Manual de Usuario

“Cryptos”

Nombre: Jhohan Ricardo Franco Sánchez

Curso: Introducción a la criptografía y a la seguridad de la información

Tabla de contenidos

Contenido

[Cifradores y descifradores 3](#_Toc431285920)

[Criptosistema 3](#_Toc431285921)

[Ventana principal 4](#_Toc431285922)

[Menú Archivo 5](#_Toc431285923)

[Menú Herramientas 6](#_Toc431285924)

[Algoritmos 6](#_Toc431285925)

[Desplazamiento 6](#_Toc431285926)

[Funciones de encriptamiento y desencriptamiento 6](#_Toc431285927)

[Ventana 6](#_Toc431285928)

[Sustitución 7](#_Toc431285929)

[Ventana 7](#_Toc431285930)

[Afín 7](#_Toc431285931)

[Funciones de encriptamiento y desencriptamiento 7](#_Toc431285932)

[Ventana 7](#_Toc431285933)

[Vigenere 7](#_Toc431285934)

[Funciones de encriptamiento y desencriptamiento 8](#_Toc431285935)

[Ventana 8](#_Toc431285936)

[Permutación 8](#_Toc431285937)

[Ventana 8](#_Toc431285938)

[DES- SIMPLIFICADO 9](#_Toc431285939)

[Ventana 9](#_Toc431285940)

[CIFRAMIENTO DE IMÁGENES 9](#_Toc431285941)

[Ventana principal 9](#_Toc431285942)

[1 SECRET 2 SHARES 9](#_Toc431285943)

[Metodología 9](#_Toc431285944)

[Ventana de Cifrado 10](#_Toc431285945)

[Ventana de descifrado 10](#_Toc431285946)

[2 SECRETS 2 SHARES 10](#_Toc431285947)

[Metodología 10](#_Toc431285948)

[Ventana de Cifrado 11](#_Toc431285949)

[Ventana de descifrado 12](#_Toc431285950)

# Cifradores y descifradores

En criptografía, el cifrado es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.

A veces el texto cifrado se escribe en bloques de igual longitud. A estos bloques se les denomina grupos. Estos grupos proporcionaban una forma de verificación adicional, ya que el texto cifrado obtenido debía tener un número entero de grupos. Si al cifrar el texto plano no se tiene ese número entero de grupos, entonces se suele rellenar al final con ceros o con caracteres sin sentido.

Aunque el cifrado pueda volver secreto el contenido de un documento, es necesario complementarlo con otras técnicas criptográficas para poder comunicarse de manera segura. Puede ser necesario garantizar la integridad la autenticación de las partes, etcétera.

# Criptosistema

Un criptosistema se define como una quíntupla (M, C, K, E, D), donde:

* M representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto plano) que pueden ser enviados.
* C representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
* K representa el conjunto de claves que se pueden emplear en el criptosistema.
* E es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente Ek para cada valor posible de la clave k.
* D es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema ha de cumplir la siguiente condición:

Dk(Ek(m)) = m

Es decir, que si tenemos un mensaje m, lo ciframos empleando la clave k y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original m.

# Ventana principal

En esta ventana se muestra todos los elementos de la aplicación, en los cuales tenemos:

Panel Texto en claro: Todas las cadenas que se deseen encriptar se ingresan por esta área de texto.

Panel Texto encriptado: Todas las cadenas que se deseen des encriptar se ingresan por esta área de texto.

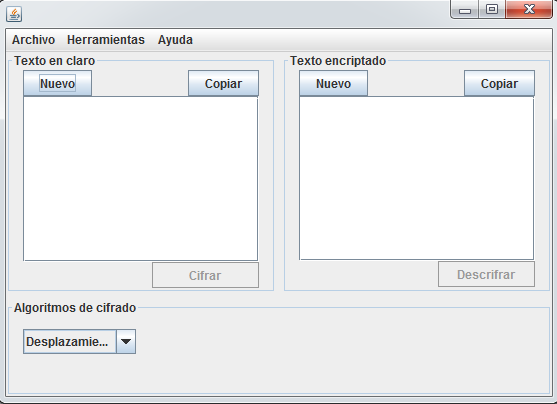
Botón Cifrar: El texto que se encuentre en el panel de Texto en claro será cifrado y mostrado en el panel Texto encriptado.

