azul **Analizar**, se procede a descifrar ese texto con todas las posibles claves. El usuario podrá filtrar por coincidencias en un recuadro, o buscar una clave particular.



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

c) Vigenere

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



Índices de Coincidencia 3

Texto Cifrado
Inserte el texto cifrado

Máximo valor de m (longitud de clave)
10

MOSTRAR ÍNDICES **LIMPIAR**

Analizar con Vigenere 4

Texto Cifrado
Inserte el texto cifrado

Longitud de clave (m)
1

ENCONTRAR CLAVE **LIMPIAR**

Clave:

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.

Filtrar por coincidencias:
Buscar en la tabla

m	índices
1	0.045
2	0.046 0.041
3	0.043 0.05 0.047
4	0.042 0.039 0.045 0.04
5	0.063 0.068 0.069 0.061 0.072

Analizar con Vigenere

Texto Cifrado
PEEWVKAKOEWADREMXMI BHHCHKIKUNVRZLH
RCLQOHP
WQAIWXNRMGWOLFKEE

Longitud de clave (m)
5

ENCONTRAR CLAVE **LIMPIAR**

Clave: janet

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.

The screenshot shows the CryptoTools interface with three main sections highlighted by green boxes and numbered 1, 2, and 3.

- Section 1: Cifrar con Afin**
 - Text input: "Texto Claro" (Inserte el texto a cifrar)
 - Text input: "Texto Cifrado" (Oprima 'CIFRAR' para ver el texto cifrado)
 - Key input: "Clave de cifrado a" (0) and "Clave de cifrado b" (0)
 - Buttons: "CIFRAR" (blue) and "LIMPIAR" (orange)
- Section 2: Descifrar con Afin**
 - Text input: "Texto Cifrado" (Inserte el texto a descifrar)
 - Text input: "Texto Claro" (Oprima 'DESCIFRAR' para ver el texto descifrado)
 - Key input: "Clave de cifrado a" (0) and "Clave de cifrado b" (0)
 - Buttons: "DESCIFRAR" (blue) and "LIMPIAR" (orange)
- Section 3: Analizar con Afin**
 - Text input: "Texto Cifrado" (Inserte el texto cifrado y oprima 'ANALIZAR')
 - Button: "ANALIZAR" (blue)
 - Button: "LIMPIAR" (orange)

At the bottom right, it says "Powered by 000webhost".

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.

The screenshot shows the 'Analizar con Afin' section of the CryptoTools interface. The 'Texto Cifrado' field contains the text "iwxsiwyriniqtps". The "ANALIZAR" button is highlighted in blue. Below the input fields, there is a section for filtering results by coincidences, with a table showing the results for different keys.

clave	texto
[1,0]	iwxsiwyriniqtps
[1,1]	hwrhvxqhmhpsor
[1,2]	guvguwpqgornq
[1,3]	fuqftvofkfnqmp
[1,4]	estoesunejemplo
[1,5]	drsndrtmdidlokn
[1,6]	cqrmcqlchcknqm

A blue arrow points downwards from the table, with the text "Continúa hacia abajo" (Continue down) next to it.

At the bottom right, it says "Powered by 000webhost".

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.

The image displays three screenshots of a web application for the Hill cipher, numbered 1, 2, and 3.

1. Cifrar con Hill (Encrypt): This interface has a dark blue background. On the left, there is a yellow button labeled 'CARGAR IMAGEN CLARA'. On the right, there are four input fields for keys: 'Clave de cifrado 1' (value 7), 'Clave de cifrado 2' (value 2), 'Clave de cifrado 3' (value 3), and 'Clave de cifrado 4' (value 13). Below these fields are three buttons: a blue 'CIFRAR' button, a yellow 'DESCARGAR IMAGEN' button, and a yellow 'LIMPIAR' button.

2. Descifrar con Hill (Decrypt): This interface is similar to the first one. It has a yellow button 'CARGAR IMAGEN CIFRADA' on the left. The key input fields on the right have the same values (7, 2, 3, 13). The buttons on the right are a blue 'DESCIFRAR' button, a yellow 'DESCARGAR IMAGEN' button, and a yellow 'LIMPIAR' button.

