

Lab #01 – Secret-Key Encryption

Lab Group 13

Kalid Ajibade (100660188)

Walid Ayub (100695612)

Zain Butt(100751676)

Konrad Herbus

Task 1: Encryption using different ciphers and modes

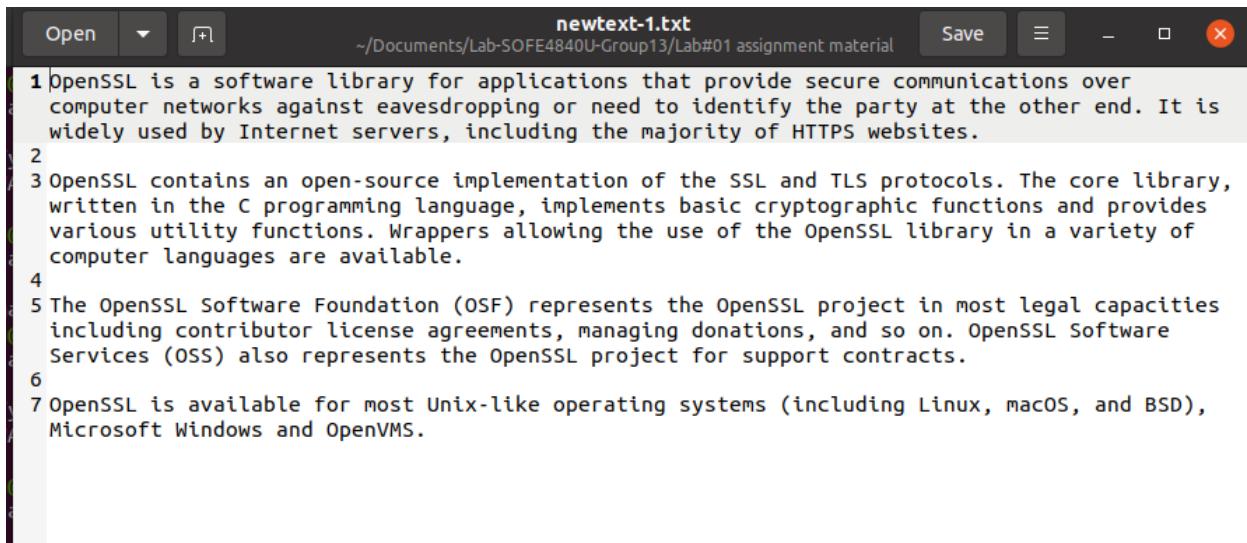
-aes-256-cbc encryption :

```
cmc.esc -ncp for summary.  
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$ openssl enc  
-aes-256-cbc -in OpenSSL.txt -out cipher-aes-256-cbc.txt  
enter aes-256-cbc encryption password:  
Verifying - enter aes-256-cbc encryption password:  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$ █
```