Botón Descifrar: El texto que se encuentre en el panel de Texto cifrado será descifrado y mostrado en el panel Texto en claro.

Selector de Algoritmos: Selecciona los algoritmos con los cuales se puede encriptar y des encriptar textos.

Botones Nuevo: Hacer click sobre estos botones activa la ventana del panel de Texto en claro para ingresar las cadenas a ser encriptadas.

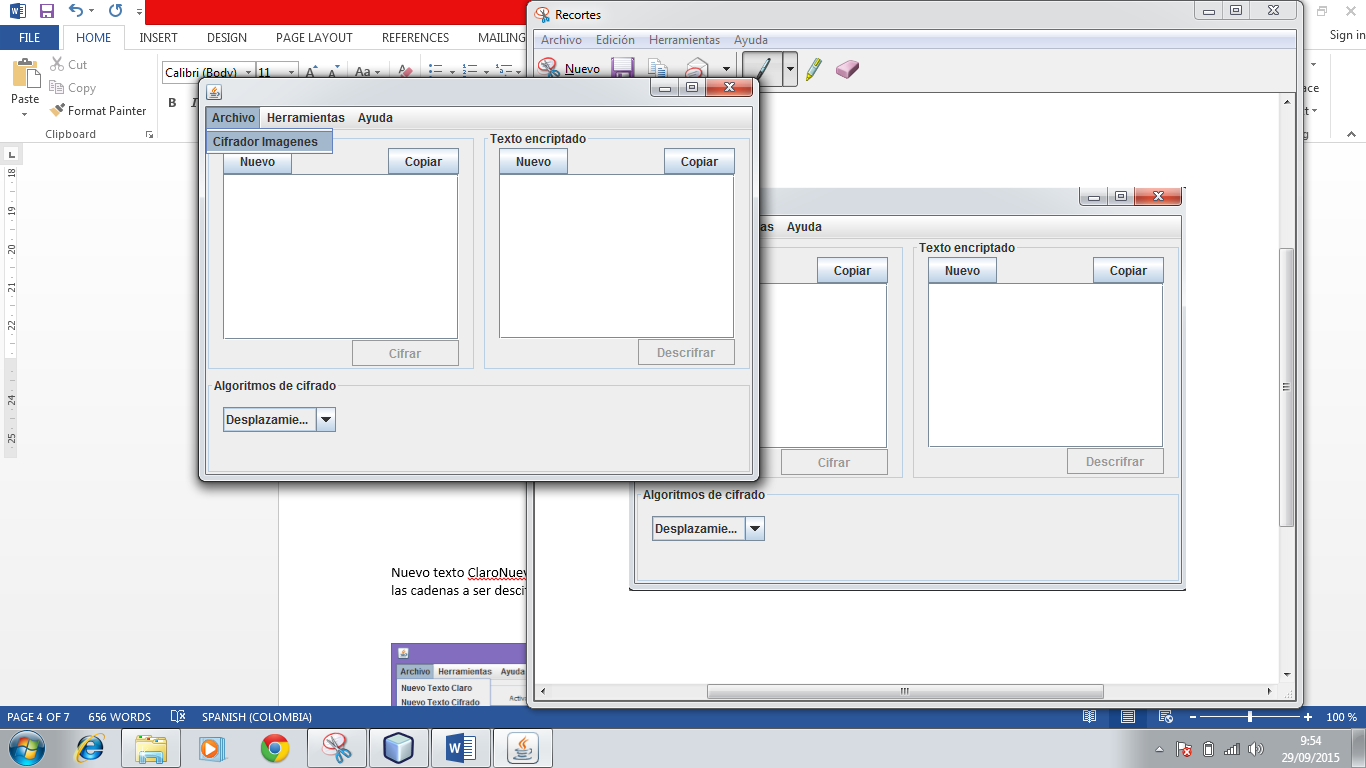
Botones Copiar: copiado de los textos una vez son cifradas o descifradas.



