

| |
|---|
| <p>Prototipo criptográfico basado en el protocolo de compartición y distribución de secretos y las funciones unidireccionales hash para la generación de claves y cifrado.</p> |
|---|

Manual de uso básico de la aplicación.

Rol Distribuidor



Bienvenid@, te presentamos nuestro Manual de uso básico de la aplicación.

El prototipo criptográfico basado en el protocolo de compartición y distribución de secretos y las funciones unidireccionales hash para la generación de claves y cifrado es una innovadora plataforma diseñada para ofrecer una experiencia única y enriquecedora a sus usuarios.

La plataforma esta basada en el protocolo de compartición y distribución de secretos (k, n) -umbral y las funciones unidireccionales HASH de manera que, se consiga implementar un sistema para cifrar información conservando las características de confiabilidad, integridad y no repudio, robusteciendo su seguridad mediante la generación de contraseñas de acceso únicas, propendiendo así a la protección de la información a transmitir por canales convencionales no seguros.

| | |
|---|----------------------|
| 0 | Índice de contenidos |
|---|----------------------|

1. Interfaz de la aplicación

- 1.1 Pantalla principal
- 1.2 Principales funciones de la interfaz
 - 1.2.1 Distribuidor

2 . Prueba de escritorio

- 2.1 Resultados rol Distribuidor

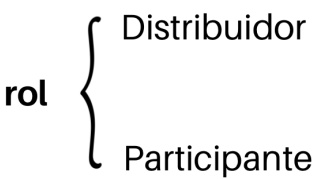
| | |
|---|---------------------------|
| 1 | Interfaz de la aplicación |
|---|---------------------------|

La interfaz que encontrara al ingresar al aplicativo es responsive con el dispositivo de visualización, esto significa que el sitio web es accesible y adaptable en todos los dispositivos: tabletas, smartphones, etc.