1 Salted_\A8\A5\9B\F2\CS581\EF
2 +\ED\B2\B22\E3\j\N\A7\FB\|E11\F8h\|F0\B4\A1d\87\A4\9R\EF\99\|B48\|D7\99=S\FE\A6\|E0\|F0\|E9+
\BC+_81\|E4\|D9"\B4\88\|F2\EC\AE\|CFZ\A8:\|BE\|83\|F01\|C7\99\|*o\|F2h\|A9\|q\|B8\|A3D\|CCy\99} -
Jj\|D9\|D7\|E2\ABQY\|EED
3 \CEG\9A\|;M\99\|D9q\|B7\|83^{\FD\A56 .\^}\EB\|\C98\|DD\|CO\|A6\|92\|E9\|8A\|FF\|B3\|90\|A7D\|B3\|8C\|ZiA\|8E;
\BB\|F7\|A9\|BC\#B0\|EE\|L\|B7\|AD~\|M\|91\|AbwF3uo\|8CUp\|BFI\|97\|8Ftb\|EB\|吳
&\AB\|B5\|E7\&\|EF\|BZb\|K\|9BkD\|92\|BF\|CDU\|AG\|E\|D\|AAz\|99\|A6\|87\|8E\|B5\|8D\|90\%CT\|EA\\$
\FA\|DDvN7\|C1\\$\\EE\|A7\|9A0\|88\|jh\|8E"\|A4B\|C5r\|.)d\|D5\|~\|95\|FF\|C7\\$\\A304\|韓
\AB\|E8nV\|EE\|F0\|83X\|F8]P\|001\|FF\|81
4 d\|96\|00
5 \CC\|F\|A2\|99\|99\|*g\|9E\|F6\|99\|F5VJ\|99\|e\|E0\|9\|810\|95\|e\|EF3\|AD\|;
\85\|C0\|9F\|F6\|F6\|93S\|AC\|F4\|F6\|D65Zu\|9\|94\|00\|FC\%B7
6 k\|87\|A0\|FE\|B5\|B8\|A2PIX\|B\|90\|DCFs\|B6hz\|BC\|CE\|IA\|I= \C6\|C7\|C870\|A6K\|B5\|z\|CE.
\FA35\|B0F\|BDT\|B8aBV\|85\|CA\|E4\|88\|89\|:\|F6l\|A5\|838\|95\|86\|TB\|C9xs\|99B\|BC\|98\|99\|Gl\|B7\|97Z\|85Y!
\A4\|90\|8D\|AA\|C0\|EE+\|FA5\|C6\|,\|D2Z\|BF\|83\|.\|89\|E6\|BE\|?M\|`>\|D6\|FB\|EE\|pI\|99\|.\|D3\\$\\CE\#\|E\|C\|D9\|P3\|E2\|F4
r\|DFR\|k\|F1\|F9\|EE8N\|95p\|F9\|E7\|90R\|00\|AE\|,\|AC<\|q\|-\|F9\|C1@A6
7 1\|BD\|80\|B\|B0\|E0[\|F9\|E7a\|F6\|A6\|C0\|B\|BD\|C8h\|D72\|J\|E82\|k\|85\|8F*\|00\|87\|FA\|8F\|A4\|98\|B95\|B91\|FA\|/-
\\$\\EC\|V\|B0\|A8\|85K\|A5\|s\|3\|39\|.5\|C\|93xe\|8E3\|CA\|.\|D3\|F8z\|86\|87\|S\|B46\|85\|B5\|97MPF!.-
4\|F2\|W\|B6q\|S\|99\|(BC\|99\|91\|Ech\|F4\|80\|A2=\|E0gDs\|8Fa\|E7\|A1\|F5\|E8y\|81\}]\|EF\|DA\|E2q\|99\|99\|99\|99\|95\|AB\|C0+
\99\|F6\|8AY14N\|9Bz* \D3\|~\|FF\|D1n6\|90\|C1\|B2H\|A0\|B6\|97\|D5@1\|A4\|, \|B0t\|ey\|C00\|]\|E7Y\|95\|D8R:
Y\|99\|v\|89T\|92\|D10\|81\|C2\|99\|.\|FE\|E0\|99\|>\|BC\|FE\|89\|D1\|C4a\|87\|B7\|B5\&e^
8 \|\984\|A5\|A5\|D1@S\|FB\|D2\|VNvg\|FC\|94\|9E\|.\|D0\|B0\|B6\|89\|FF\|99\|c\|A6\|E6\|99\|EBU:
\96\|B7\|C6\|~\|BDCU\|FB\|9F\|DC\|D0\|E6\|C7\|= \FBKZK\|E8\|91\|89\|85\|+'
\8D\|F6\|k7\|DB\|w\|E8\|85Zu\|F2\|B6\|A3Bv7\|B4\|B8\|F9\|E7\|DD\|B\|E8\|B8\#6\|FC\#G\|A7@~\|D5\|CF\|
p\|00mdo\|B8\|,\|FC\|9Ake\!7\|B7\|C5\|.\|89p\|188gk\|O\|FC\|DS1\|CC5\|8EU\|B2C\|AF\|895\|E3\|D5\|~\|L\|91y
\AE\|D78jh\|9E\|AC\|EC\|9Aa8d\|D9\|E3\|80\|B3\|C6\|E5d\|E7\|B8\|0\|A5\|93\|B5\|9F9E\|BF\|CFW\|FF\|ACK\|87
9 =\|83\|BFj\|B6\|DE\|EB\|99\|CS\|~\|B0\|A1a

Decryption:

```
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$ openssl enc  
-d -aes-256-cbc -in cipher-1.txt -out newtext-1.txt  
enter aes-256-cbc decryption password:  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$
```



-aes-192-cbc encryption :

```
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$ openssl enc  
-e -aes-192-cbc -in OpenSSL.txt -out cipher-2.txt  
enter aes-192-cbc encryption password:  
Verifying - enter aes-192-cbc encryption password:  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$
```