## Menú Archivo

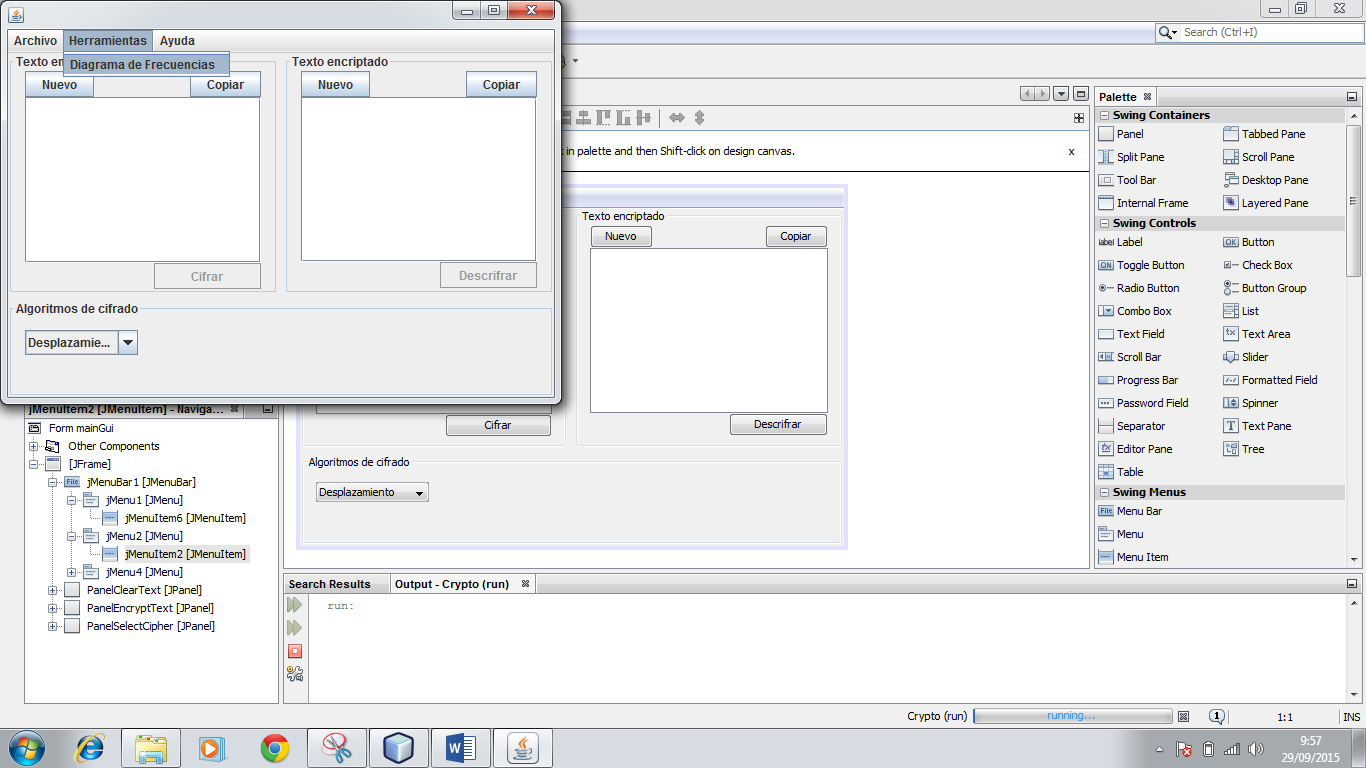
En este menú podemos seleccionar:

Cifrador Imágenes: Activa la ventana del panel de cifrado de imágenes.



## Menú Herramientas

En este menú se pueden encontrar las herramientas de apoyo para Cifrar y Descifrar textos.



# Algoritmos

## Desplazamiento

### Funciones de encriptamiento y desencriptamiento

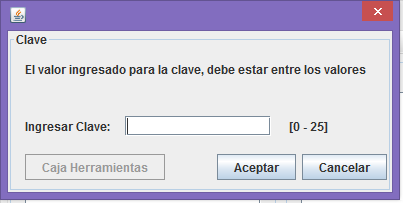
E_n(x) = x + n \mod {27}.

D_n(x) = x - n \mod {27}.

### Ventana

Ventana que permite ingresar un número del 0 al 25 para realizar el desplazamiento

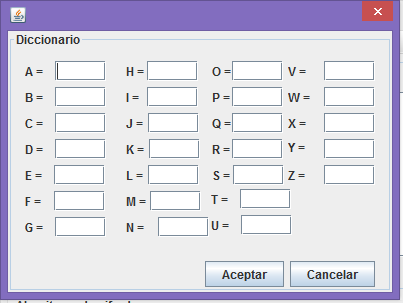
Botón Caja Herramientas: da acceso a la caja de herramientas de DESENCRIPTAMIENTO del algoritmo.