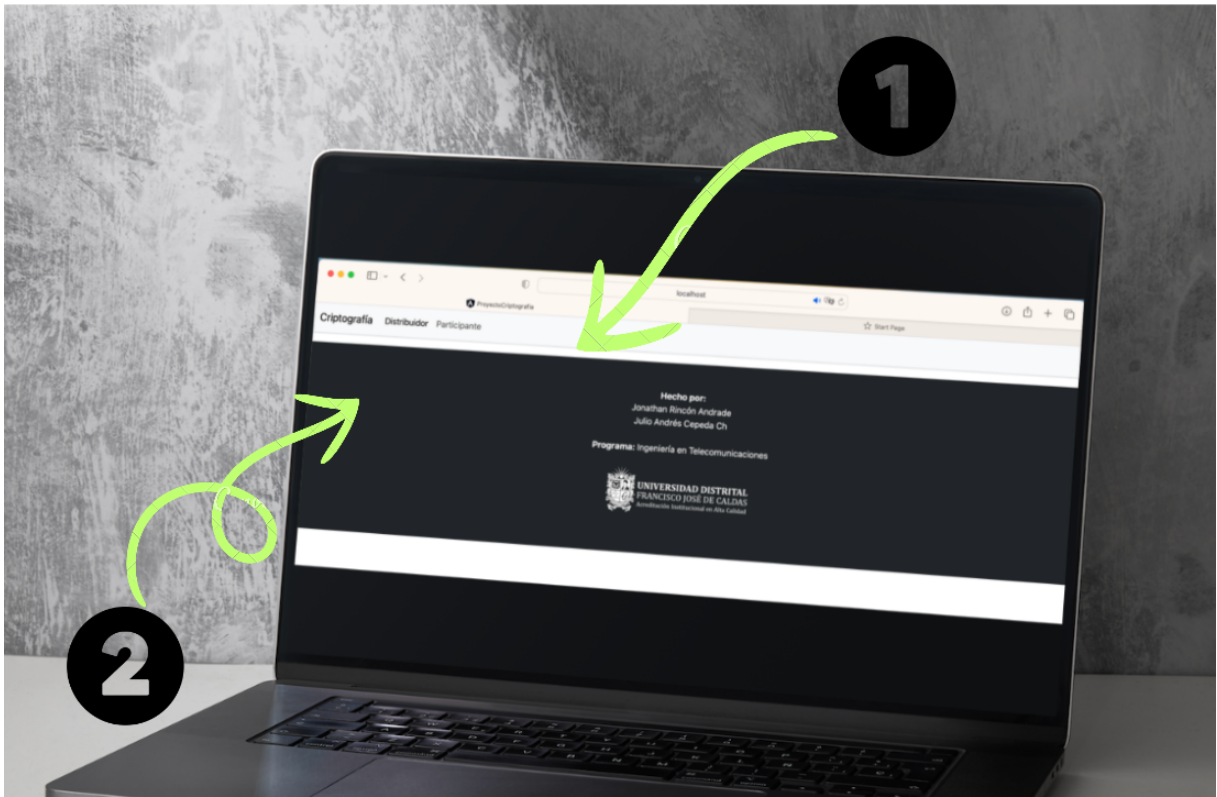
1.1 Pantalla principal

En la pantalla principal podrá gestionar que acción desea realizar. Para ello debe identificar:

1 . Barra de navegación: le permite seleccionar el rol a desempeñar.



2 . Banner principal: le permite visualizar información de los creadores de la aplicación.





1.2 Principales funciones de la interfaz

Al seleccionar un rol en la barra de navegación, usted sera direccionado a una pantalla diferente.

Nota: Considere y tenga en cuenta que cada rol ejecutara acciones independientes.

1.2.1 Distribuidor

La interfaz que encontrara en el rol “Distribuidor” tiene como objetivo generar claves seguras. Se compone de cuatro secciones: Generación de Claves, Generación de Sombras, Cifrado y Ayuda.

Generación de Claves

Generación de Sombras

Cifrado

Ayuda

A continuación se explican los componentes y funcionalidad de cada sección.

☐ **Sección: Generación de Claves**

Generación de Claves

Generación de Sombras

Cifrado

Ayuda

Elegir secreto (Zp)

1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359,

SS esquema umbral (k=3, n=5)

[C] 0

CARGAR

Enmascarado 1

0

Enmascarado 2

0

DESCARGAR [C]

GENERAR CLAVES

☐ Cargar claves

CLAVE 1 [SHA(2)-256]

aquí va clave 1

CLAVE 2 [SHA(2)-256]

aquí va clave 2

Favor utilizar claves para proteger archivo

Desde “Generación de Claves” vamos a poder configurar las opciones básicas de este rol como pueden ser: seleccionar un valor secreto para la variable “c” y generar 2 claves seguras diseñadas con la función SHA-2.

- La primera acción que debe realizar es elegir un secreto. Desde la caja que se encuentra en el panel izquierdo de la interfaz podrá navegar y seleccionar un valor dando click, automáticamente el valor se cargara en el campo [C].

Elegir secreto (Zp)

1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359,

- Posteriormente debe dar click al botón “CARGAR”.

SS esquema umbral (k=3, n=5)

[C] 151

CARGAR

Se cargaran los valores correspondientes a “Enmascarado 1” y “Enmascarado 2”.

Enmascarado 1


29516614416


Enmascarado 2

984327876

DESCARGAR [C]

- Al dar click en el botón “DESCARGAR [C]” obtendrá un archivo de tipo plano .txt que podrá conservar en su ordenador.

 Valor_C.txt
3 bytes



- Finalmente, al dar click en el botón “GENERAR CLAVES” se ejecutara la función SHA-2 con los valores cargados previamente en “Enmascarado 1” y “Enmascarado 2”.