1 Salted_kI\7^h\EEV\95\EEO\DE-\DCN=\B7\8A\F7\B8h
2 \BC\|F9\J\EE\CBF\E1#\D3\|9B\Z\00\8F-[9A\AE]b\98\EBQ\|F5\B6\B2\85
rtI\84e \B7\|D7m\|B8\|d\|PNDW\|DA,\|b\|A5\B2\|B7\|EBY\|3\|A7NZ\|F8\|B8q\|C6.\|A7\|B8k(:0`i\|AC\AD\9C
3 \|
4 \|EB\|CB\|80\|8F\|BD\|BC\|CD>\|E9\|C6.5\|F4g\|FAX\|93\|81
\|F5j\|F8\|CF\|DF\|E7\|CAW+aS~\|90:\|DE\|E\|89\|B4z\|F\|p@t)
\|FC\|E0\|CB\|E1\|F0\|E8.\|90\|F3\|C7\|E2\}\|88\|F3d\|9\|F6w
D7\|3\|CC\|EB\|C7,\|A6z\|EF\|F6n\|/
\|F4CHxS\|81\|9\|M`.\|00\|A\|C0&\|F4\|AA\|AB\|FD\|E2\|97\|C8\|C\|D2+u%
\|DB\|FC+\|A7\|B2Z\|F8\|FA\|98\|E2g\|F1\|E8a"\|91p\|87Wb\|FFL\|F8\|E3\|CE\|94T\|B5\|@\|91\|E80\|83\|I\|C9\|F4\|A\|C0
97\|AES\|
5 \|D8\|E2\|9\|L\|ED\|e\|8B\|83\%D3" F\|A5u\|C5P\|92\|
\|C6V\|ED\|86\|C1\|A0\|F7g\|CF\|88\|9\|F4l\|AF\|91\|DEX\|Adqq\|90w\|CB7\|88Q\|C\|CG#\|9E\|E4Lo\|86M\|FB\|94r\|
\|E1\|K8\|A8\|DB\|FE-K\|8B*\|A84\|CB=\|8C\|99,\|99\|95\|DFC+-\|FB\|9A\|FD
6 \|E9'\|CO\|E7\|E7\|CF\|94\|B6\|83\|L\|AC\|E2\|D8\|F0\|90P\|3\|B8\|A\|{D4\| -
\|E9\|E2\|C6\|F35\|C5\|E1\|FF2\|F\|96\|ED\|F7\|86\|A1\|B0\|D6\|C9\|E3\|E6\|9E\|C\|qH\|FF\|E8\|94\|CB\|8D\|C
\|9Cp\|FE\|AD\|C8yQ\|99\|D0\|D8B\|I\|0\|1\|:\|{I\|/\|B6\|EC\|B7\|D5@\|DC\|K\|F3\|A2c0\|84\|8A\|F1~
7 \|E20\|F\|y\|A9<\|93\|7\|D1X5\|A1\|w2\|I\|9c\|/\|88\|DC\|F4Y\|FF\|FA\|B2\|E2\|I,\|96\|D1\|F5\|90\|A9\|AF\|ED:
8 \|FD\|8B\|8B\|wV\|B3\|A82\|F8F\|90\#5\|B5\|C2\|B9\|E50A\|D9Z\|FB\|CC\|Zi\|BAS\|C7[\|ED\|(\|8D3\| -
i\|B5\|90\|9A4\|89ksd\|A4\|C2\|A4\|80s\|^\|9B\|94-
\|F34\|84\|B8\|EB\|Z\|C3\|FEU\|B3\|98\|C2\|EE\|E7\|90\|CO\|DE5\|EF\|88\|E8-\|8F\|00!
e\|B8\|AF\|A1\|A6\|E1\|92\|FD\|F5\|0\|AC\|EF\|8E< (\\$|ED\|-\|8C\|i\|BB\|84>A\|BB\|AAj\|CA\|EC\|C0\|9B\|dz\|C8K/-
F\|9EWI\|A1\|A2\|AAp\|FD!\|BCK\|F\| -
m\|B62\|D5\|C8C\|A6m5\|D3\|V\|EEx\|A3g\|FFvx\|ECA(\|F0\|85\|A9#\|8FF+\|i\|yh\|E\|YM^(\|D2E\|96\|95#\|DF
\|E5\|00\|9B\|FE\|CS\|o\|BC\|A6\|EF\|90\|870\|BC\|901\|96\|AE\|9ef\|CF\#-Z-
\|893\|A69\|-\|DA\|DE\|A\|86\|967\|8C9\|e\|9\|9A\|8F\|B3\|CFO\|B6A\|DF\|
\|F0\|C7\|R\|CC\|F0*QK\|EB\|Cp\|A2g\|EB\|W\|A7\|B9\|EB\|EB\|BC\|E6

