



# CIFRADO Y DESCIFRADO

MANUAL DE USUARIO

Cryptography 3CV2  
Hayde Barbosa

# CONTENIDO

1. Ejecutar el programa
2. Llaves de usuarios
  1. AES simplificado
    1. Nueva llave
    2. Nueva llave aleatoria
  2. Cifrado y descifrado
3. Cifrar un archivo
4. Descifrar un archivo



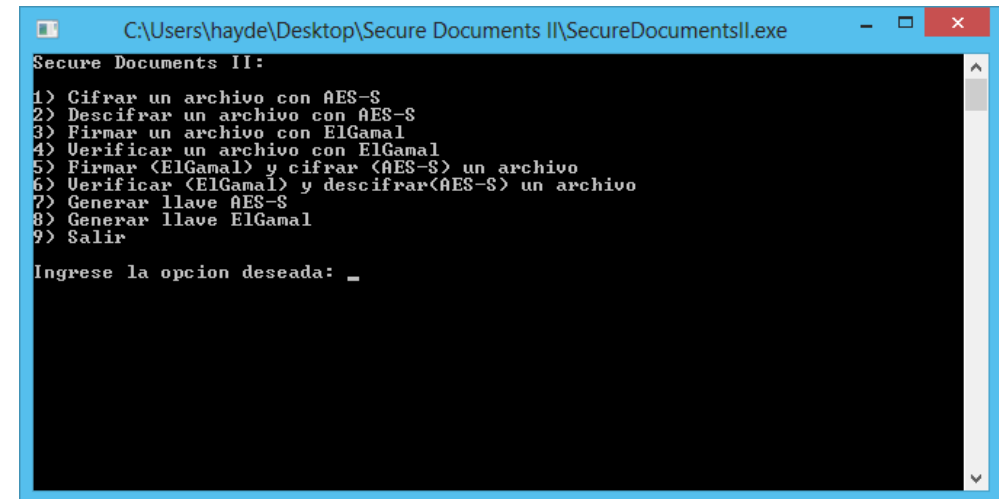
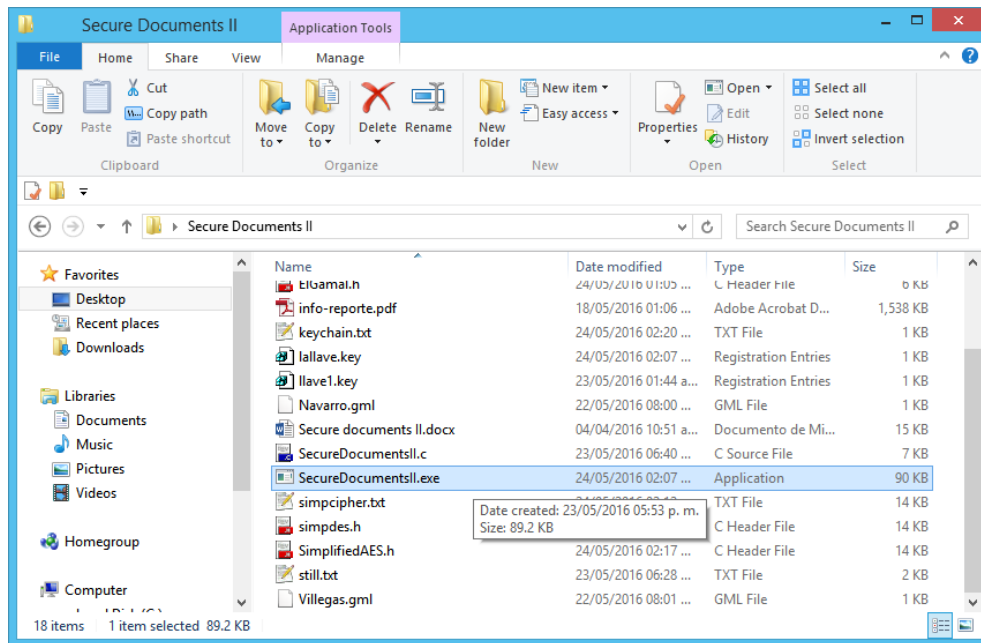
# 1. EJECUTAR EL PROGRAMA

COMO SE EJECUTA EL PROGRAMA?



# 1. EJECUTAR EL PROGRAMA

- Para ejecutar el programa, simplemente se debe dar doble click a CifradoYDescifrado.exe.
- El programa se ejecutara.



En la izquierda se muestra como se ubica dentro de una carpeta el programa SecureDocumentsII.exe y en la derecha se muestra el programa ejecutándose.



