



Criptografía

MANUAL DEL USUARIO

2019

Chávez, Luis
Flores, Nestor
Juarez, Evert

Índice

Introducción	3
Contenido	5
Conociendo la aplicación.....	6
Interfaz del sistema	6
Dentro del programa.....	7
Configuraciones	7
Keystore	10
Certificados digitales	12
Cifrado Asimétrico	15
Cifrando y descifrando.....	16
Cifrado Asimétrico.....	16
Cifrando (RSA)	16
Descifrando (RSA).....	17
Cifrado simétrico	18
• AES	18
• DES	18
• Modo ECB	18
• Modo CBC	19
• Modo CFB	19
• Modo OFB	19
Cifrando y descifrando.....	19
Cifrado simétrico	19
• AES	19
• DES	23

Introducción

El cifrado es un método que desde tiempos antiguos se ocupa para ocultar un mensaje, con el fin de evitar que un tercero no deseado conozca el contenido de este, podemos hablar de diferentes métodos con los cuales nuestros antepasados lograron con éxito esta tarea, en la actualidad para evitar que alguien pueda tener acceso a nuestra información, datos u otro tipo de contenido sensible es necesario la preservación de un nivel alto de seguridad. Este método consiste en alterar un mensaje antes de enviarlo, generalmente mediante una clave, quienes no tengan esta llave, el mensaje no será legible.

Con la aplicación se pretende tener una herramienta que facilite esta tarea, no solamente implementar un cifrado predeterminado que una herramienta online en internet sin certificado de seguridad pueda ofrecer o los algoritmos utilizados no son los adecuados o están previamente vulnerados, siendo lo esencial que la herramienta cumpla con los estándares de seguridad requeridos por el usuario.

No es solo necesario cifrar, sino hacerlo de manera que la información sea inteligible y no manipulada por otros, la última condición es esencial en la herramienta, puesto que sin esta, el cifrado no tendría valor alguno y lo único que generarían sería caracteres y números al azar, esto implica que el sistema esté comprometido, que no se conozca forma de romperlo, usamos mecanismos de cifrado robusto, siendo estos actualizados y monitoreados de forma dinámica, muchos mecanismos pueden ser robustos y tener aspecto seguro para el usuario en este momento, pero en cualquier segundo, instante o minuto este mecanismo ya ha sido vulnerado.

Además, en El Salvador la firma electrónica y certificados digitales es una propuesta que se mantiene en cajón, con la herramienta se pretende sentar los primeros indicios y bases, siendo el desarrollo de la aplicación un avance en

materia tecnológica para El Salvador. Ayudará a la integridad, confidencialidad y no repudio de la información

El Manual describe cómo funciona la aplicación CRIPTO SYSTEM 1.0, utilizando el framework JavaFX, la cual, consiste en la implementación de algoritmos de cifrado simétrico, asimétrico y firmas digitales, con el objetivo de cifrar/descifrar/firmar/verificar mensajes mediante la utilización de las diferentes funciones del sistema.

La aplicación cuenta además, con la función de criptoanálisis de frecuencia de mensajes cifrados, utilizando el alfabeto español, con el propósito de verificar la frecuencia de letras o grupo de letras para que el usuario formule sus hipótesis y le ayude a descifrar el texto cifrado.

Contenido

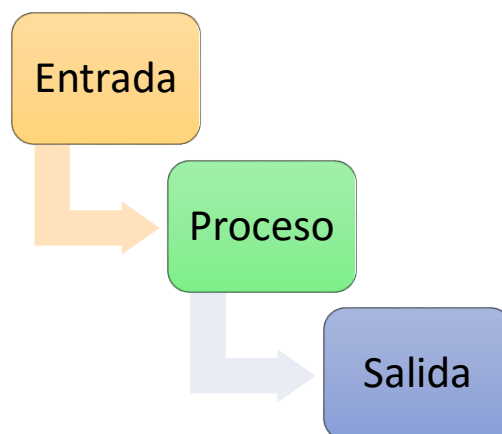
Para poder utilizar la aplicación se debe instalar en el equipo la JRE de Java, el cual puede realizarse desde la página web oficial de Java¹, ya que es una aplicación con carácter freeware y está disponible para sistemas operativos Windows, Mac, GNU/Linux y Solaris.

La licencia utilizada para el programa es GNU (General Public License v3.0) es decir que, es una aplicación en la cual se garantiza a los usuarios la libertad de usar, estudiar, compartir y modificar la aplicación.

CRIPTO SYSTEM 1.0 está diseñado para poder cifrar, descifrar, firmar y verificar mensajes de una forma rápida y segura con diferentes tipos de algoritmos, además habilita las firmas digitales para poder firmar mensajes. La aplicación depende de una carpeta recursos para poder funcionar, ya que es ahí donde se almacenan los certificados.

Para el módulo de firmas digitales, la aplicación generará certificados digitales para firmar/verificar mensajes, mediante el uso de digestos SHA-3 (512 bits), y de los algoritmo RSA/ECB.

Para los usuarios que desconocen de informática pero están preocupados por su seguridad, se debe tener en claro que todo programa informático funciona de la siguiente manera:



En los próximos apartados se abordará cada una de las partes de la aplicación, la entrada, el proceso y la salida de la información de CRIPTO SYSTEM 1.0.