Decryption:

```
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$ openssl enc  
-d -aes-192-cbc -in cipher-2.txt -out newtext-2.txt  
enter aes-192-cbc decryption password:  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$
```

-aes-192-ecb encryption :

```
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$ openssl enc  
-e -aes-192-ecb -in OpenSSL.txt -out cipher-3.txt  
enter aes-192-ecb encryption password:  
Verifying - enter aes-192-ecb encryption password:  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$
```

```

1 Salted _00\ACNp\B200\F8\965\0701\CD\CO\8700\AB\99\B5\E4e00\ED\F5\07\9B6\EAoz`0000(*Ku\98\9EPh\F7
2 N\81+|_0\BD\f2\EEH n\0F9\A8\B75<:$95\96\$ P*A]\08A\95\CB\04V\0FE\B2W\0C0Kcu\AA-
\CS00\FC7Hy\0FBa\0C4@100.00{0B[\0E300(9)2S\0FB\0F6\0E4\0BCP\0D0
3 \A9`n\96\0C38\B600\A1\AB\EA\B72\&8000;75'00\0C200Q\9A5]\0F7G00
\AF@hv00\0D28\0FA\CA00\0C5d\0FD\0B100\99\AF\84\90C\0F0t\0F300\AB,
\843\0DFt\08F\90,J\0F2\0EB\096\09B\085\0B0\0C900\0BF\0F1N\0C400a\0A9h00\0E1\0DD00\0S00\08D\0DF\0D4/J\0D$0
\8B\AE5j\085\AC\0B0\08AM00L00?0X\0BF!T\0AC\EE\08T\0E8\0D0\0CB\0E3\0D8y/\08F,\0000\0F6d00
4 X\A900\B500\0BF\0BB3\0A7\0B2fL\0A4"1\09F_<\0A0\0E7\0CE\0YR7\0A5\0ED100 ;\0EF~Y\0AD00D\095\0B6y\0B3Z\0B0-‐
99\0A6\0FB\0CS\0EBR00\086\0D9\0F4\086\0D8oD\095\0A6\0F5\0A4v\$1\08A\08C\0B6\0A6Z/-‐
l\0D1M\088\0A800<I\0E5\08F\0Oaxh@0\0CEU00\090mG00\0D4aU,
5 \0E8L\0B2\0A7\0B8\0A2\0A8q00\0BA\0E1Q\0B000-
Q\0B2\084&00\082\0BF00>\0F1MQA\0BA]Z\0E5\0CFHAA\085\0F5\0E8\09FM\0E4LZ\0FEb)
\0F2a\08C\08CeI200X\0CEV\08B0000\0A6\08F7\09200\$1\089E\08A+\0BF\093\0ECZ+
\0BFQ\0B4\0B1\0F300L0<\0F5\0A8\0F1(\0AA7\0q\0E800\0EA400\0A73\08D\08En\098@sh\0A0U00\0V\0F2\09C\0FE.
\091[00\0B1]>\0FB00\099\0DC00\0D78\0A8\0AF00\090\0FE\0\085F00\0FB?\084d\08D\0BD\0B4\085\096N\08AZI\085R\0C000
d0\0BF\0CA\0E300\0B200Zi\0B1\0875\094\0DC\0C4n\085i\0kMP00*\$1\0F0\0B1\0DFk7"0\087F!-
x00\0CF\0CF\0DBpl\083\0E0\0ED\09D\0ED1\0E900\0F1\08C3\094\0FD\091\09A\097\0BA00\0BZ00[\0BAs:\0A359\0C300\08\0B500\0CC,
\0B5\0E22\0\0F6\09F00\0B5\0A6\0FDI\08A\0F0]00h=t\0CC%,
\0A8\0B4\0D1<\0F8\0ACZ000\0EF\0D7W\093\0D9\0F5\0A6;\080xN\0AB\0C0\$.
\087h#\08ANF3\08C\0C4\0C8[<\0D1K\0ACE\0FE\080\0C401b\090n\0CA1|\096\097(\0B50\09B\$0
\0BA~\0B0\0A1\0A6\0C3"00\0U\0ABwf,N\0B6\0E900=b/\097_S00T\0AE;dx\0B7\0FC\08D00\0D7\0EE\0D2\0C4P
6 \097\0CC0000H\0FA\0C9V\0B7^006\0AB9\0E900T\0A2FMW\0DE\0D2\0D5\0D400\0T\0CDS\000\0EA\$1\0C9\$d\0B4\088R\09F+\0FE<'H]00|-‐
j\0C800\0DB\0B0\0E+\0ED\0EA00!1\0B8\0D400\085\0V00\0C5\0EF\0CBA\08A\0R|-‐
x,v\0E6\0D2\0F2\0ABN\0DB\0DFq=i'\0C2V\089U00\080(`\03\093\0A6\0CB00MF\0D6HC/m\0F2\0B0
B\0D9%I\0C7005W\0E6\0E9\0D4\0E7\0B0!!i\0CE\0C0\0E700\0CC00\09E\0B5!
\0A9`w\0F5t\0B300,/79\0A4\09900\0BD\088\0B500\08A\0AA\0
\080\091\090\0E6\0E0*LH8\0B7\0E7\0UC\0B8\0CB\0C34\089M00\0B1\0F7\0FA\0F9,<0\0EAe\0E6g\0B3\09C"Y,7