3. Analizar con Hill: This interface has a dark blue background. It features two large text input areas. The first is labeled 'Texto Claro' with a placeholder 'Inserta el texto claro'. The second is labeled 'Texto Cifrado' with a placeholder 'Inserta el texto cifrado'. At the bottom left is a blue button 'ENCONTRAR CLAVE', and at the bottom right is a yellow 'LIMPIAR' button. Below the buttons, there is a label 'Clave:' followed by a text input field.

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.

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

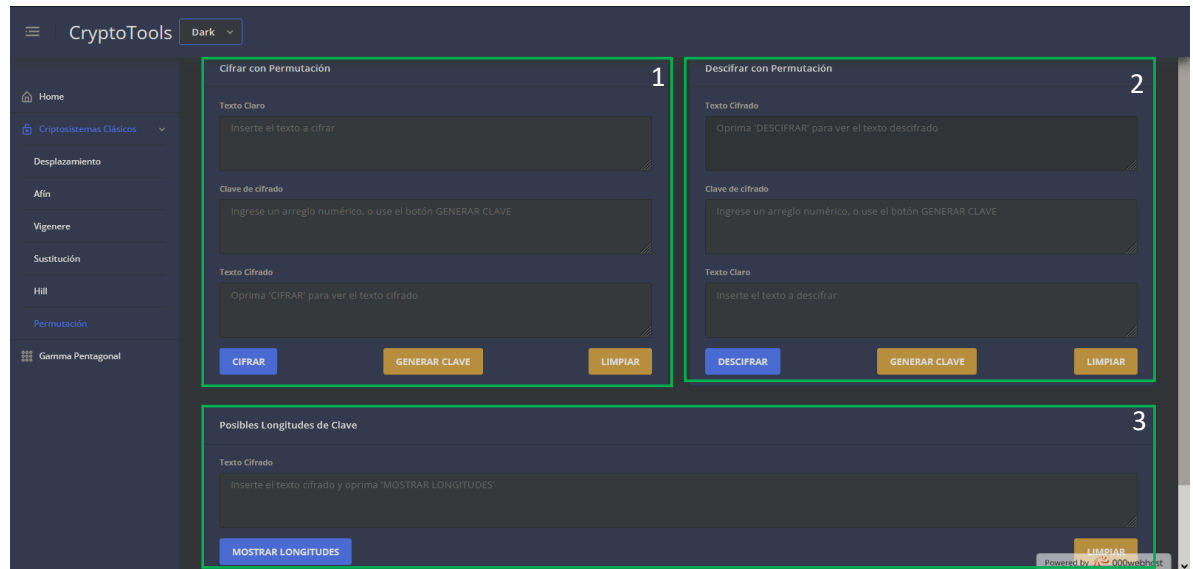
Se recomienda que esta matriz sea invertible para poder descifrar la imagen ingresada y que no sea la matriz identidad para que el cifrado sea apropiado. Una buena clave es la que viene por defecto.

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

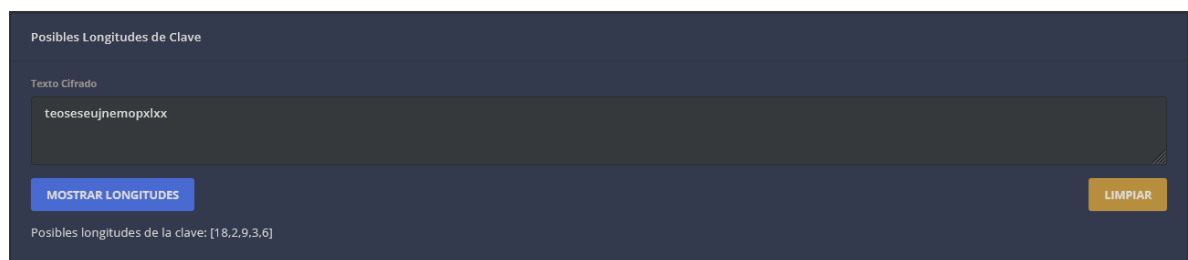
En la sección de **Permutación** distinguimos tres subsecciones.



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 $\{1, 2, \dots, m\}$.

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.