CLAVE 1 [SHA(2)-256]

b44a30f970ee81996815ac2aa387f858c3b961b557e69562f5da2d606f8317c8

CLAVE 2 [SHA(2)-256]

96895b59700775107e186deb1802b320937da51a1a8625bb49150349e208cb69

Favor utilizar claves para proteger archivo

Sección: Generación de Sombras

ProyectoCriptografia

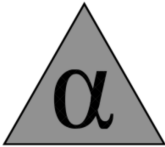
Start Page

Generación de Claves

Generación de Sombras

Cifrado

Generación, Distribución Sombras



polinomio

[f1]^k


polinomio^K



polinomio

[f2]^k

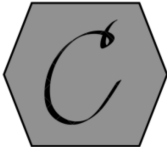
polinomio^K



polinomio

[f3]^k

polinomio^K



polinomio

[f4]^k

polinomio^K



polinomio

[f5]^k

polinomio^K

PUBLICAR

IMPRIMIR

Desde la sección “Generación de Sombras”, al dar click en “CARGAR” podrá evaluar a un polinomio $f(n)$ con 5 valores, donde, cada valor se encuentra representado por una figura geométrica y por medio del botón “IMPRIMIR” va a importar 5 valores $[fn]^k$ diferentes.

Sección: Cifrado

ProyectoCriptografia

Start Page

Generación de Claves

Generación de Sombras

Cifrado

Cifrado y protección de archivo

Mensaje

Aquí puede escribir su mensaje

CIFRAR

Mensaje cifrado

Mensaje cifrado

EXPORTAR

NOTA: Proteger el archivo cifrado con las claves para GENERACIÓN DE CLAVES

Desde la sección “Cifrado” podrá ingresar el mensaje que desea cifrar. Por medio del botón “CIFRAR” el mensaje ingresado en la caja “Mensaje” sera cifrado y el resultado se visualizara en la caja “Mensaje cifrado” y finalmente, con el botón “EXPORTAR” podrá generar un archivo de texto plano que contiene el mensaje cifrado.

Sección: Ayuda

Desde la sección “Ayuda” podrá consultar el manual de uso básico de la aplica

2

Prueba de escritorio

A continuación se presentan los resultados después de generar una prueba aleatoria con la aplicación.

Resultados en el rol Distribuidor

Sección: Generación de Claves

Criptografía

Distribuidor

Participante

Generación de Claves

Generación de Sombras

Cifrado

Ayuda

Elegir secreto (Zp)

SS esquema umbral (k=3, n=5)

927431, 927439, 927491, 927497, 927517, 927529, 927533, 927541, 927557, 927569, 927587, 927629, 927631, 927643, 927649, 927653, 927671, 927677, 927683, 927709, 927727, 927743, 927763, 927769, 927779, 927791, 927803, 927821, 927833, 927841, 927847, 927853, 927863, 927869, 927961, 927967, 927973, 928001, 928043, 928051,

[C] 928043

CARGAR

Enmascarado 1

942169187716

Enmascarado 2

1011557200644

DESCARGAR [C]

GENERAR CLAVES

Cargar claves

CLAVE 1 [SHA(2)-256]

12415d5d92503225ab39c1d2c003d9a1dea28053ce3d875d2add870a9f100448

CLAVE 2 [SHA(2)-256]

e1261afe1fdcc05b66f8b1da4c39dfdb488d79f32e4958310244ff09ed69d0bb

Favor utilizar claves para proteger archivo

Sección: Generación de Sombras

Criptografía

Distribuidor

Participante

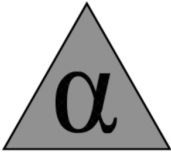
Generación de Claves

Generación de Sombras

Cifrado

Ayuda


Generación, Distribución Sombras



1048373

[f1]^k


1152252031649471100



1253925

[f2]^k

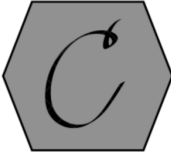
1971581269060828200



1544699

[f3]^k


3685798561333364000



1920695

[f4]^k

7085576926559702000



2381913

[f5]^k

13513806127923415000

PUBLICAR

IMPRIMIR

Sección: Cifrado

Cifrado y protección de archivo

Mensaje

test para el manual de uso basico de la aplicacion

CIFRAR

Mensaje cifrado

YJXYEUFWFEJPEQFRZFPPEJJEZXTEGFXNHTEJEPFEFUPNHFHN

EXPORTAR

NOTA: Proteger el archivo cifrado con las claves para GENERACIÓN DE CLAVES