

SEGURIDAD EN REDES

PRÁCTICA 2

CRIPTOGRAFÍA SIMÉTRICA – AES

1. ¿Cuál es la fortaleza de seguridad del algoritmo de cifrado simétrico AES?

Es un algoritmo de cifrado por bloques, el tamaño fijo del bloque es de 128 bits. La longitud de la clave se puede elegir, y puede ser de 128, 192 y 256 bits.

2. Describa el algoritmo de cifrado AES

El algoritmo tiene dos entradas: Texto claro y llave, el texto claro se va al proceso de cifrado y la llave original va a otro para generar subllaves en cada ronda del algoritmo.

1. Se toma la matriz de estado donde se encuentra el texto claro y mediante XOR se le suma el contenido de la matriz donde esta almacenada la llave (suma la llave de la ronda).

2. (9 rondas) En cada ronda se realiza una transformación:

- sustitución de bytes: sustitución no lineal donde cada byte es reemplazado con otro de acuerdo con una tabla de búsqueda.
- desplazamiento de filas: se realiza una transposición donde cada fila del state es rotada de manera cíclica un número determinado de veces.
- multiplicación de columnas: es la operación de mezclado que opera en las columnas del state, combinando los cuatro bytes en cada columna usando una transformación lineal.
- Se le suma la llave de la sub-ronda. (En total 9 subllaves): cada byte del state es combinado con la clave «round»; cada clave «round» se deriva de la clave de cifrado usando una iteración de la clave.

3. Ronda final.

Aplica 3 transformaciones:

- sustitución de bytes.

- desplazamiento de filas.
- se le suma la llave de la ronda.

3. Describa el algoritmo de descifrado AES

1. Aplica 3 transformaciones:

- se le suma la llave de la ronda.
- desplazamiento de filas.
 - sustitución de bytes.

2. Nueve rondas con las siguientes transformaciones:

- se le suma la llave de la ronda.
- multiplicación de columnas.
- desplazamiento de filas.
- sustitución de bytes.

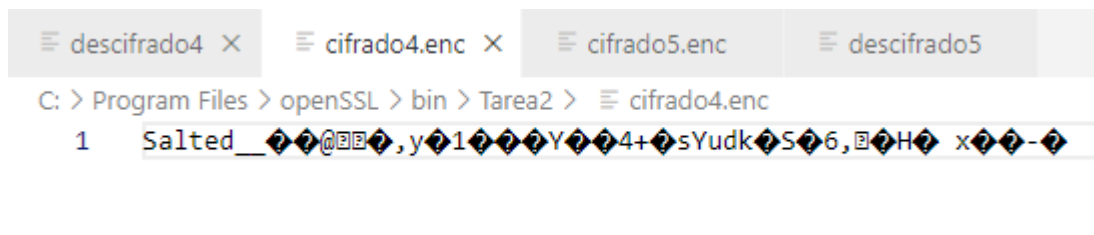
3. Suma de la llave de la ronda (original).

Descargue e instale OpenSSL (<https://www.openssl.org>) en su computadora. Usando OpenSSL realice los siguientes cifrados y descifrados, devuelva el texto cifrado, la llave secreta de 128 bits y las líneas de comando usadas:

4. Cifre/Descifre su nombre completo, usando **AES-CBC**.

Nombre: Isabel Rodríguez Cisneros

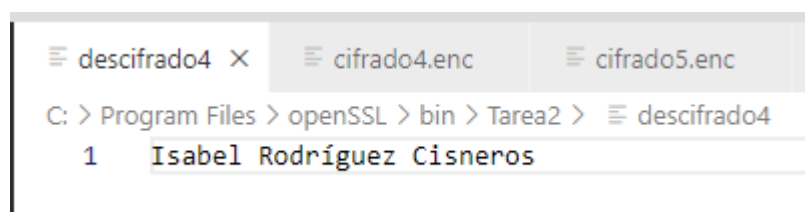
Texto cifrado:



Llave: Color190

```
c:\Program Files\openSSL\bin\Tarea2>openssl aes-128-cbc -in Nombre4.txt -out cifrado4.enc
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

c:\Program Files\openSSL\bin\Tarea2>openssl aes-128-cbc -d -in cifrado4.enc -out descifrado4
enter aes-128-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

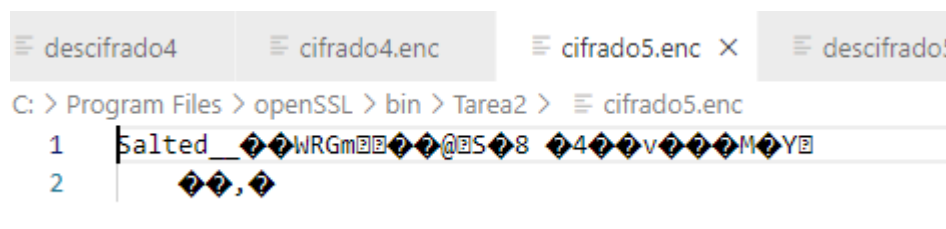


The screenshot shows a Windows Explorer window with the address bar displaying 'C: > Program Files > openSSL > bin > Tarea2 > descifrado4'. The file 'descifrado4' is highlighted in the file list. The window title bar shows three tabs: 'descifrado4', 'cifrado4.enc', and 'cifrado5.enc'.

5. Cifre/Descifre su nombre completo, usando **AES-CFB**.

Nombre: Isabel Rodríguez Cisneros

Texto cifrado:



The screenshot shows a Windows Explorer window with the address bar displaying 'C: > Program Files > openSSL > bin > Tarea2 > cifrado5.enc'. The file 'cifrado5.enc' is highlighted in the file list. The window title bar shows four tabs: 'descifrado4', 'cifrado4.enc', 'cifrado5.enc', and 'descifrado5'. The file list shows two files: '1 Salted_??WRGm??@?S?8 ?4??v??M?Y?' and '2 ??,?'.

Llave: Color190

```
c:\Program Files\openSSL\bin\Tarea2>openssl aes-128-cfb -in Nombre5.txt -out cifrado5.enc
enter aes-128-cfb encryption password:
Verifying - enter aes-128-cfb encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

c:\Program Files\openSSL\bin\Tarea2>
c:\Program Files\openSSL\bin\Tarea2>openssl aes-128-cfb -d -in cifrado5.enc -out descifrado5
enter aes-128-cfb decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

```
≡ descifrado4  ≡ cifrado4.enc  ≡ cifrado5.enc  ≡ descifrado5 X
C: > Program Files > openssl > bin > Tarea2 > ≡ descifrado5
1  Isabel Rodríguez Cisneros
```

6. Cifre/Descifre su nombre completo, usando **AES-CTR**.

Nombre: Isabel Rodríguez Cisneros

Texto cifrado:

```
≡ cifrado6.enc X  ≡ descifrado6
C: > Program Files > openssl > bin > Tarea2 > ≡ cifrado6.enc
1  Salted__U??D(*?k??}??X??A?h??B??A?l??
```

Llave: Color190

```
c:\Program Files\openssl\bin\Tarea2>openssl aes-128-ctr -in Nombre6.txt -out cifrado6.enc
enter aes-128-ctr encryption password:
Verifying - enter aes-128-ctr encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

c:\Program Files\openssl\bin\Tarea2>openssl aes-128-ctr -d -in cifrado6.enc -out descifrado6
enter aes-128-ctr decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

```
≡ cifrado6.enc X  ≡ descifrado6 X
C: > Program Files > openssl > bin > Tarea2 > ≡ descifrado6
1  Isabel Rodríguez Cisneros
```

7. Cifre/Descifre su nombre completo, usando **AES-ECB**.

Nombre: Isabel Rodríguez Cisneros

Texto cifrado:

```
cifrado7.enc x descifrado7
C: > Program Files > openssl > bin > Tarea2 > cifrado7.enc
1 Salted__5H8?p??^%lng4)v9>J??????=sa??g??
```

Llave: Color190

```
c:\Program Files\openssl\bin\Tarea2>openssl aes-128-ecb -in Nombre7.txt -out cifrado7.enc
enter aes-128-ecb encryption password:
Verifying - enter aes-128-ecb encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

c:\Program Files\openssl\bin\Tarea2>openssl aes-128-ecb -d -in cifrado7.enc -out descifrado7
enter aes-128-ecb decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

```
cifrado7.enc x descifrado7 x
C: > Program Files > openssl > bin > Tarea2 > descifrado7
1 Isabel Rodríguez Cisneros
```

8. Cifre/Descifre su nombre completo, usando **AES-OFB**.

Nombre: Isabel Rodríguez Cisneros

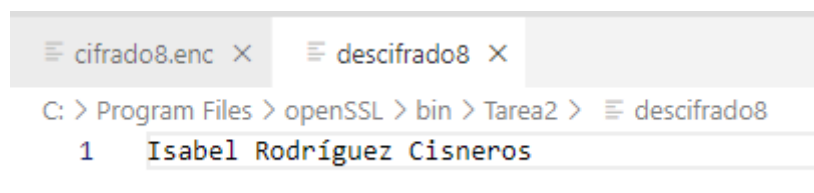
Texto cifrado:

```
cifrado8.enc x descifrado8
C: > Program Files > openssl > bin > Tarea2 > cifrado8.enc
1 Salted__7e?Ö^?wc?.0000Ehpx?:00090Z?
```

Llave: Color190

```
c:\Program Files\openssl\bin\Tarea2>openssl aes-128-ofb -in Nombre8.txt -out cifrado8.enc
enter aes-128-ofb encryption password:
Verifying - enter aes-128-ofb encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

c:\Program Files\openssl\bin\Tarea2>openssl aes-128-ofb -d -in cifrado8.enc -out descifrado8
enter aes-128-ofb decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```



CARPETA CON ARCHIVOS:

Archivos de programa > openssl > bin > Tarea2

Nombre	Fecha de modificación	Tipo	Tamaño
cifrado4	19/08/2021 12:32 a. m.	Archivo ENC	1 KB
cifrado5	19/08/2021 12:36 a. m.	Archivo ENC	1 KB
cifrado6	19/08/2021 12:51 a. m.	Archivo ENC	1 KB
cifrado7	19/08/2021 12:55 a. m.	Archivo ENC	1 KB
cifrado8	19/08/2021 12:59 a. m.	Archivo ENC	1 KB
descifrado4	19/08/2021 12:33 a. m.	Archivo	1 KB
descifrado5	19/08/2021 12:37 a. m.	Archivo	1 KB
descifrado6	19/08/2021 12:51 a. m.	Archivo	1 KB
descifrado7	19/08/2021 12:55 a. m.	Archivo	1 KB
descifrado8	19/08/2021 12:59 a. m.	Archivo	1 KB
Nombre4	19/08/2021 12:09 a. m.	Archivo TXT	1 KB
Nombre5	19/08/2021 12:09 a. m.	Archivo TXT	1 KB
Nombre6	19/08/2021 12:09 a. m.	Archivo TXT	1 KB
Nombre7	19/08/2021 12:09 a. m.	Archivo TXT	1 KB
Nombre8	19/08/2021 12:09 a. m.	Archivo TXT	1 KB
openssl	25/03/2021 08:34 p. m.	Aplicación	531 KB

9. ¿Qué diferencias observa en los textos cifrados anteriores?

Se pueden ver algunos caracteres distintos y no varían demasiado el tamaño entre sí.

10. ¿Qué diferencias observa entre los textos cifrados usando DEA y AES?

Se observan más combinaciones de los caracteres en AES y en DEA no había una cantidad aproximada para lo cifrado, en cambio en AES no varía mucho la cantidad.