```

Decryption:

```

kalid@kalid-virtual-machine:~/Documents/Lab-S0FE4840U-Group13/Lab#01 assignment material$ openssl enc
-d -aes-192-ecb -in cipher-3.txt -out newtext-3.txt
enter aes-192-ecb decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
kalid@kalid-virtual-machine:~/Documents/Lab-S0FE4840U-Group13/Lab#01 assignment material$ 

```

-des-ed3-cbc encryption :

```

kalid@kalid-virtual-machine:~/Documents/Lab-S0FE4840U-Group13/Lab#01 assignment material$ openssl enc
-e -des-ed3-cbc -in OpenSSL.txt -out cipher-4.txt
enter des-ed3-cbc encryption password:
Verifying - enter des-ed3-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
kalid@kalid-virtual-machine:~/Documents/Lab-S0FE4840U-Group13/Lab#01 assignment material$ 

```

Decryption:

```
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$ openssl enc  
-d -des-ede3-cbc -in cipher-4.txt -out newtext-4.txt  
enter des-ede3-cbc decryption password:  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$
```

Conclusion: Each chypher looks silmar but looking at them closely are each much different. Theres no distinct difference between them though.

Task 2: Encryption Mode – ECB vs. CBC

Display the encrypted picture using any picture viewing software

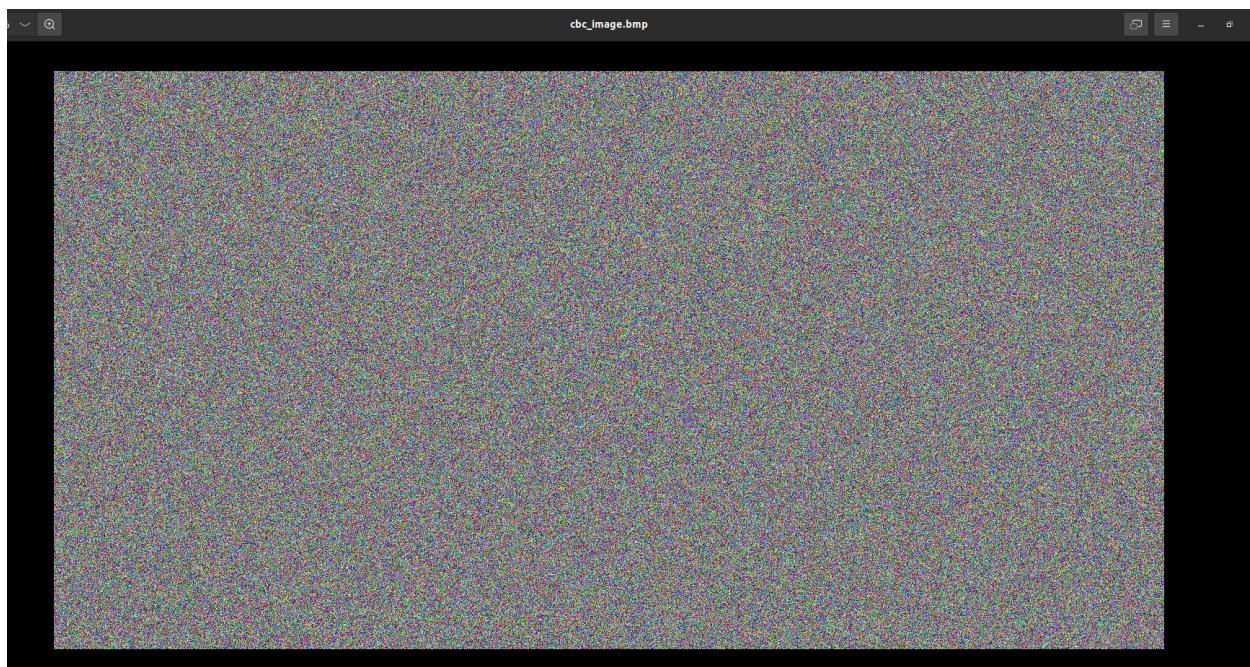
FCB

```
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$ openssl enc  
-e -aes-128-ecb -in image.bmp -out image1.bmp  
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.
```