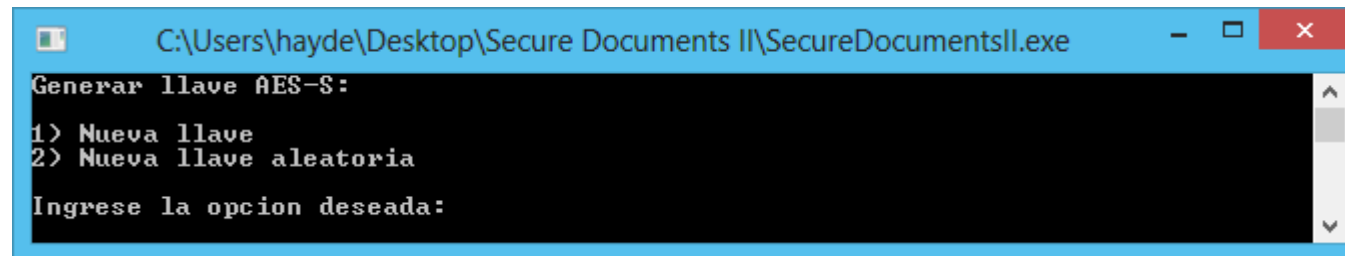
## 2. LLAVES DE USUARIOS

COMO GENERAR LLAVES?



## 2.1 AES SIMPLIFICADO

- Dentro del menú principal del programa, se ingresa la opción 7.
- El menú mostrara 2 opciones:
  - 1) Nueva llave
  - 2) Nueva llave aleatoria



```
C:\Users\hayde\Desktop\Secure Documents II\SecureDocumentsII.exe
Generar llave AES-S:
1> Nueva llave
2> Nueva llave aleatoria
Ingrese la opcion deseada:
```

## 2.1.1 NUEVA LLAVE

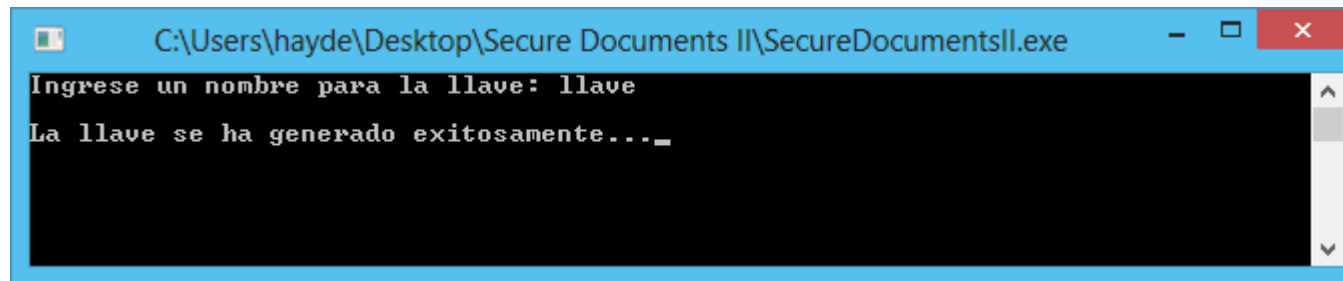
- Tras ingresar la opción 1) *Nueva llave*, del menú anterior, se pedirá un nombre para la nueva llave. Nota: si se ingresa el nombre de una llave existente el contenido se sobrescribirá.
- El usuario deberá ingresar valores para formar la nueva llave.



```
C:\Users\hayde\Desktop\Secure Documents II\SecureDocumentsII.exe
Ingrese un nombre para la llave: llave
Ingrese el valor 1 <entre 0-15>: 4
Ingrese el valor 2 <entre 0-15>: 8
Ingrese el valor 3 <entre 0-15>: 13
Ingrese el valor 4 <entre 0-15>: 0
La llave se ha generado exitosamente..._
```

## 2.1.2 NUEVA LLAVE ALEATORIA

- Tras ingresar la opción 2) *Nueva llave aleatoria*, del menú anterior, se pedirá un nombre para la nueva llave. Nota: si se ingresa el nombre de una llave existente el contenido se sobrescribirá.
- La nueva llave aleatoria será generada automáticamente.



```
C:\Users\hayde\Desktop\Secure Documents II\SecureDocumentsII.exe
Ingrese un nombre para la llave: llave
La llave se ha generado exitosamente...
```





## 3. CIFRADO Y DESCIFRADO

COMO UTILIZAR AES-S?



## 3.1 CIFRAR UN ARCHIVO

- Primero, para cifrar un archivo con AES-S se necesita una llave.
- Se coloca el archivo a cifrar en la misma carpeta que el programa *SecureDocumentsII.exe*. En este caso se cifrara una imagen (*imagen.jpg*).
- En el menú principal se elige la opción *1) Cifrar un archivo con AES-S*. El programa solicitara la siguiente información:
  - *Nombre del archivo, se deberá incluir la extensión.*
  - *Nombre del archivo cifrado*
  - *Nombre de la llave, se deberá ingresar el nombre de la llave. Nota: esta llave es extensión \*.key, no debe confundirse con la llaves privada y publica de ElGamal.*
- *Posteriormente se deberá elegir un modo de operación:*
  - *CTR (opción elegida para este ejemplo)*
  - *CBC*