2. Criptosistemas de bloque.



Para acceder a los criptosistemas de bloque, se selecciona la opción “Criptosistemas de Bloque” y allí saldrá un menú desplegable con las siguientes opciones:

Nota: Si no se alcanzan a ver todos los botones de los recuadros, en la parte inferior hay una barra de desplazamiento para poder ver todo el contenido. También se puede esconder el menú principal de la izquierda dando click al lado izquierdo del título de la página web.

a) S-DES

El más sencillo de todos los criptosistemas de bloque, requiere para texto una entrada de ocho bits en binarios, también una clave de diez bits en binario, tanto para cifrar como para descifrar, con estas dos entradas le damos click a cifrar o descifrar para cualquiera de nuestros dos propósitos, en la siguiente imagen podemos ver un ejemplo de cifrado y otro de descifrado.

Cifrar con DES Simplificado

Texto Claro

Clave de cifrado

Texto Cifrado

CIFRAR LIMPIAR

Descifrar con DES Simplificado

Texto Cifrado

Clave de cifrado

Texto Claro

DESCIFRAR LIMPIAR

b) DES


Al hacer click en esta opción se mostrará una página que contiene dos recuadros por cada modo de ciframiento, uno para cifrar y otro para descifrar. Lo primero que debemos hacer es buscar en los títulos de los recuadros qué modo de ciframiento queremos: ECB, CBC, OFB, CFB, o CTR.

Luego, si el modo escogido es **ECB**, para **cifrar** tendremos que: escribir en el cuadro de texto correspondiente una **clave** usando **hexadecimales** (de longitud 16 en minúsculas las letras), dar click en el botón de “**CARGAR IMAGEN CLARA**” y darle al botón cifrar. La imagen cifrada aparecerá en el cuadro adjunto de descifrado.

Cifrar con DES-ECB

Clave


CARGAR IMAGEN CLARA CIFRAR DESCARGAR IMAGEN LIMPIAR



Descifrar con DES-ECB

Clave

CARGAR IMAGEN CIFRADA DESCIFRAR DESCARGAR IMAGEN LIMPIAR



Para **descifrar**, primero hacemos click en limpiar en el recuadro de cifrar, luego podemos subir una imagen cifrada (o usar la que ya aparezca) y para descifrarla elegimos el tamaño de clave, escribimos la clave con la que se cifró y le damos al

botón descifrar:

Cifrar con DES-ECB

Clave


Inserte clave para cifrar

CARGAR IMAGEN CLARA

CIFRAR

DESCARGAR IMAGEN

LIMPIAR



Descifrar con DES-ECB

Clave


f1c3521bd935ca3b

CARGAR IMAGEN CIFRADA

DESCIFRAR

DESCARGAR IMAGEN

LIMPIAR



Además, para **cifrar** en los otros modos (CBC, OFB, CFB, o CTR) se sigue un procedimiento similar, sólo que en este caso se requiere de otro parámetro (**Vector Inicial, hexadecimales de longitud 16**) Así, digitamos la clave y el vector inicial, cargamos la imagen clara y le damos al botón “**CIFRAR**”:

Cifrar con DES-CBC

Clave

f1c3521bd935ca3b

Vector Inicial


c35f1383c65ad09a

CARGAR IMAGEN CLARA

CIFRAR

DESCARGAR IMAGEN

LIMPIAR



Descifrar con DES-CBC

Clave

Inserte clave para descifrar

Vector Inicial


Inserte texto para usar como vector inicial

CARGAR IMAGEN CIFRADA

DESCIFRAR

DESCARGAR IMAGEN

LIMPIAR



Luego, para **descifrar** en CBC, OFB o CFB en primer lugar se le da al botón “**LIMPIAR**” en la sección de cifrado en el modo, después se usan los mismos parámetros de clave y vector inicial para descifrar la imagen que se suba con el botón “**CARGAR IMAGEN CIFRADA**” o con la que ya aparezca usando el botón “**DESCIFRAR**”.