CBC:

```
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$ openssl enc  
-e -aes-128-cbc -in image.bmp -out image2.bmp  
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.  
kalid@kalid-virtual-machine:~/Documents/Lab-SOFE4840U-Group13/Lab#01 assignment material$
```



Can you derive any useful information about the original picture from the encrypted picture?

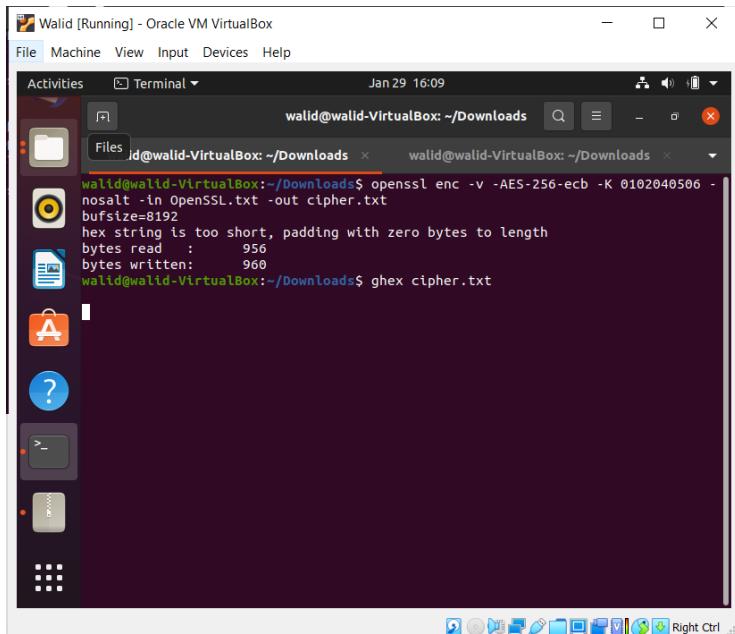
In the ECB image you can slightly make out the words ubuntu but other then that image is hidden, in the CBC you can see any resemblance.

Please explain your observations.

ECB: seems to scramble the image in blocks or patches according to similar pixels or shapes because were still able to see the overall shape of the image.

CBC: completely scrambles the whole image making it unrecognizable.

Task 3: Encryption Mode – Corrupted Cipher Text



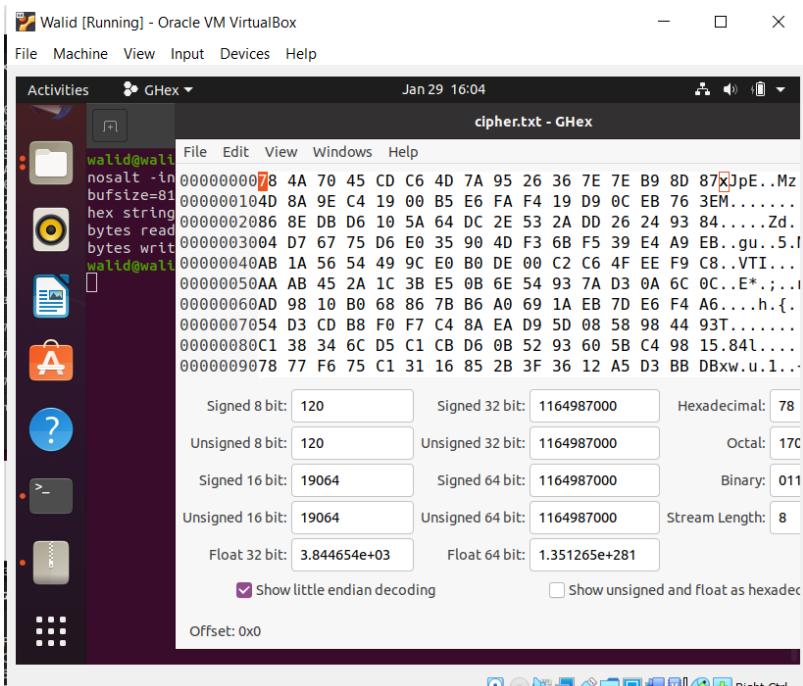
The screenshot shows a Linux desktop environment with a dark theme. A terminal window is open, showing the command:

```
openssl enc -v -AES-256-ecb -K 0102040506 -nosalt -in OpenSSL.txt -out cipher.txt
```