¹ <https://www.java.com/es/download/>

Conociendo la aplicación

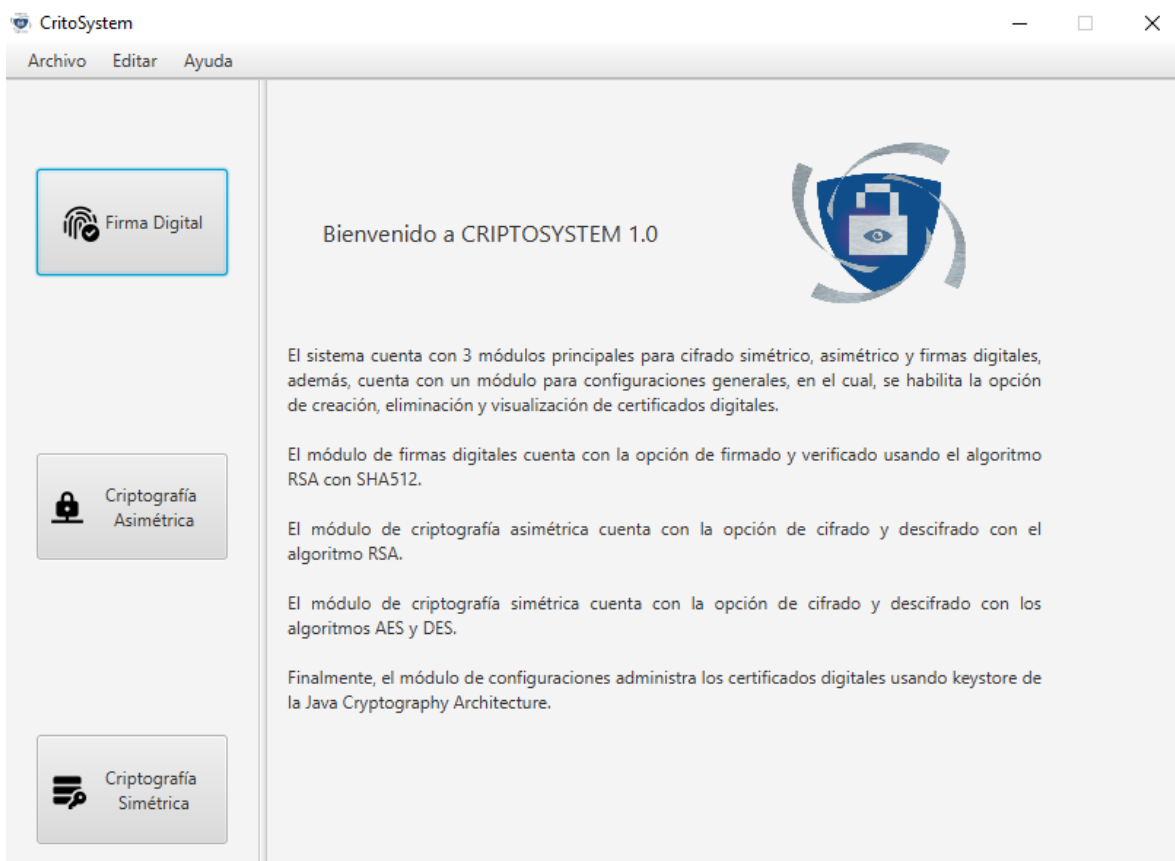
Para abrir el programa, el usuario debe de dar doble clic en el icono de CRIPTO

SYSTEM 1.0

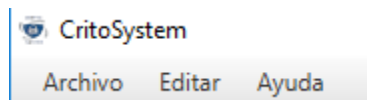


Interfaz del sistema

Cryptosystem cuenta con una pantalla de inicio minimalista y fácil de entender, de rápida orientación para el usuario, explicando los algoritmos que se pueden utilizar para cifrar, hasta el apartado de firma digital. Brindando opciones en criptografía entre, cifrado simétrico y asimétrico.

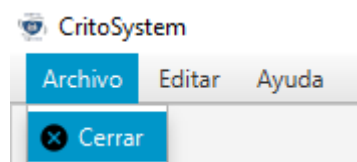


Dentro del programa



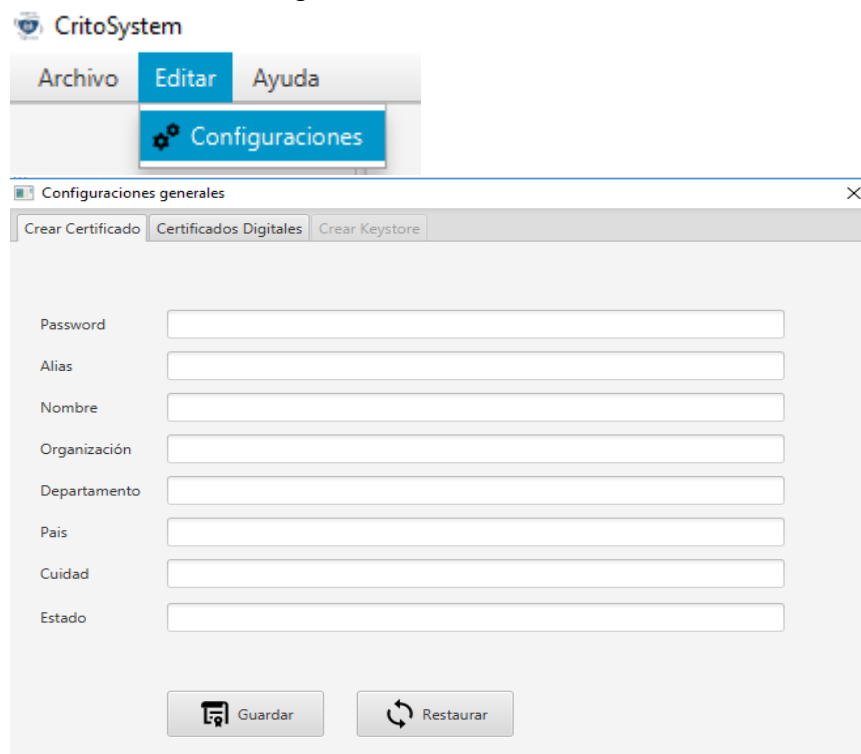
En la aplicación, se puede usar de la siguiente manera:

- Pestaña de archivo, cierra el programa

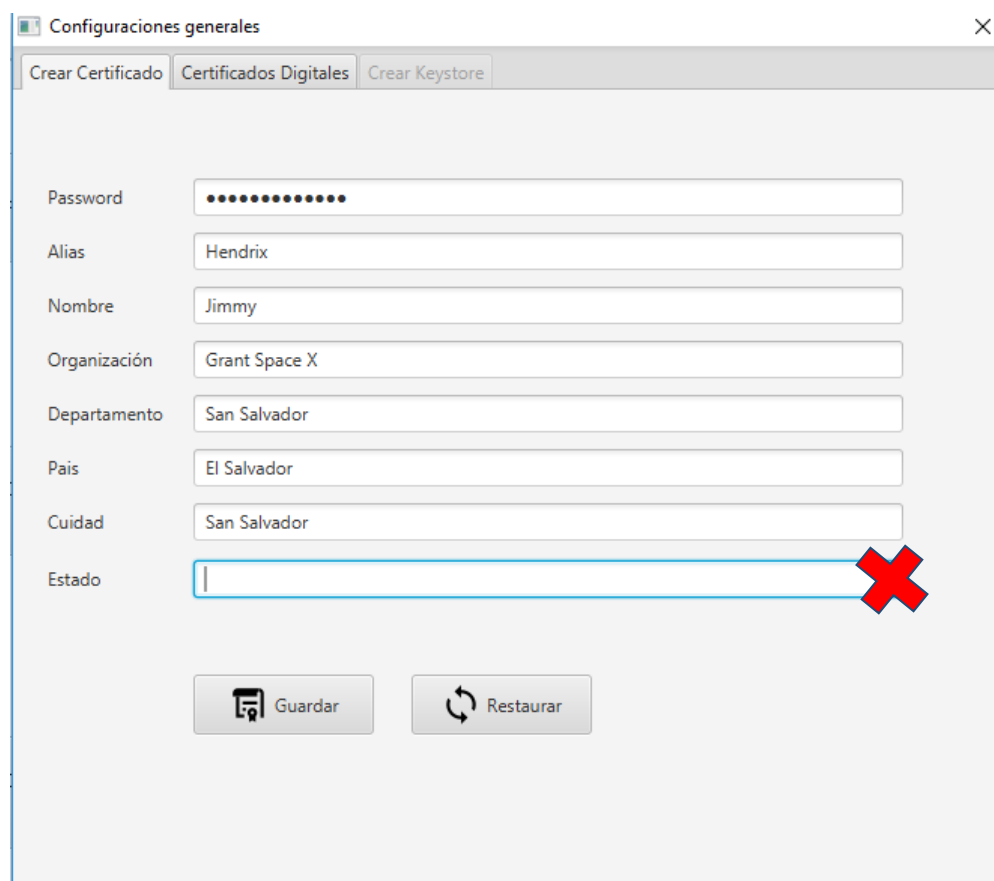


Configuraciones

- Editar, proporcionar la configuración y **creación de certificados digitales** y entre estas configuraciones existe la posibilidad de crear y gestionar certificados, de la siguiente manera.



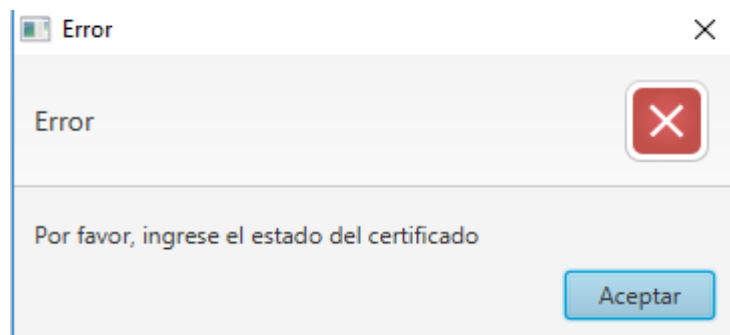
Para la creación de certificados digitales se debe rellenar cada uno de los campos, dicho paso es obligatorio, la aplicación no permite la creación de un certificado si queda un campo en blanco. Para la creación es necesario utilizar un password el cual debe contener (con 13 caracteres mínimos, mayúsculas, minúsculas, cifras y caracteres especiales, para tener una contraseña segura) un alias, nombre, organización (Educativa, Investigación o sitio de trabajo, dependiendo el uso que le dará a la aplicación), departamento (Dónde se encuentra dicha organización), país, ciudad y estado (dependiendo el país de procedencia del usuario que use la aplicación, este campo puede ser una provincia también).



The screenshot shows a window titled 'Configuraciones generales' with three tabs: 'Crear Certificado', 'Certificados Digitales', and 'Crear Keystore'. The 'Certificados Digitales' tab is active. The form contains the following fields:

- Password: A text box with 13 dots, indicating a masked password.
- Alias: A text box containing 'Hendrix'.
- Nombre: A text box containing 'Jimmy'.
- Organización: A text box containing 'Grant Space X'.
- Departamento: A text box containing 'San Salvador'.
- Pais: A text box containing 'El Salvador'.
- Cuidad: A text box containing 'San Salvador'.
- Estado: An empty text box, highlighted with a red X, indicating it is a required field.

At the bottom of the form are two buttons: 'Guardar' (with a save icon) and 'Restaurar' (with a refresh icon).



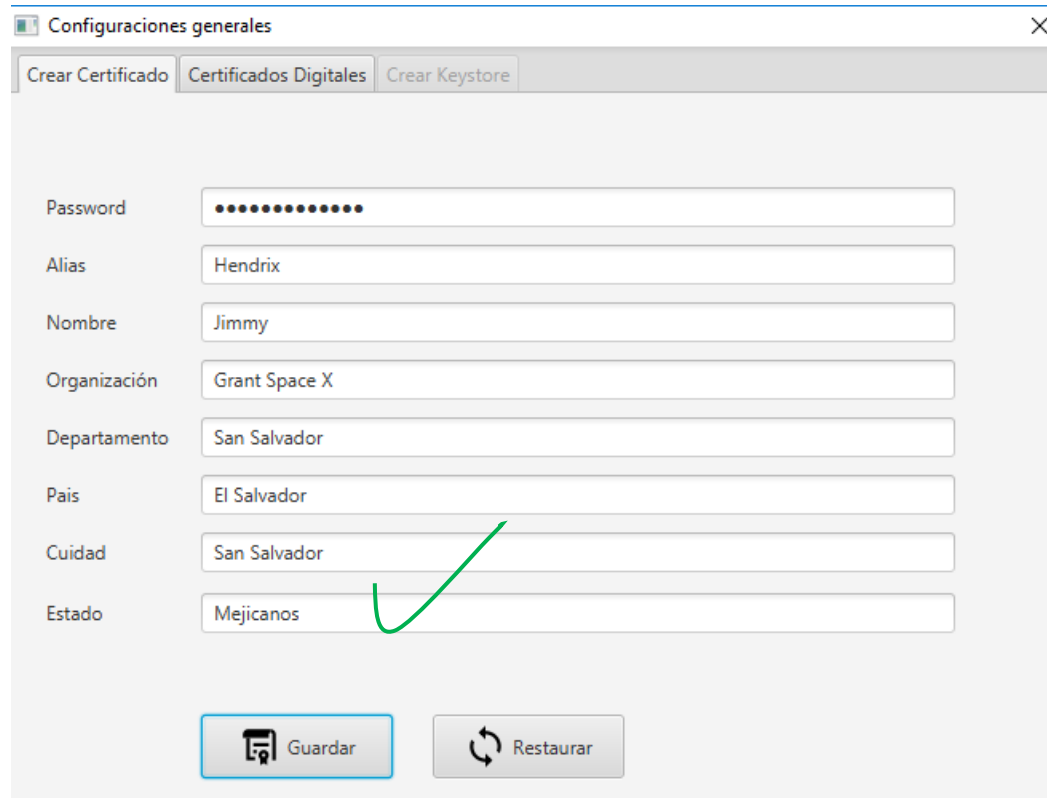
The screenshot shows an 'Error' dialog box with a red 'X' icon in the top right corner. The text inside the dialog reads:

Error

Por favor, ingrese el estado del certificado

At the bottom right of the dialog is a blue button labeled 'Aceptar'.