## 3.1 CIFRAR UN ARCHIVO

```
C:\Users\hayde\Desktop\Secure Documents II\SecureDocumentsII.exe
Ingrese el nombre del archivo a cifrar (incluya la extension): imagen.jpg
Ingrese un nombre para el archivo cifrado: imagenCifrado
Ingrese el nombre de la llave (AES-S): llave
```

```
C:\Users\hayde\Desktop\Secure Documents II\SecureDocumentsII.exe
Seleccione el modo de cifrado:
1) CTR
2) CBC

Ingrese la opcion deseada: 1

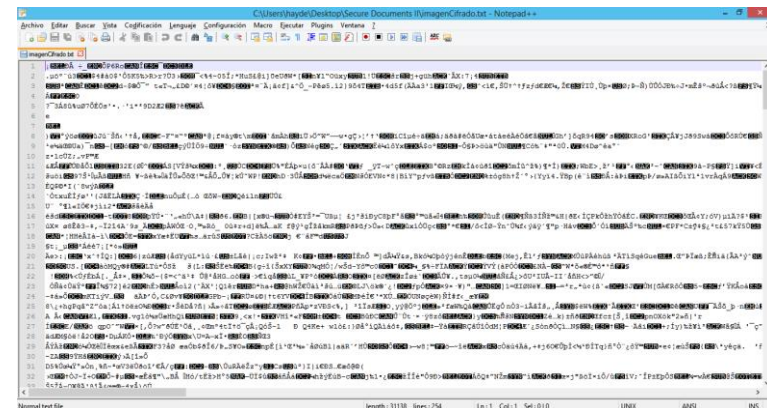
El archivo imagen.jpg ha sido cifrado, verifique imagenCifrado.txt...
```

Proceso para cifrar un archivo.

- Como resultado se obtendrá un archivo \*.txt con el archivo cifrado.



Imagen.jpg

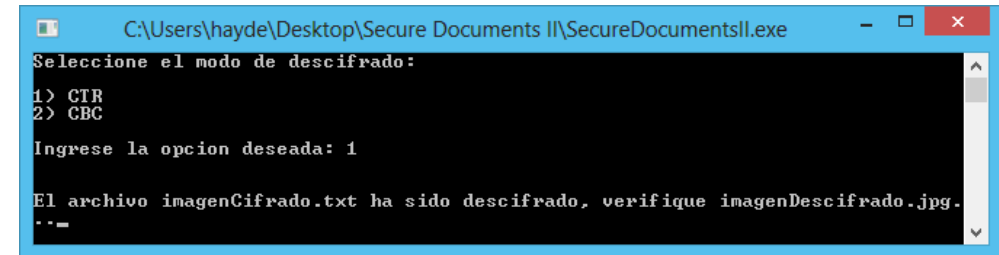
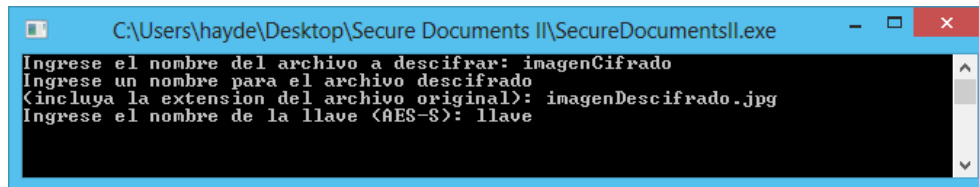


ImagenCifrado.txt

## 3.2 DESCIFRAR UN ARCHIVO

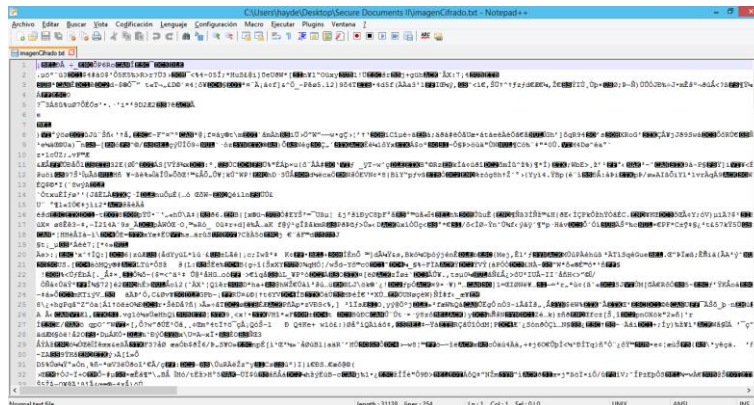
- Primero, se deberá contar con la llave usada para cifrar así como del archivo cifrado, los cuales deberán estar en la misma carpeta que el programa *SecureDocumentsII.exe*.
- En este caso se descifrara una imagen (*imagen.jpg*) del archivo cifrado *imagenCifrado.jpg*.
- En el menú principal se elige la opción 2) *Descifrar un archivo con AES-S*. El programa solicitara la siguiente información:
  - *Nombre del archivo a descifrar (en este ejemplo imagenCifrado).*
  - *Nombre del archivo descifrado, se deberá incluir la extensión del archivo original.*
  - *Nombre de la llave, se deberá ingresar el nombre de la llave con la que se cifro.*
- *Posteriormente se deberá elegir un modo de operación:*
  - *CTR (opción elegida para este ejemplo)*
  - *CBC*

## 3.2 DESCIFRAR UN ARCHIVO



Proceso para descifrar un archivo.

- Como resultado se obtendrá el archivo original.



ImagenCifrado.txt



ImagenDescifrado.jpg