Name: Kwa Li Ying (1003833)
CSE Class: CI03

CSE Lab 5 Report

Part 1 Questions

Q1: Try to print to your screen the content of the input files, i.e., the plaintexts, using `System.out.println()`. What do you see? Are the files printable?

Yes. With the help of the BufferReader class, the content of the input files are printable and readable.

Q2: Store the output ciphertext (in byte[] format) to a variable, say `cipherBytes`. Try to print the ciphertext of the smaller file using `System.out.println(new` String(cipherBytes)). What do you see? Is it printable?

I see a chunk of garbage-print or symbols. It is not printable (not human-readable).

Q3: Now convert the ciphertext in Question 2 into `Base64` format and print it to the screen. Is the `Base64` encoded data generally printable?

Yes, the Base64 encoded data is printable. Even though the string does not make sense, it is still ASCII characters.

Q4: Is `Base64` encoding a cryptographic operation? Why or why not?

No. Secrecy is not involved in encoding, since it is just converting data by the use of a code. Cryptography maintains data confidentiality with the use of secret keys. Base64 encoding does not maintain confidentiality, since anyone is able to decode encoded data. Therefore, it is not a cryptographic operation.

Q5: Print out the decrypted ciphertext for the small file. Is the output the same as the output for question 1?

Yes, the output is the same.

Q6: Compare the lengths of the encryption result (in `byte[]` format) for smallFile.txt and largeFile.txt. Does a larger file give a larger encrypted byte array? Why?

Yes, a larger file gives a larger encrypted byte array. For DES, a 64-bit input will result in a 64-bit encrypted output. Thus the size of the encrypted byte array should be proportional input file size (and hence input byte array size). This results in a larger file giving a larger encrypted byte array.

Name: Kwa Li Ying (1003833)
CSE Class: CI03

Part 1 Output

```
Original content:
I've seen the world
Done it all
Had my cake now
Diamonds, brilliant
And Bel Air now
Hot summer nights, mid July
When you and I were forever wild
The crazy days, city lights
The way you'd play with me like a child
Will you still love me
When I'm no longer young and beautiful?
Will you still love me
When I got nothing but my aching soul?
I know you will, I know you will
I know that you will
Will you still love me when I'm no longer beautiful?
I've seen the world, lit it up
As my stage now
Channeling angels in the new age now
Hot summer days, rock 'n' roll
The way you play for me at your show
And all the ways I got to know
Your pretty face and electric soul
Will you still love me
```

```
When I'm no longer young and beautiful?
Will you still love me
When I got nothing but my aching soul?
I know you will, I know you will
I know that you will
Will you still love me when I'm no longer beautiful?
I've seen the world, lit it up
As my stage now
Channeling angels in the new age now
Hot summer days, rock 'n' roll
The way you play for me at your show
And all the ways I got to know
Your pretty face and electric soul
Will you still love me
When I'm no longer young and beautiful?
Will you still love me
When I got nothing but my aching soul?
I know you will, I know you will
I know that you will
Will you still love me when I'm no longer beautiful?
Dear Lord, when I get to heaven
Please let me bring my man
When he comes tell me that you'll let him in
Father tell me if you can
Oh that grace, oh that body
Oh that face makes me wanna party
```

Name: Kwa Li Ying (1003833)
CSE Class: CI03

```
He's my sun, he makes me shine like diamonds
Will you still love me
When I'm no longer young and beautiful?
Will you still love me
When I got nothing but my aching soul?
I know you will, I know you will
I know that you will
Will you still love me when I'm no longer beautiful?
Will you still love me when I'm no longer beautiful?
Will you still love me when I'm not young and beautiful?
<binary data>
<binary data>
o35BINO8D1EFrAhvK+zoMYmEQQnvEA/28qiYk+Y/4SGtMTkXw4xzQTw71QyZpeSB7VIdYid7jtXCwka+S++Fj9lBQy7r1kyrddGWyS4uZ5bR+EOXuUwb5c3TwYRnlLfW5VZy148+iziWyRyJHzPCn22DmjKDu60IKt

I've seen the world
Done it all
Had my cake now
Diamonds, brilliant
And Bel Air now
Hot summer nights, mid July
When you and I were forever wild
The crazy days, city lights
The way you'd play with me like a child
Will you still love me
When I'm no longer young and beautiful?
Will you still love me
```

```
When I got nothing but my aching soul?
I know you will, I know you will
I know that you will
Will you still love me when I'm no longer beautiful?
Dear Lord, when I get to heaven
Please let me bring my man
When he comes tell me that you'll let him in
Father tell me if you can
Oh that grace, oh that body
Oh that face makes me wanna party
He's my sun, he makes me shine like diamonds
Will you still love me
When I'm no longer young and beautiful?
Will you still love me
When I got nothing but my aching soul?
I know you will, I know you will
I know that you will
Will you still love me when I'm no longer beautiful?
Will you still love me when I'm no longer beautiful?
Will you still love me when I'm not young and beautiful?
Length of file shorttext.txt is 1480 and length of file longtext.txt is 17360

Process finished with exit code 0
```