Cifrar con DES-CBC

Clave

Inserte clave para cifrar

Vector Inicial


Inserte texto para usar como vector inicial

CARGAR IMAGEN CLARA

CIFRAR

DESCARGAR IMAGEN

LIMPIAR



Descifrar con DES-CBC

Clave

f1c3521bd935ca3b

Vector Inicial


c35f1383c65ad09a

CARGAR IMAGEN CIFRADA

DESCIFRAR

DESCARGAR IMAGEN

LIMPIAR



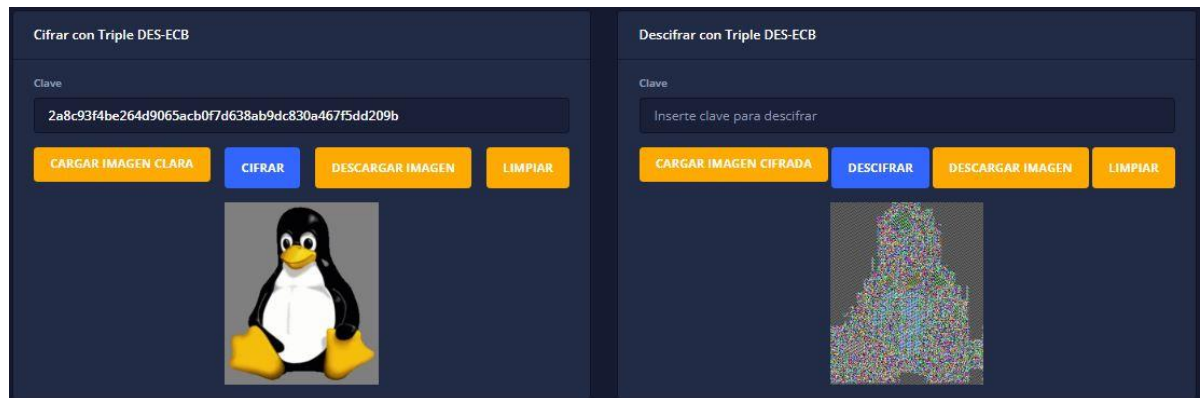
Nota: Para el modo contador (CTR) el vector inicial debe tener al menos los últimos 8 hexadecimales en 0, pueden ser menos de 8 pero depende del tamaño de bits de la imagen, es decir, la cantidad de bloques a cifrar, ejemplo, el siguiente vector inicial puede tomar imágenes para hasta dos elevado a la treinta y dos cifrados o descifrados: **7a6d39e400000000**.

(Estos cifrados pueden tardar entre 5 segundos y 1 minutos, por favor aguarde a que se cifre o descifre la imagen).

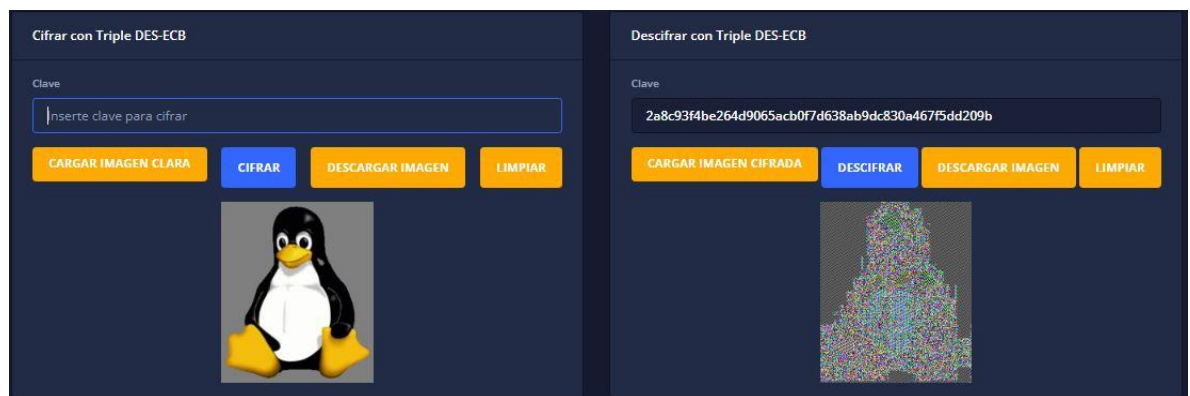
c) T-DES

Al hacer click en esta opción se mostrará una página que contiene dos recuadros por cada modo de ciframiento, uno para cifrar y otro para descifrar. Lo primero que debemos hacer es buscar en los títulos de los recuadros qué modo de ciframiento queremos: ECB, CBC, OFB, CFB, o CTR.