## Sustitución

### Ventana

Ingresar cada uno de los valores para cada letra a ser reemplazada



## Afín

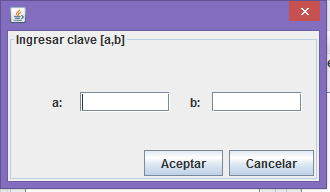
### Funciones de encriptamiento y desencriptamiento

\mbox{E}(x)=(ax+b)\mod{m},

\mbox{D}(x)=a^{-1}(x-b)\mod{m},

### Ventana

Ventana para ingresar los valores de a y b respectivamente



## Vigenere

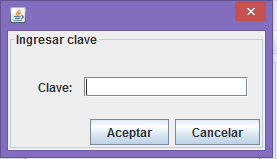
### Funciones de encriptamiento y desencriptamiento

C_i = E_K(M_i) = (M_i+K_i) \mod {26}

M_i = D_K(C_i) = (C_i-K_i) \mod {26}

### Ventana

Ventana para ingresar la palabra clave.

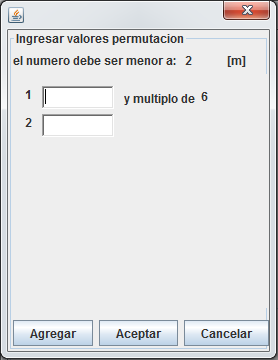


## Permutación

### Ventana

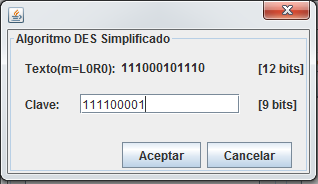
Ventana para ingresar la clave de cifrado y descifrado.

Botón Agregar: botón para agregar un espacio al arreglo de la clave.



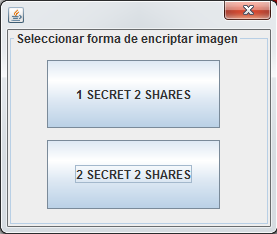
## DES- SIMPLIFICADO

### Ventana



# CIFRAMIENTO DE IMÁGENES

### Ventana principal



## 1 SECRET 2 SHARES

### Metodología

El algoritmo que se siguió para la expansión del pixel fue basado en la siguiente tabla:

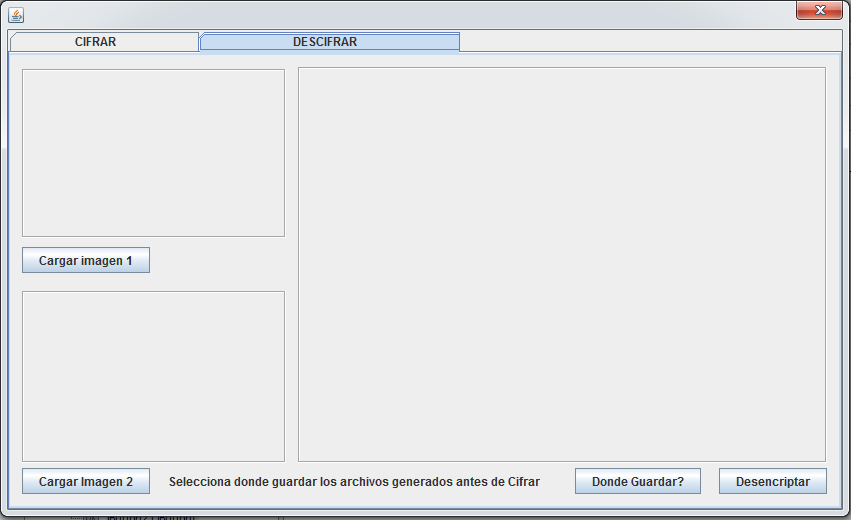


Tabla.1: modelo de criptografía visual Naor y Shamir

### Ventana de Cifrado



### Ventana de descifrado



## 2 SECRETS 2 SHARES

### Metodología

El algoritmo que se siguió para la expansión del pixel fue basado en la siguiente tabla:



Tabla.2: Esquema de Chen y Wu para 2 imágenes compartidas

### Ventana de Cifrado



### Ventana de descifrado