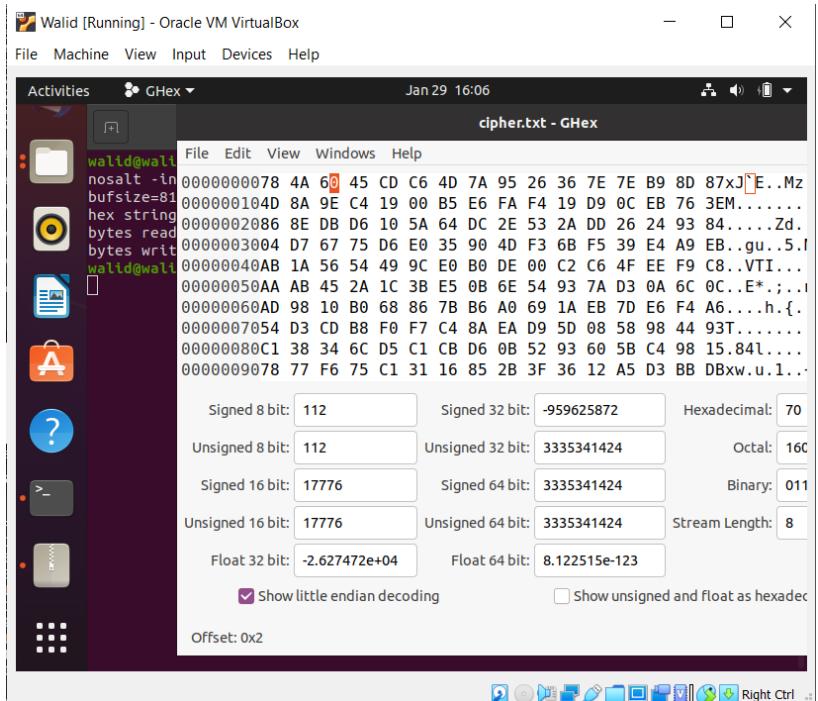
The output of the command is displayed:

```
bufsize=8192
hex string is too short; padding with zero bytes to length
bytes read : 956
bytes written: 960
walid@walid-VirtualBox:~/Downloads$ ghex cipher.txt
```

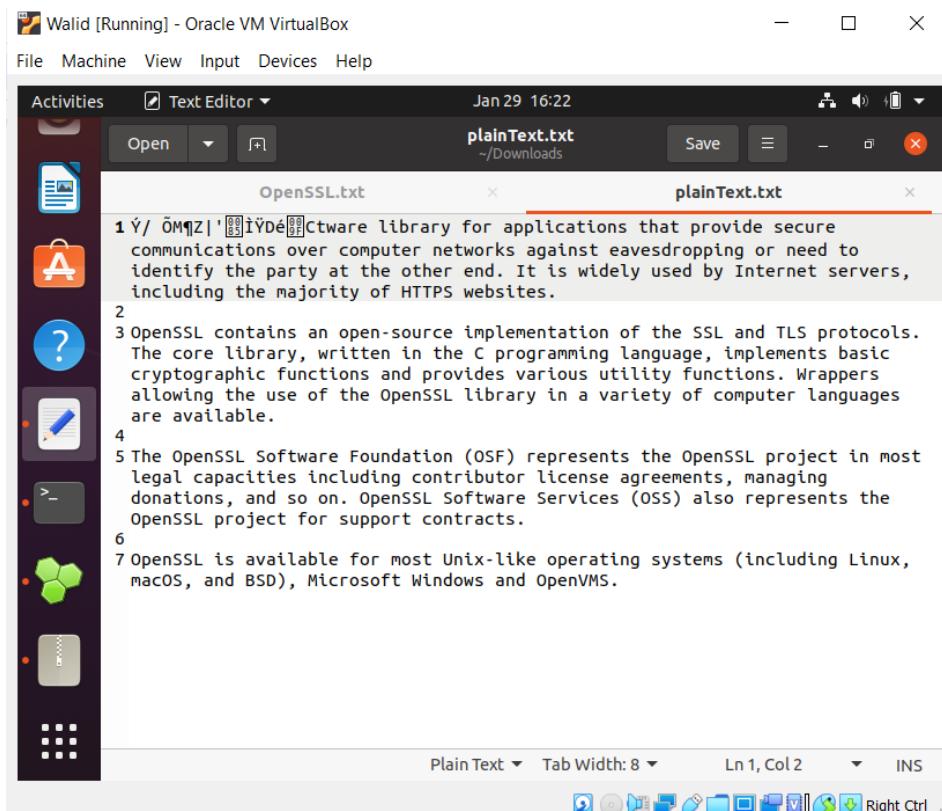
```
walid@walid-VirtualBox:~/Downloads$ openssl enc -d -v -AES-256-ecb -K 0102040506 -nosalt -in cipher.txt -out plainText.txt  
bufsize=8192  
hex string is too short, padding with zero bytes to length  
bytes read : 960  
bytes written: 956  
walid@walid-VirtualBox:~/Downloads$
```