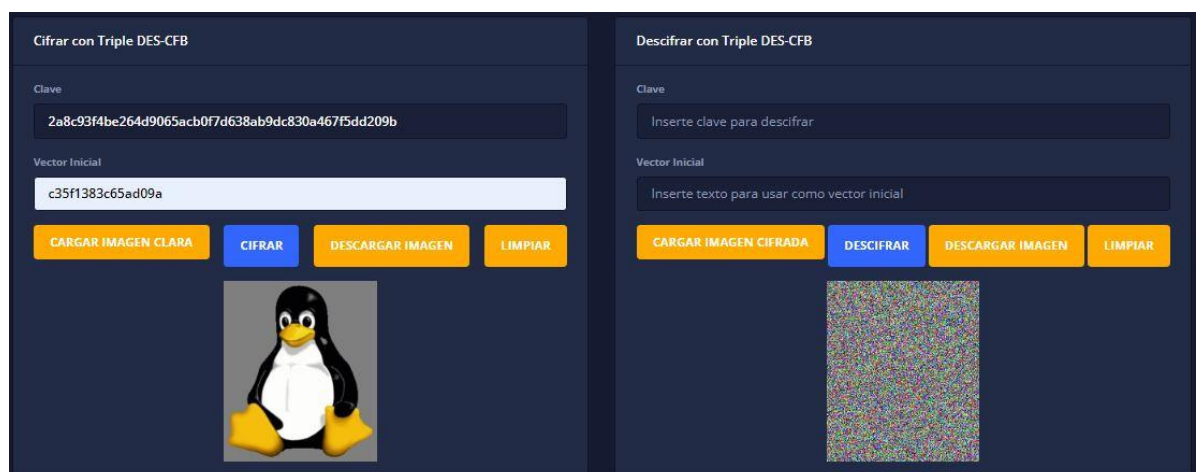
Luego, si el modo escogido es **ECB**, para **cifrar** tendremos que: escribir en el cuadro de texto correspondiente una **clave** usando **hexadecimales** (de longitud 46 en minúsculas las letras), dar click en el botón de “**CARGAR IMAGEN CLARA**” y darle al botón cifrar. La imagen cifrada aparecerá en el cuadro adjunto de descifrado.



Para **descifrar**, primero hacemos click en limpiar en el recuadro de cifrar, luego podemos subir una imagen cifrada (o usar la que ya aparezca) y para descryptarla elegimos el tamaño de clave, escribimos la clave con la que se cifró y le damos al botón descifrar:



Además, para **cifrar** en los otros modos (CBC, OFB, CFB, o CTR) se sigue un procedimiento similar, sólo que en este caso se requiere de otro parámetro (**Vector Inicial, hexadecimales de longitud 16**) Así, digitamos la clave y el vector inicial, cargamos la imagen clara y le damos al botón “**CIFRAR**”:



Luego, para **descifrar** en CBC, OFB, CFB, o CTR en primer lugar se le da al botón “**LIMPIAR**” en la sección de cifrado en el modo, después se usan los mismos parámetros de clave y vector inicial para descifrar la imagen que se suba con el botón “**CARGAR IMAGEN CIFRADA**” o con la que ya aparezca usando el botón “**DESCIFRAR**”.