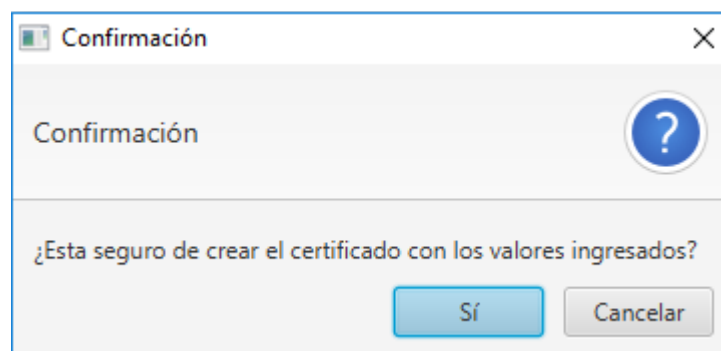
Una vez completos los campos, la aplicación crea el certificado digital



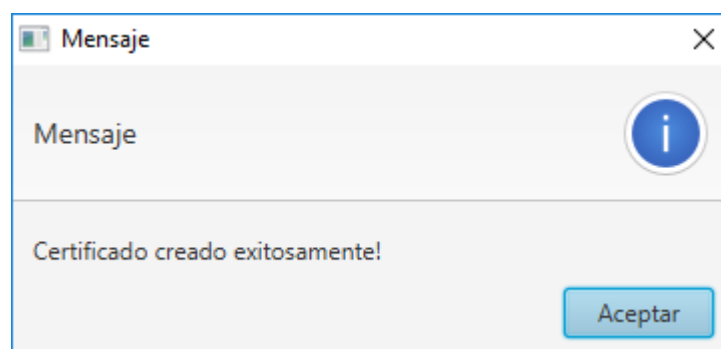
The 'Configuraciones generales' dialog box contains the following fields and values:

Field	Value
Password	••••••••••
Alias	Hendrix
Nombre	Jimmy
Organización	Grant Space X
Departamento	San Salvador
Pais	El Salvador
Cuidad	San Salvador
Estado	Mejicanos

At the bottom, there are two buttons: 'Guardar' (with a floppy disk icon) and 'Restaurar' (with a circular arrow icon).



The 'Confirmación' dialog box displays a question mark icon and the text: '¿Esta seguro de crear el certificado con los valores ingresados?'. It includes two buttons: 'Sí' and 'Cancelar'.



The 'Mensaje' dialog box displays an information icon and the text: 'Certificado creado exitosamente!'. It includes a single button: 'Aceptar'.

Inicialmente, los certificados se guardan en un almacén con su clave privada. En la pestaña de certificados digitales, se pueden consultar los usuarios y sus certificados creados en formato X509, los certificados pueden ser eliminados si así lo desea el usuario.

Configuraciones generales

Crear Certificado | Certificados Digitales | Crear Keystore

Ver | Eliminar

Número	Alias	Nombre	Organización	Unidad
1	hendrix	Jimmy	San Salvador	Grant Space X
2	mario cruz	Mario Cruz	BANDESAL	IT
3	nestor flores	Nestor Flores	Grant Thronton El Salvador	IT
4	evert juarez	Evert Juárez	CLARO	IT
5	luis chavez	Luis Chávez	BANDESAL	IT

Para fines académicos el proceso que se utilizó para la creación de un certificado es el autofirmado. El nivel de seguridad que ocupan los certificados digitales es el uso de digestos SHA-3 (512) y el algoritmo RSA/ECB.

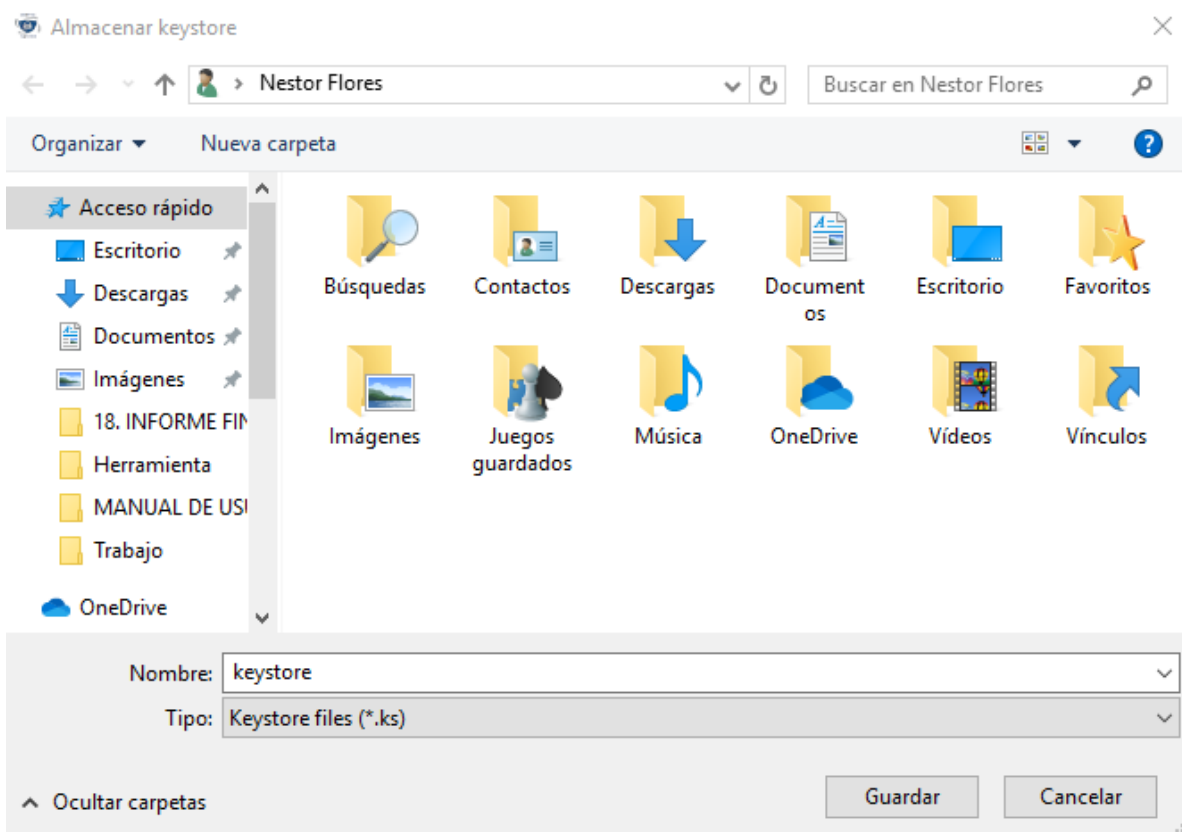
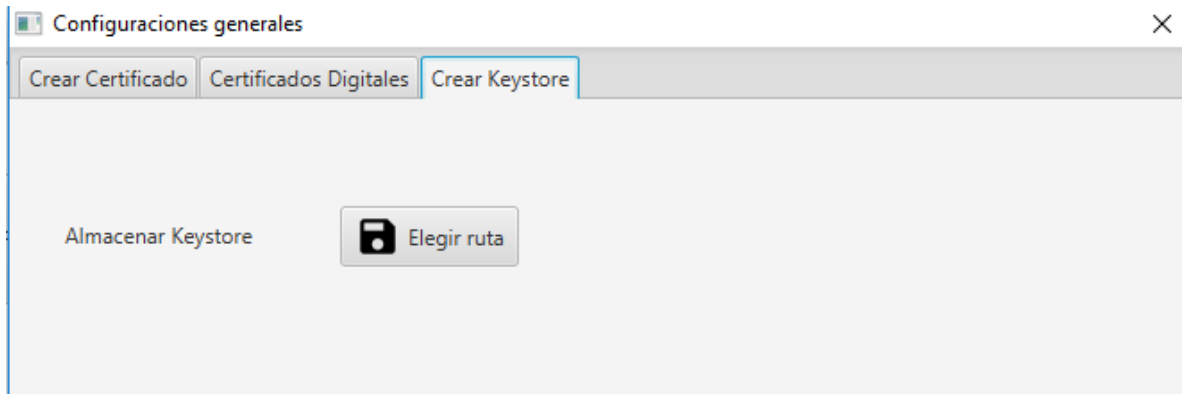
Información de certificado

