

<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 Participante



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.

1. Interfaz de la aplicación

1.1 Pantalla principal

1.2 Principales funciones de la interfaz

1.2.2 Participante

2 . Prueba de escritorio

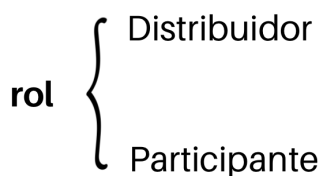
2.2 Resultados rol Participante

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.

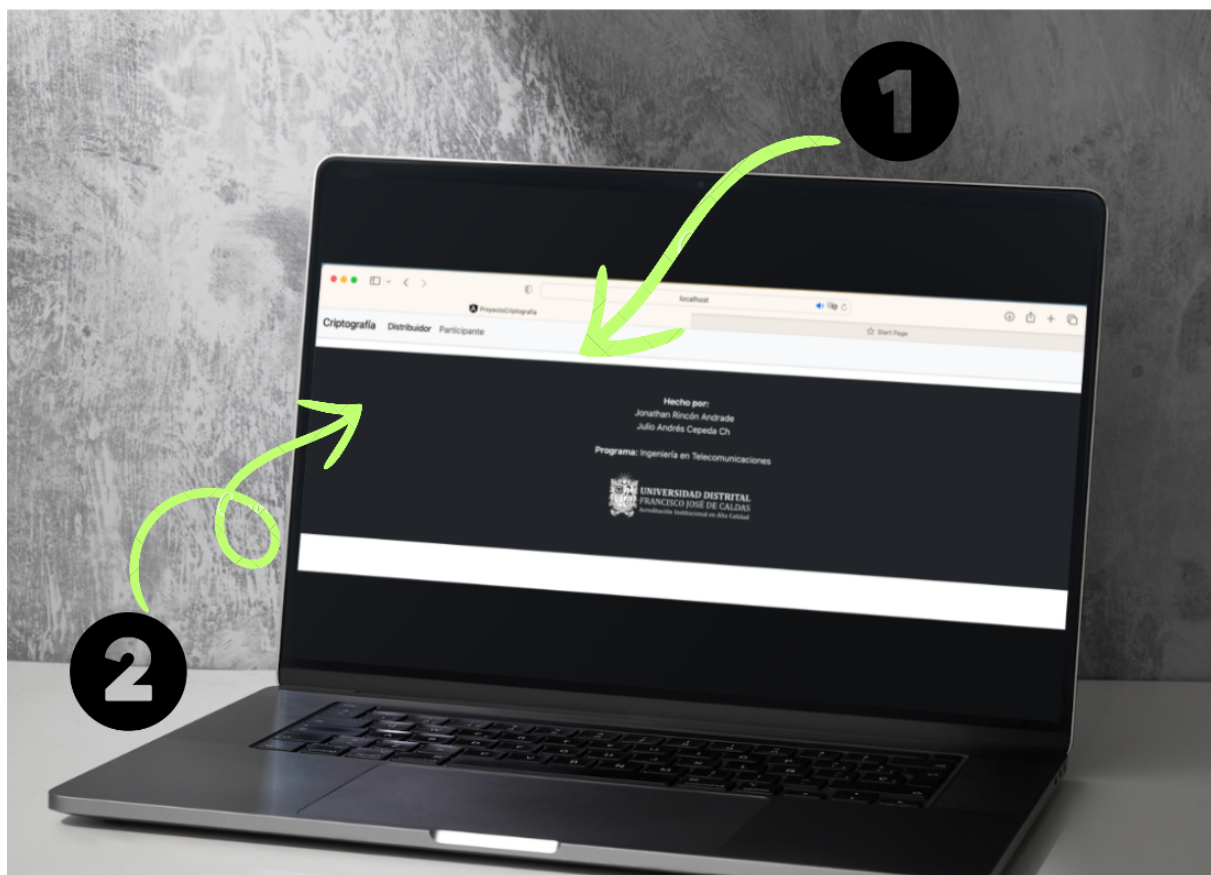
1.1 Pantalla principal

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.

1.2.2 Participante

La interfaz que encontrara en el rol "Participante" tiene como objetivo recuperar claves cifradas con anterioridad en la interfaz del "Distribuidor". Se compone de tres secciones: Recuperación de Claves, Descifrado y Ayuda.

Recuperación de Claves

Descifrado

Ayuda

☐ Sección: Recuperación de Claves

ProyectoCriptografia

Start Page

Criptografía


Distribuidor

Participante

Recuperación de Claves


Descifrado

Ayuda




{}^k

polinomio




{}^k

polinomio




{}^k

polinomio



{}^k

polinomio



{}^k

polinomio

Recuperar Secreto [C]

aqui se recupera c

0

Recuperar claves de acceso

Clave 1 [SHA(2)-256]

Clave 2 [SHA(2)-256]

Nota: favor utilizar claves para apertura del archivo.

Desde la sección "Recuperación de Claves", podrá ingresar como mínimo 3 valores correspondientes a la evaluación de un polinomio $f(n)$. Al dar click en "Recuperar Secreto [C]" se recuperara el valor de c y al oprimir "Recuperar claves de acceso" se generaran dos claves por medio de la función SHA-2 .

☐ Sección: Descifrado

Recuperación de Claves

Descifrado

Ayuda

Decifrado del mensaje

Mensaje cifrado

Aquí puede escribir su mensaje cifrado

DESCIFRAR

Mensaje Original

Mensaje original

EXPORTAR

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

☐ Sección: Ayuda

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

2	Prueba de escritorio
---	----------------------

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

Resultados rol Participante

☐ Sección: Recuperación de Claves

Criptografía


Distribuidor

Participante

Recuperación de Claves


Descifrado

Ayuda




α

1152252031649471100



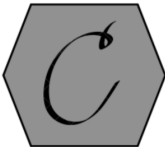
φ

1971581269060828200




Φ

3685798561333364000



C

polinomio



Ω

polinomio

Recuperar Secreto [C]

aqui se recupera c

928043

Recuperar claves de acceso

Clave 1 [SHA(2)-256]

12415d5d92503225ab39c1d2c003d9a1dea28053ce3d875d2add870a9f100448

Clave 2 [SHA(2)-256]

e1261afe1fdcc05b66f8b1da4c39dfdb488d79f32e4958310244ff09ed69d0bb

Nota: favor utilizar claves para apertura del archivo.

Sección: Descifrado

Decifrado del mensaje

Mensaje cifrado

YJXYEUFWFEJPEQFRZFPEIJEZXTEGFXNHTEIJEPPFEFUPNHFHN

DECIFRAR

Mensaje Original

TEST PARA EL MANUAL DE USO BASICO DE LA APLICACION

EXPORTAR