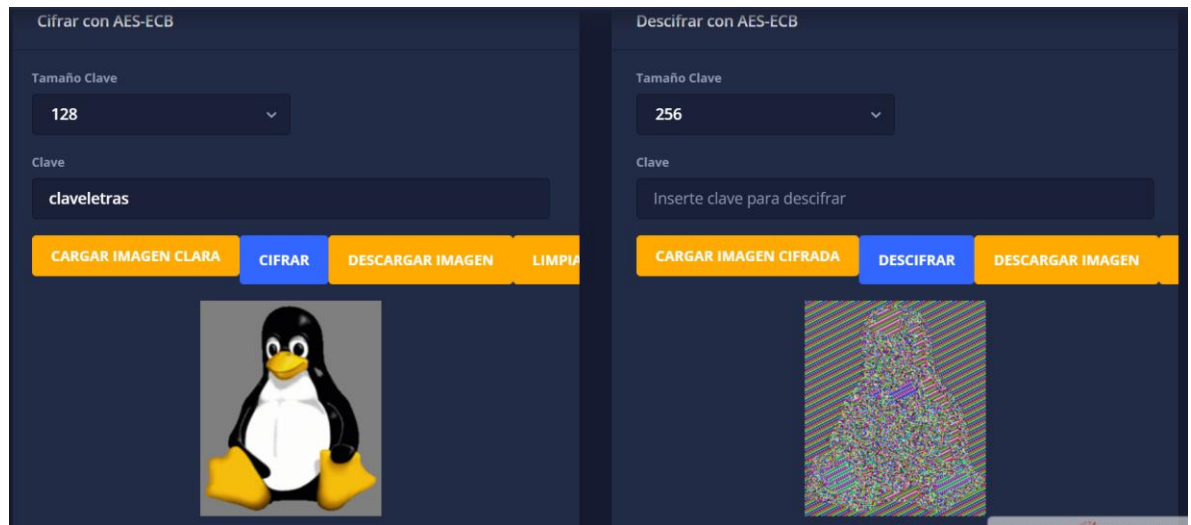
Nota: Para el modo contador (CTR) el vector inicial debe tener al menos los últimos 8 hexadecimales en 0, pueden ser menos de 8 pero depende del tamaño de bits de la imagen, es decir, la cantidad de bloques a cifrar, ejemplo, el siguiente vector inicial puede tomar imágenes para hasta dos elevado a la treinta y dos cifrados o descifrados: **7a6d39e400000000**.

(Estos cifrados pueden tardar entre 5 segundos y 1 minutos, por favor aguarde a que se cifre o descifre la imagen).

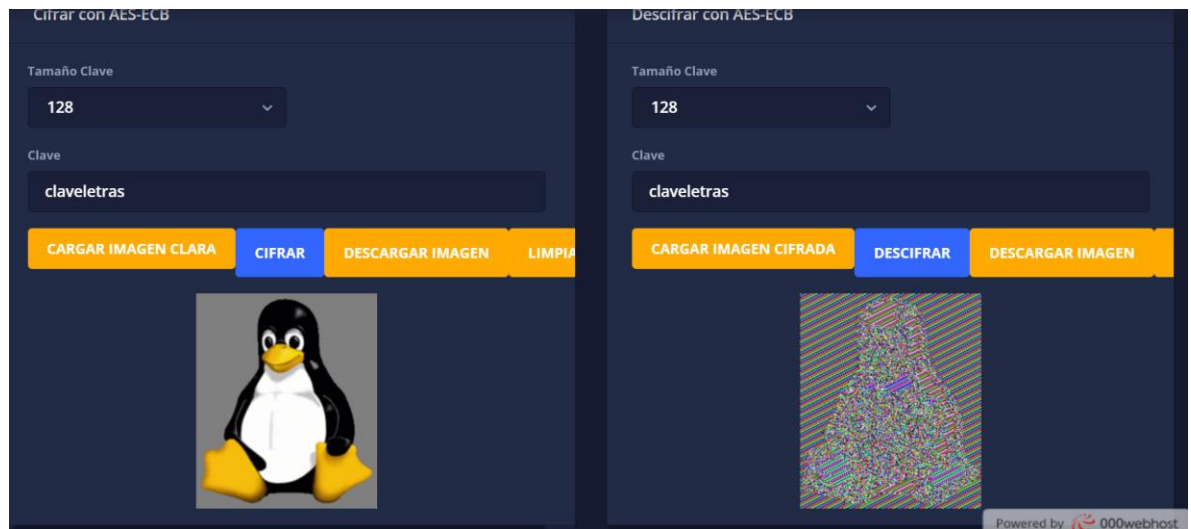
d) AES

Al hacer click en esta opción se mostrará una página que contiene dos recuadros por cada modo de ciframiento, uno para cifrar y otro para descifrar. Lo primero que debemos hacer es buscar en los títulos de los recuadros qué modo de ciframiento queremos: ECB, CBC, OFB, CFB, o CTR.