Certificado	<pre>[[Version: V3 Subject: CN=Jimmy, OU=Grant Space X, O=San Salvador, L=San Salvador, ST=Mejicanos, C=El Salvador Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13 Key: Sun RSA public key, 4096 bits modulus: 76153571999487034779855636545969327774614639757408046486565375052 09007727782346145515491389089554035845518843376505688061591815502 30396297934701846724687115921382080908559249334894671675326213241 64643518542277810040952178741612952714048592480622742265379018195 76220119613230243129820899226707167344932677673673943330140736971 03445293500585058301906027821897589426639540536071909588080179566 01202675242105107227508268254701080808022668127071702661561858166</pre>
-------------	--

Keystore

La aplicación permite guardar un archivo keystore.ks, el cual consiste en un repositorio para almacenar certificados digitales mediante una contraseña, cada certificado posee una contraseña, con el fin de acceder a la clave pública y privada del mismo. Dichas claves (pública y privada) sirven para

cifrar, descifrar, firmar y verificar mensajes. Sin dicho almacén o keystore, la aplicación no funciona. Puesto que maneja los certificados creados con el algoritmo RSA de 4096 bits.



Certificados digitales

Una vez realizado este paso se pueden firmar mensajes con el certificado digital, al firmarlo, se obtiene el digesto y el mensaje a transmitir para que la otra persona, pueda verificarlo.

Firma digital

Firmar mensajes

Verificar mensajes

Mensaje

Hola, este es un mensaje de prueba

Certificado

hendrix

Passphrase

.....

Firmar

Restaurar

Digesto

c572dd5617af96df2456f47f78fe9cf83f7999d5971ed969d276cbfc63f663d9ac62bc04f8770c1b35e19888d7044d854214bc967c67685724ed566c15e663

Certificado

[
Version: V3
Subject: CN=Jimmy, OU=Grant Space X, O=San Salvado, L=San Salvador, ST=Mejicanos, C=El Salvador
Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

Key: Sun RSA public key, 4096 bits
modulus:

fAFC2bCzDSXkonKTSSF1/Ae7xLcIK3U06Gnnueslxhu1hCO8BV3cc7Q9mryprvQWwhLp52AD
WafYF9AkwwTUz6d1Tan6XCRrRN2k4T24jxu6snlNB/n+aye5kT1650PbvzdpOrBHZ+2umd
uASQGSmlE6tCRGzUh91TJeHCok8vkcSuCVhR5ew8Im8MN7kDTml/gQfuJpWTo6rN4IUriv
0j2oQXFy8nHGyDoAsiQn1SSuPOxQyhHGzNh7S0KV3ax+fdeMLnLrAABgwpRF1Islb3rtsBuh
AdqTbWq3SQPVjoh31860K71LR55PHr9ZWaOXDNxMxO+H0PJHcHnDCfH+nAAgH2RcO
WYIDeLgcJa9tADjmVV0XoMfTyHnImtFW+oVeGX6en94+oONSELwym9T/NKtqq12OJ78Lr
WYUaKfOBWOXM9Pc7mm4PN44CqLNeGw4xYM40QDEeymxRwvrlXp1AHUyfkBeRsDNzn
SG9sYSwgZXN0ZSB1cyB1biBtZW5zYWwplIGRIIHBydWVlYV9mQUZDMmJDeKRTWgtvbkU
1NGMS9BZTd4TGNJSzNVMDZHbm51ZXNseGh1MWhtDTzhCVjNjYzdROW1yeXBldlFXaGh
McDUyQURXYWZZRjB3d3VfV6NmQxVGfuNihDUjSTmcyazRUmJRqH2c25sTkIvbithe
WU1a1QxNjUwUGJ2emRwT3JCSForMnVtZHVBU1FHU21MRTZOQ1JHelVoOTFUSmVIQ29r
OHZreFN1Q1ZoUjVldzhjbThNTjdrFRtSS9nUWZ1SnBXVG82ck40bFVSaXYwajVUvHGeThu
SEd5RG9Bc2lRbjFTU3VQT3hReWhtIR3pOaDdTMETmWM2F4K2ZkZU1MbKxyQUFCZ3dwUkYx
SXNJYjNydhNCdWb3ZHFUyYldXM1NRUFZqb0loMzE4NjBlnZFMUjU1UEhyOVpXYU9YRE54

Firma digital

Mensaje a transmitir

El usuario puede verificar mensajes a partir de los certificados digitales creados, dentro de la aplicación se pega en el recuadro el mensaje a verificar (previamente generado) se selecciona el certificado digital con el cual se verificará, este paso da como resultado el mensaje original.