Ghex Editor Before



Ghex Editor After



PlainText decryption

Cipher Text

(1) How much information can you recover by decrypting the corrupted file if the encryption mode is ECB, CBC, CFB, or OFB, respectively? Please explain why. What is the implication of these differences?

When operating in ECB mode, a block cipher that sends a single value at a time is used. This indicates that the same key is used to decrypt each block one at a time. This may be used to XOR the previous y bits of the ciphertext with the x bits of the plaintext to encrypt the blocks. While this is happening, n bits at a time can be processed using cypher feedback. The encryption technique takes the previous ciphertext as input and uses it to generate a pseudo random output. To create an output unit of ciphertext, the plaintext file and the key are used. Last but not least, the structure of the output feedback is the same except for the input to the encryption method is the output of the previous data standard.

ECB - blocks are decrypted in single instances with the same key

CBC- blocks are encrypted

CFB-uses a block cipher as a component of a random number generator

OFB- Similar to CFB mode and is an AES block cypher mode

Task 4: Pseudo-Random Number Generation

Please generate a 20 bytes random password in base64 format and print it on the terminal.

Please generate a 20 bytes random password in base64 format in the output.txt file and compare it to a 20 bytes random password in hex format saved in output1.txt.

Please explain your observations.

```
walid@walid-VirtualBox:~/Downloads$ openssl rand -hex 20  
efc526cd015f19e4760c96c037f189b496bbf3f8  
walid@walid-VirtualBox:~/Downloads$ openssl rand -out output.txt -base64 20  
walid@walid-VirtualBox:~/Downloads$ openssl rand -out output1.txt -hex 20  
walid@walid-VirtualBox:~/Downloads$ █
```

The screenshot shows a desktop environment with two terminal windows and a file manager window.

- File Manager:** Shows three files: OpenSSL.txt, plainText.txt, and output1.txt. The content of output1.txt is: `1 3e39c4939b1b7b41a285a42e8e15d53de565ecb7`.
- Terminal 1:** Shows the command `openssl rand -base64 30` being run twice, resulting in different outputs:


```
walid@walid-VirtualBox:~/Downloads$ openssl rand -base64 30
L3A0m7C/vyK9tKd9v0IMeZm8rQkHeiKhFbj1wyNx
walid@walid-VirtualBox:~/Downloads$ openssl rand -base64 30
xnHDFZs4Cy7SvFg7rnehsFPIaqG322Ko3LPvH5Vn
walid@walid-VirtualBox:~/Downloads$
```
- Terminal 2:** Shows the command `openssl rand -hex 30` being run twice, resulting in different outputs:


```
walid@walid-VirtualBox:~/Downloads$ openssl rand -hex 30
1 F5EOA/zy3RupYmw5vK+HI8u4hi8=
walid@walid-VirtualBox:~/Downloads$
```

If you generate two random passwords in base64 format with 30 bytes, would it be the same? Explain why?

hex passwords only contain lowercase letters and base64 passwords contain both upper and lowercase letters. Therefore, two randomly generated base64 passwords with 30 bytes would not be identical. Also, Hex passwords are longer.

Task 5 A: Get Pseudo Random Numbers from /dev/random (Bonus)

Task 5 B: Get Random Numbers from /dev/urandom