Please include the following in your lab writeup:

- Lab number, your full name and Student ID.

- Clearly labelled answers to the questions (Core 1, Challenge 99, etc).

- Report is submitted in electronic form as a PDF file.

LAB NUMBER: 1

FULL NAME: Elisha Jones

STUDENT ID: 300573902

--------------------------------------------------------------

\*\*CORE TASK 1\*\*

cashmere-lounge% history

1 cd

2 ls

3 cd Desktop

4 ls

5 cd LabWork

6 ls

7 cd Cybr171

8 ls

9 mkdir cybr171-lab1

10 ls

11 cd cybr171-lab1

12 ls

13 curl -O https://www.gutenberg.org/files/36/36-0.txt

14 ls

cashmere-lounge%

Book name is The War of the Worlds by H.G. Wells

\*\*COMPLETION TASK 1\*\*

- Briefly describe what each of the following commands do: `ls`, `more` and `tail`.

- ls list directory contents.

- list information about the files (current directory is default).

- more is the file perusal filter for crt viewing.

- more is a filter for paging through text one screenshot at a time.

- tail outputs the last part of a file.

- Print out the last 10 lines of each file to standard input.

cashmere-lounge% ls -l

total 20

drwx------ 2 joneselis1 students 512 Mar 4 13:12 cybr171

drwx------ 4 joneselis1 students 512 Mar 4 16:12 Desktop

drwx------ 2 joneselis1 students 512 Mar 4 13:25 Downloads

drwx------ 2 joneselis1 students 512 Feb 25 2013 private

drwx--x--x 2 joneselis1 students 512 Feb 25 2013 public\_html

cashmere-lounge% tail 36-0.txt

Most people start at our Web site which has the main PG search

facility: www.gutenberg.org

This Web site includes information about Project Gutenberg-tm,

including how to make donations to the Project Gutenberg Literary

Archive Foundation, how to help produce our new eBooks, and how to

subscribe to our email newsletter to hear about new eBooks.

\*\*CORE TASK 2\*\*

- List the command used in your answer and submit the MD5 hashes for both `declaration.bin` and `declaration-dec.txt`.

curl -0 https://ecs.wgtn.ac.nz/foswiki/pub/Courses/CYBR171\_2021T1/Lab1/declaration.txt was used to download the file

cashmere-lounge% openssl enc -aes-128-ecb -pbkdf2 -in declaration.txt -out declaration.bin

enter aes-128-ecb encryption password:

Verifying - enter aes-128-ecb encryption password:

set password as rabbit

cashmere-lounge% openssl enc -aes-128-ecb -pbkdf2 -d -in declaration.bin -pass pass:rabbit for opening

opens file - fist line: He Wakaputanga o te Rangatiratanga o Nu Tireni

cashmere-lounge% md5sum declaration.bin

f808710963dac9d7f619cbbce9d2ed6c declaration.bin

\*\*COMPLETION TASK 2\*\*

- List the commands you use to demonstrate what happens as well as the output from the commands.

Decrypting with another algorithm will produce a different result or output that what wanted and will appear as gibberish.

cashmere-lounge% openssl enc -aes-192-ecb -pbkdf2 -d -in declaration.bin -pass pass:rabbit

sample of output: ï¿½HRzï¿½ï¿½bKï¿½ï¿½!ï¿½Fqï¿½ï¿½ï¿½ï¿½ohï¿½9LVdï¿½ï¿½Ð³ï¿½Ç½]ï¿½N--ï¿½KZ7ï¿½Eï¿½fTSï¿½2ï¿½AÍ½ï¿½cï¿½

ï¿½ï¿½5ï¿½ï¿½ï¿½awÔšï¿½ï¿½kâ–’ï¿½ï¿½ï¿½Rdf/aï¿½ï¿½ï¿½ÍŠÈ„ï¿½ï¿½ï¿½Qrï¿½ï¿½[ï¿½(5ï¿½ï¿½ï¿½ï¿½Vï¿½Yï¿½ ï¿½ï¿½\ï¿½ep{ï¿½Fv#ï¿½hï¿½+ï¿½ï¿½ï¿½ï¿½UIï¿½CtFï¿½ï¿½o;ï¿½ï¿½!ï¿½ËƒEï¿½ï¿½7ï¿½

\*\*CHALLENGE TASK 2\*\*

- Document the process you used to attempt this task and the hidden message that is revealed.

\*\*CORE TASK 3\*\*

- Submit the md5 hashes and the encrypted images.

File downloaded using Curl -O

File encrypted:

barretts% openssl enc -aes-128-ecb -pbkdf2 -in pic\_original.bmp -out pic\_original.ecb.bmp-

enter aes-128-ecb encryption password:

Verifying - enter aes-128-ecb encryption password:

barretts% dd if=pic\_original.bmp of=pic\_original.ecb.bmp bs=1 count=54 conv=notrunc

54+0 records in

54+0 records out

54 bytes copied, 0.00110977 s, 48.7 kB/s

barretts% openssl enc -aes-128-cbc -pbkdf2 -in pic\_original.bmp -out pic\_original.cbc.bmp

enter aes-128-cbc encryption password:

Verifying - enter aes-128-cbc encryption password:

barretts% dd if=pic\_original.bmp of=pic\_original.cbc.bmp bs=1 count=54 conv=notrunc

54+0 records in

54+0 records out

54 bytes copied, 0.00114006 s, 47.4 kB/s

barretts% md5sum pic\_original.cbc.bmp

847ff8f6dc906bdbc5436250eaeeab8b pic\_original.cbc.bmp

barretts% md5sum pic\_original.ecb.bmp

fbd7d602a823b01f9cf105865e97be9e pic\_original.ecb.bmp

\*\*COMPLETION TASK 3\*\*

Answer the following questions:

1. What do you observe about the ECB image? What does this imply about the problem with ECB mode.

The image can still be roughly made out implying that there is a pattern that can be easily discernible and therefore easily decrypted.

2. Explain why using CBC in this case is more secure than ECB and how the image illustrates it.

The main advantage of using CBC over ECB is that ECB results in a lack of image diffusion, which may result in the original image be discernable. On the other hand, CBC encryption uses a pseudo-random encryption, resulting in no clear discernible image being present.

3. Explain why CBC is less robust than ECB with respect to data corruption.

With regards to ECB, each block can be accessed randomly and any loss of data on one block has no effect on the other, meaning that the missing block could still be discernible. CBC on the other hand, the encryption is completely serial so you cannot encrypt a block until the previous one is, meaning that any loss of data will render all blocks of information after the corrupted one completely unencryptable.

\*\*CHALLENGE TASK 3\*\*

- Document your findings and explain how OpenSSL manages to do this while still only requiring knowledge of the original key in order to successfully decrypt the ciphertexts.