Firma digital

Firmar mensajes

Verificar mensajes

Mensaje a verificar

dTMEtWM2F4K2ZkZU1MbKxyQUFCZ3dwUkYxSXNJYjNydHNCdWhBZ
HFUYldxM1NRUFZqb0IoMzE4NjBLNzFMUjU1UEhyOVpXYU9YRE54TXh
PK0gwUEplY0huRENmSCtuQUFnSDJSY09XWWxEZUxnY0phOXRBGRpt
VIYwWG9NRnR5SG5sbXRGVyVtVmVHWDZlbjK0K29PTINFTHd5bTIUL0
5LdHFxMTJP5jc4THJXWXVBa0ZPQldPWE05UGM3bW00UE40NENxTESI
R3c0eFINNDBRREVIeW14Und2cklYcDFB5FV5ZmtCZVJzRE56bjVpSFhzb
114cmxpNH83Wlg3QmRyckg0cFBrSUZRYXo3R3cyQXRaNWZNNUM2Z
DE0L0hpOWtIOEV3RXJldEZUT0d1Z0dJbmVwUW92aFNja3BPRk5sczRR
djNqR2xuVUV2aEx4STdOQ1c0UHR1U1NJMUNCN3haWVNIVkhYdHR5
cDUyZHIHN3BFQXpEY0F3cnE0U24wd25zRndEaHE3NVAXY2dIYUdjJR
VTU5VVzNFcXRXZDB4UjRVYzF6SDVianRIQkpqNXZLVTO=

Certificado

hendrix

Verificar

Restaurar

Certificado

[
[
Version: V3
Subject: CN=Jimmy, OU=Grant Space X, O=San Salvador, L=San Salvador, ST=Mejicanos,
C=El Salvador
Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

Key: Sun RSA public key, 4096 bits
modulus:

Sun RSA public key, 4096 bits
modulus:
761535719994870347798556365459693277746146397574080464865637505209007727
7823461455154913890895540358455188433765056880615918155023039629793470184
6724687115921382080908559249334894671675326213241646435185422778100409521

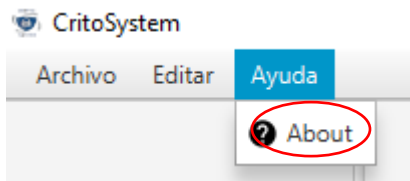
fAFC2bCzDSXkonKTSSF1/Ae7xLclK3U06Gnnueslxhu1hCO8BV3cc7Q9mryprvQWhhLp52AD
WafYF9AkwwTUz6d1Tan6XCRrRNg2k4T24jxu6snlNB/n+aye5kT1650PbvzdpOrBHZ+2umd
uASQGSmlE6tCRGzUh91TJeHCok8vKxSuCVhR5ew8Im8MN7kDTml/gQfujpWto6rN4IUriv
Oj2oQXFy8nHGyDoAsiQn1SSuPOxQyhHGzNh7S0KV3ax+fdeMLnLrAABgwpRF1slb3rtsBuh
AdqTbWq3SQPVjoh31860K71LR55PHr9ZWaOXDNxMxO+H0PJHcHnDCfH+nAAgH2RcO
WYIDeLgcJa9tADjmVV0XoMFtyHnImtFW+oVeGX6en94+oONSELwym9T/NKtqq12OJ78Lr
WYUakFOBWOXM9Pc7mm4PN44CqLNeGw4xYM40QDEeymxRwvrlXp1AHUyfkBeRsDNzn
5iHXcR8RliAawZY7BdrH4nPhlEQaz7Gu2At75fM5C6d1A/Hi9ka8FwErHtETOgugGln/Oov

Firma digital

Mensaje original

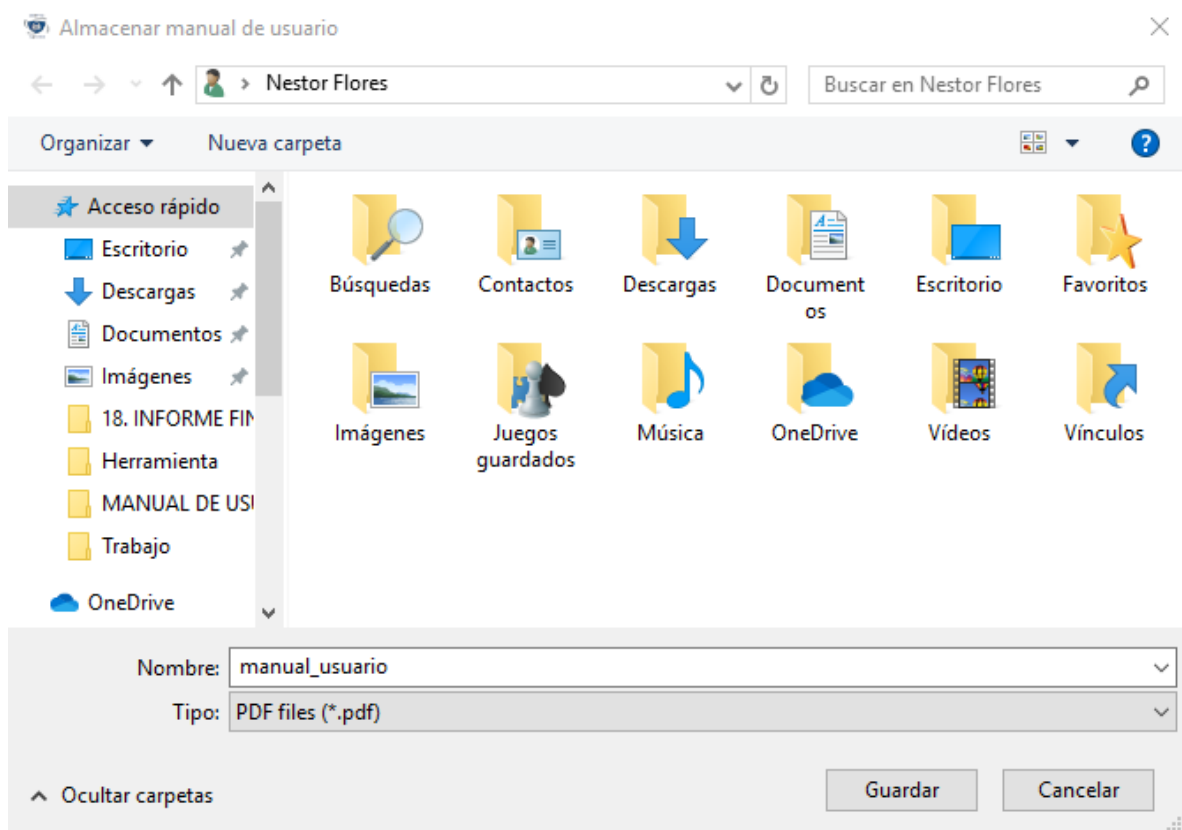
Hola, este es un mensaje de prueba

- Pestaña, ayuda, se encuentra el manual del usuario, licencia de la aplicación así como los involucrados en el proyecto.