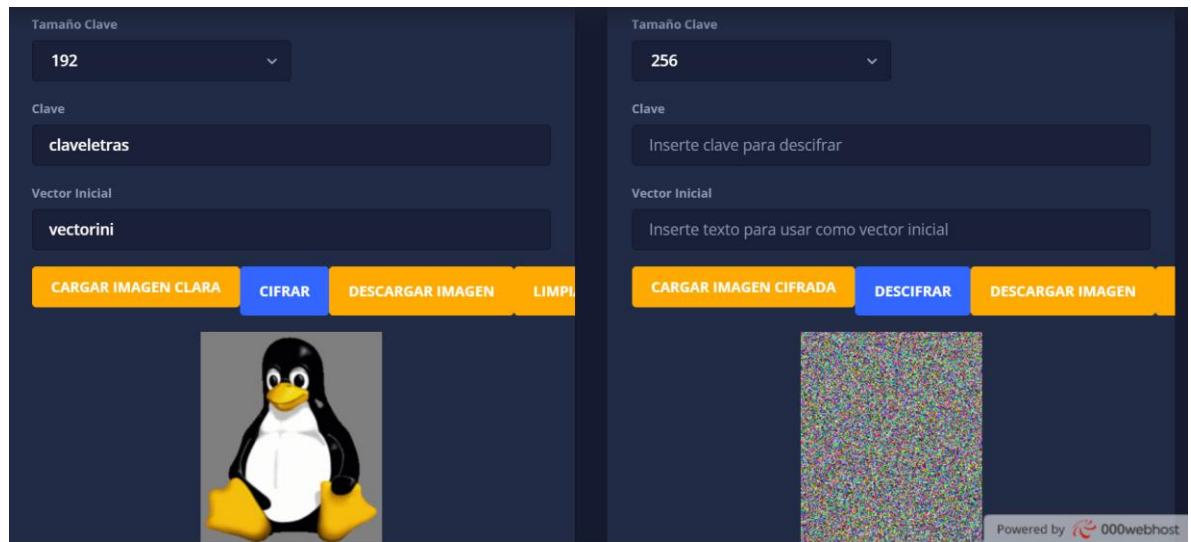
Luego, si el modo escogido es **ECB**, para **cifrar** tendremos que: elegir el tamaño deseado de la clave, escribir en el cuadro de texto correspondiente una **clave** usando **letras** (esta será completada y transformada en los bits necesarios), dar click en el botón de “**CARGAR IMAGEN CLARA**” y darle al botón cifrar. La imagen cifrada aparecerá en el cuadro adjunto de descifrado.



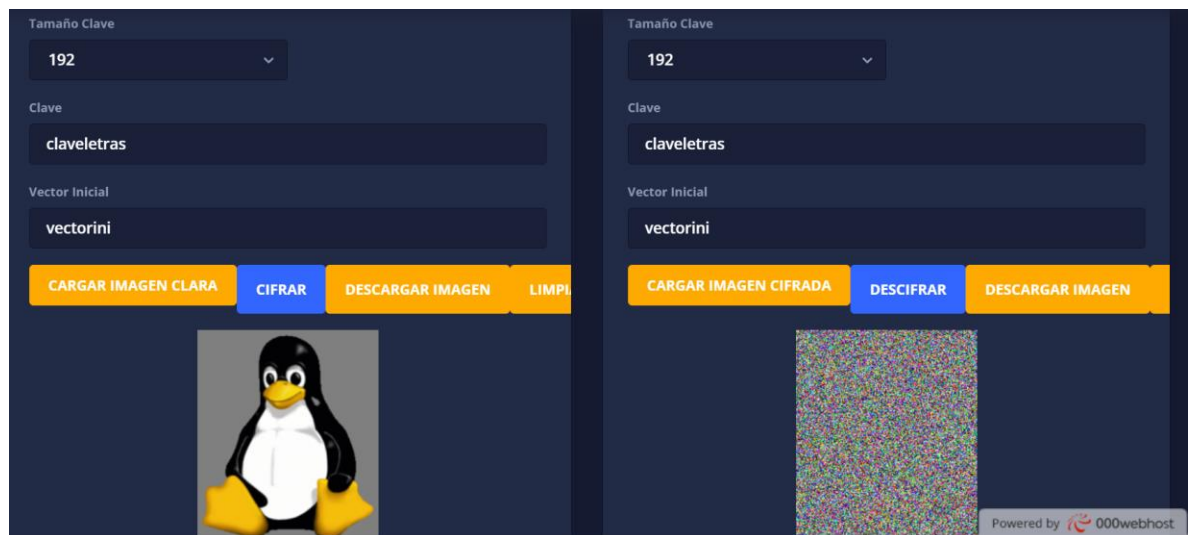
Para **descifrar**, primero hacemos click en limpiar en el recuadro de cifrar, luego podemos subir una imagen cifrada (o usar la que ya aparezca) y para descryptarla elegimos el tamaño de clave, escribimos la clave con la que se cifró y le damos al botón descifrar:



Además, para **cifrar** en los otros modos (CBC, OFB, CFB, o CTR) se sigue un procedimiento similar, sólo que en este caso se requiere de otro parámetro (**Vector Inicial**) que es un **texto** formado por **letras**. Así, seleccionamos el tamaño de clave, digitamos la clave y el vector inicial, cargamos la imagen clara y le damos al botón “CIFRAR”:

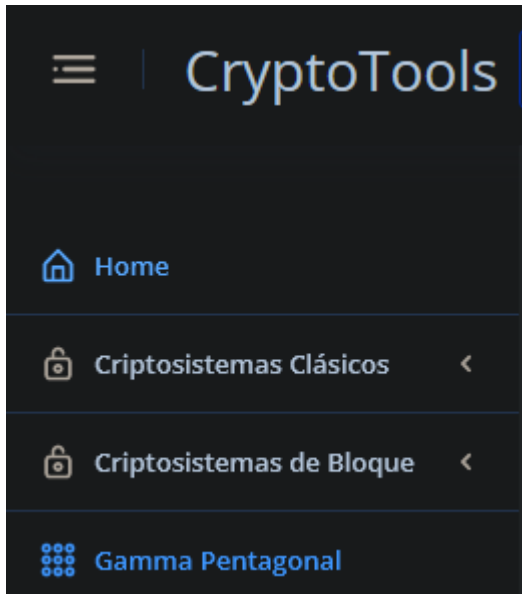


Luego, para **descifrar** en CBC, OFB, CFB, o CTR en primer lugar se le da al botón “**LIMPIAR**” en la sección de cifrado en el modo, después se usan los mismos parámetros de longitud de clave, clave y vector inicial para descifrar la imagen que se suba con el botón “**CARGAR IMAGEN CIFRADA**” o con la que ya aparezca usando el botón “**DESCIFRAR**”.



Nota: Al descifrar con los modos CBC y CFB el vector inicial sólo se usa para el primer bloque por lo que puede omitirse para estos modos al descifrar.

3. Gamma pentagonal.



Para acceder al criptosistema **Gamma Pentagonal**, se selecciona ese módulo en la barra izquierda de la página web.

En **Gamma Pentagonal** solo se cuenta con una única sección seleccionada por defecto, allí distinguimos siete subsecciones.

En este caso el orden de las subsecciones es importante para acceder al cifrado y descifrado usando el criptosistema gamma pentagonal. Estos dos siendo las dos subsecciones **6** y **7** de forma respectiva.

En la **primera** subsección se piden dos enteros **x,y** que corresponden al punto inicial del grafo a dibujar.

En la **segunda** subsección se requiere una permutación que se utilizará en el cifrado. Una vez ingresada una permutación válida el usuario deberá seleccionar el botón **de APLICAR PERMUTACIÓN** para ingresarla al sistema después de esto el usuario verá reflejada la permutación ingresada y su efecto en la subsección **cinco**.

En la tercera subsección se selecciona el grafo a utilizar en el **Cifrado (Descifrado)** una vez seleccionado se debe seleccionar el botón **DIBUJAR GRAFO** donde el usuario verá reflejado el grafo seleccionado en la subsección cuatro.

La sección **seis (siete)** corresponde al **cifrado (descifrado)** donde se pide al usuario un texto **claro (cifrado)**. Aquí la clave es una tupla compuesta por el punto inicial, el grafo ingresado y la permutación.

Restricciones sobre la clave: El punto inicial debe tener coordenadas enteras, la permutación debe ser válida.

El botón amarillo de **LIMPIAR** en las subsecciones seis y siete elimina el texto ingresado.