El manual del usuario puede descargarse dando clic en el apartado “descargar manual” este contiene paso a paso la forma de ocupar la aplicación CRIPTO SYSTEM 1.0.





Cifrado Asimétrico

- RSA

Las claves RSA pueden cifrar todo el documento y la firma de archivo, mientras que una DSA solo se usa para firmar documentos. La RSA permite a los usuarios generar pares de claves cuyos tamaños son mayores de 1024 bits (la aplicación utiliza un tamaño de 4096 bits). RSA es un algoritmo de cifrado asimétrico, o de clave pública, y es uno de los algoritmos más utilizados en la actualidad. La mayor parte de los sitios hoy corren sobre SSL/TLS, y permiten la autenticación mediante cifrado asimétrico basado en RSA.

Cifrando y descifrando

Cifrado Asimétrico

Cifrando (RSA)

Utilizando el algoritmo de RSA, se debe elegir el certificado con el cual se desea firmar el texto cifrado, se redacta el mensaje a cifrar y se procede a dar clic en la opción de cifrar, realizado esto, se obtiene el certificado, la llave pública y el texto cifrado.

The screenshot shows a web application titled "Cifrado asimétrico" with three tabs: "Cifrar mensajes", "Descifrar mensajes", and "Criptoanalizar RSA". The "Cifrar mensajes" tab is active.

Mensaje a cifrar: A text area containing "Hola, este es un mensaje de prueba." is highlighted with a red border.

Certificado: A dropdown menu shows "hendrix".

Buttons: "Cifrar" (with a lock icon) and "Restaurar" (with a refresh icon).

Results:

- Certificado:**

```
[
[
  Version: V3
  Subject: CN=Jimmy, OU=Grant Space X, O=San Salvador, L=San Salvador,
  ST=Mejicanos, C=El Salvado
  Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13

Key: Sun RSA public key, 4096 bits
```
- Llave pública:**

```
Sun RSA public key, 4096 bits
modulus:
5359478917525546995110357047182827631460621762191916516613521798757900383
1204918944348441306583681611563280851861158670013693851908695073203865447
.....
```
- Texto cifrado:**

```
IE/ski4all5HSxtX+cAt47g7UqpcbLinLb7btHieThquktk8EdCzrlo+AH5pShZTA8Os78UPTaaT
Ka3rVyWYON7ESgN0V4kCOdvdN/XXleJcPkv1R/8pUSU7aaWeYM6AuaF4m0aWW4PIVYK6
KllnvB/rFo/mbDSTmJA4Soni5j6Wdz26bM4PzO2aRY2IY4IoiglChw+nk66+ToBzfn93itGdkM
JyxkyM8dY1SK5iPctG9n6zVXGs0bv3PUnt+ibKurEcVTTMb3vW1zjr7IZYcvfwkiQqACS7CcOE
dKvuSIQp3Azf4bE8yaYfPiO31bJ/EILWsQrlnaKR8MCT+tUIX1cL7xPg5ESpHWlvH4UH5ae/C3
A5qWTJ7gloaalk2n35ws3jcW5sDoESBSovpwxFZourNXzEP39Klrt7uEMloli7CJjz0XCSk9ZTFN
KUDvQqa+dobI5krYE89JFXJbDy+dPWe8rPTvgPv5gTE6YuaW0W4wlDwZ6PZvtetGTKltaCG
FWF9U+XmlyfCfOaaUvJvC1Vla7JNyM7SdLt8nurOf+e+RSGkP6yb/rdJcxR+D13C8YSWdxy9
```


Descifrando (RSA)

Al momento de descifrar el mensaje se debe pegar en el campo de “mensaje a descifrar” el mensaje cifrado obtenido en el paso anterior (generado en “cifrando RSA”) se selecciona el certificado con el cual se debe hacer la validación y el passphrase (la contraseña con la cual se creó el certificado). Se introducen estos campos de la forma correcta, se obtiene el mensaje original. En este ejemplo se utiliza el certificado creado con nombre Hendrix.

Cifrado asimétrico

Cifrar mensajes

Descifrar mensajes

Criptoanalizar RSA

Mensaje a descifrar

ZTA8Os78UPTaaTKa3rVyWY0N7ESgN0V4kC0dvdN/XXleJcPkv1R/8pUS
U7aaWeYM6AuiaF4m0aWW4PIYyK6KIInvB/rFo/mbDSTmJA4Soni5j6Wd
z26bM4PzO2aRY2IY4loiglChw+nk66+To8zfn93itGdkMJyxkyM8dY1SK5i
PctG9n6zVXGs0bv3PUnt+ibKurEcVTTMb3vW1zjr7IZYcvfwkiQqACS7Cc
OEdKvuSIQp3Azf4bE8yaYfPiO31bJELWsqRlnaKR8MCT+tUIX1cL7xPg5E
SpHWlvH4UH5ae/C3A5qWTJ7gloaalk2n35ws3jcW5sDoESBSovpwxFZou
rNXzEP39Klrt7uEMlOl7CJjz0XCsk9ZTFNKUDvQqa+dob15krYE89JFXJbDy
+dPWe8rPTvgPv5gTE6YuaW0W4wlDwZ6PZvtetGTKltaCGFWF9U+Xmlyf
CfOaaUVJvC1Vla7JNyM7SdLt8nurOf+e+RSGkP6yb/rdJcxR+D13C8YSW
dxy9zpGypa8OWEWtOCs22ujyQc5CHKUxCGP5nPGmWeXvpG3xqyN71f
/kLIZJGVBgBfgcChxvp42RjJnERUMA0E7oU3J0X2Ne0B0rqLY=

Certificado

hendrix

Passphrase

.....

Descifrar

Restaurar

Certificado

[
[
Version: V3
Subject: CN=Jimmy, OU=Grant Space X, O=San Salvador, L=San Salvador,
ST=Mejicanos, C=El Salvado
Signature Algorithm: SHA512withRSA, OID = 1.2.840.113549.1.1.13
Key: Sun RSA public key, 4096 bits

Mensaje original

Hola, este es un mensaje de prueba.

Cifrado simétrico

- **AES**
- **DES**

El módulo solicitará la clave y vector de inicialización configurables por el usuario, con el propósito de que el cifrado sea dinámico, también ofrecerá la posibilidad de criptoanalizar el texto cifrado, usando el alfabeto español.

Modos de operación de una unidad de cifrado por bloques².

The screenshot shows a web application titled 'Cifrado simétrico'. It has two tabs: 'CIFRADO DES' and 'CIFRADO AES'. The 'CIFRADO DES' tab is active. Inside this tab, there is a section titled 'Modo de Operacion' with four radio buttons: 'ECB' (selected), 'CBC', 'CFB', and 'OFB'. Below this, there are four input fields: 'Texto a Cifrar', 'Clave Cifrado', 'Vector Inicial', and 'Texto Cifrado'. There are two buttons: 'Cifrar' and 'Habilitar'. Below these, there are two more input fields: 'Clave Descifrado' and 'Texto Descifrado', with a 'Descifrar' button below them.

- **Modo ECB:** El mensaje es dividido en bloques, cada uno de los cuales es cifrado de manera separada. Modo ECB **no usa el vector de inicialización**.

² https://es.wikipedia.org/wiki/Modos_de_operaci%C3%B3n_de_una_unidad_de_cifrado_por_bloques

- **Modo CBC:** (cipher-block chaining), Antes de ser cifrado, a cada bloque de texto se le aplica una operación XOR con el bloque previo ya cifrado. De este modo, cada bloque cifrado depende de todos los bloques de texto claros usados hasta ese punto. Además, para hacer cada mensaje único se debe usar un vector de inicialización en el primer bloque.
- **Modo CFB:** El cifrado en bloque opere como una unidad de flujo de cifrado: se generan bloques de flujo de claves, que son operados con XOR y el texto en claro para obtener el texto cifrado. CFB es útil para transmisiones de flujos continuo.
- **Modo OFB:** output feedback) emplea una clave para crear un bloque pseudoaleatorio que es operado a través de XOR con el texto claro para generar el texto cifrado. Requiere de un vector de inicialización que debe ser único para cada ejecución realizada.

Cifrando y descifrando

Cifrado simétrico

- **AES**

Para cifrado AES, El tamaño de la clave

128 bit = 16 caracteres = Vector Inicial

192 bit = 24 Caracteres= Vector Inicial

256 bit = = Vector Inicial

Utilizará vector inicial **solo en Modos CBC, CFB, OFB**, el tamaño del dicho vector también debe ser de 8 caracteres, Los controles se deshabilitaran cuando se procesa el texto a cifrar y el botón habilitar los iniciara nuevamente.

CIFRADO DES

CIFRADO AES

Tamano en bit

☒ 128

☐ 192

☐ 256

Modo de Operacion

☒ ECB

☐ OFB

☐ CBC

☐ CFB

Texto a Cifrar

Para ECB no se necesita VI (vector inicializacion)

Clave Cifrado

para128-16bitsss

Vector Inicial

Texto Cifrado

qBn9uqD8HAI4Z7fw5SQ8t8UMj/+96Gjq/ZurUucNOWAJU/wxonMCA6H5VLTCHDMArt++LoD4gtZbXTAX2K4yZ8Q==

Cifrar

Habilitar

Clave Descifrado

para128-16bitsss

Texto Descifrado

Para ECB no se necesita VI (vector inicializacion)

Descifrar

CIFRADO DES

CIFRADO AES

Tamano en bit

☐ 128

☒ 192

☐ 256

Modo de Operacion

☐ ECB

☒ CBC

☐ OFB

☐ CFB

Texto a Cifrar

Para CBC, OFB, CFB se necesita VI (vector inicializacion)

Clave Cifrado

para 192-key de 24bitsss

Vector Inicial

VI de 16 bitssss

Texto Cifrado

jzwzTw1ZWgEH9B2uQdMg+Ewie83UrlAj10QIXiQN4IfQkmkLkbi8fW76CYwzhKjP/7kgxOSr1cXDATSQm+rf4g==

Cifrar

Habilitar

Clave Descifrado

para 192-key de 24bitsss

Texto Descifrado

Para CBC, OFB, CFB se necesita VI (vector inicializacion)

Descifrar

CIFRADO DES

CIFRADO AES

Tamano en bit

☐ 128

☐ 192

☒ 256

Modo de Operacion

☐ ECB

☒ CBC

☐ OFB

☐ CFB

Texto a Cifrar

Para CBC, OFB, CFB se necesita VI (vector inicializacion) desde 256 bits

Clave Cifrado

para 256 se necesita clave de 32

Vector Inicial

vector de 16 bit

Texto Cifrado

dIN8rPlO7bP8OYwSrff8DmBwWtcrU52eHHsE9LasKNdv2z/lre/9sM8b3
qge/qoYmW78IkTL3pLhUowoQsxLI3CDII6WlzmU4v+mdPnNuk=

Cifrar

Habilitar

Clave Descifrado

para 256 se necesita clave de 32

Texto Descifrado

Para CBC, OFB, CFB se necesita VI (vector inicializacion) desde 256 bits

Descifrar

- **DES**

Para cifrado DES, El tamaño de la clave es de 8 bit (caracteres) y se utilizara vector inicial **solo en Modos CBC, CFB, OFB**, el tamaño del dicho vector también debe ser de 8 caracteres

CIFRADO DES

CIFRADO AES

Modo de Operacion

☒ ECB ☐ CBC ☐ CFB ☐ OFB

Texto a Cifrar

el algoritmo bloque ECB

Clave Cifrado

algorith

Vector Inicial

Texto Cifrado

BluRQlaNQp4KbQSCg4LSWM5KLDs3+xPD

Cifrar

Habilitar

Clave Descifrado

algorith

Texto Descifrado

el algoritmo bloque ECB

Descifrar

CIFRADO DES

CIFRADO AES

Modo de Operacion

☐ ECB

☐ CBC

☒ CFB

☐ OFB

Texto a Cifrar

el algoritmo bloque CFB

Clave Cifrado

albloque

Vector Inicial

vectorin

Texto Cifrado

Kk+qKhm/LhogM90wvn+XLPrzch1oY7j

Cifrar

Habilitar

Clave Descifrado

albloque

Texto Descifrado

el algoritmo bloque CFB

Descifrar