Name: Kwa Li Ying (1003833)
CSE Class: CI03

Part 2

Q1: Compare the original image with the encrypted image. What similarities between them do you observe? Can you identify the original image from the encrypted one?

In the encrypted image, the SUTD logo is still visible, although it is slightly fuzzy and the image is in a different color. The original image is still somewhat identifiable from the encrypted one.

Q2: Why do those similarities exist? Explain the reason based on what you find out about how the ECB mode works.

ECB codes each block of 64 bits independently. Identical plaintext blocks are encrypted into identical ciphertext blocks, thus it does not hide data patterns well. When ECB is used to encrypt a bitmap image which uses large areas of uniform color, even though the color of each individual pixel is encrypted, the overall image may still be discerned as the pattern of identically colored pixels in the original version remains in the encrypted version.

Q3: Now try to encrypt the image using the CBC mode instead (i.e., by specifying " `DES/CBC/PKCS5Padding` "). Compare the result with that obtained using ECB mode). What differences do you observe? Explain the differences based on what you find out about how CBC mode works.

In the encrypted image, the shape of the SUTD logo at the top somewhat resembles the original, but the rest of the image is extremely fuzzy and does not resemble the original at all.

Unlike ECB mode where each block is coded independently, CBC uses the result of encrypting the previous block to encrypt each current block. This explains why the top of the image (start of each column of pixels) still has the outline of the SUTD logo, while the pixels stray further and further from the original as we move down the image.

Q4: Do you observe any issue with image obtained from CBC mode encryption of " `SUTD.bmp`"? What is the reason for such observation? Can you explain and try on what would be the result if data were taken from bottom to top along the columns of the image? Can you try your new approach on "`triangle.bmp`" and comment on observation?

Since the shape of the logo at the top is still somewhat recognisable, a malicious user with the relevant knowledge can still discern the information in the image. The reason why the shape is as shown is explained in Q3.

If the data were taken from bottom to top along the columns of the image, for SUTD.bmp, the image would be less well-shaped since the shape (of the smaller-font text) at the bottom of the image is not as well defined.

Name: Kwa Li Ying (1003833)
CSE Class: CI03

For triangle.bmp, the transition between dots to lines are inverted. For top to bottom, the top of the image starts with lines, then become dots when it enters the triangle (black to white). For bottom to top, the bottom of the image starts with lines, remain as lines but change slightly as it enters the triangle, then become dots as it leaves the triangle (white to black).

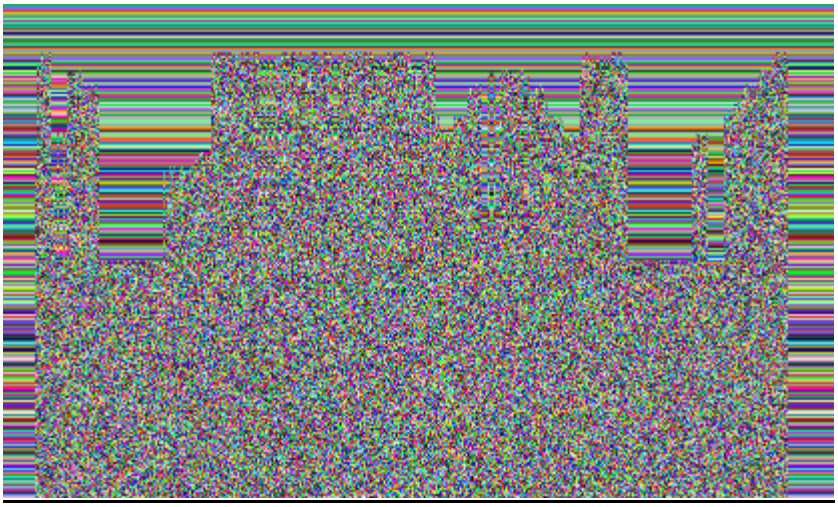
More generally, greater transition between shapes and colors will be more obvious at the bottom of the image if the data is taken from bottom to top.

Name: Kwa Li Ying (1003833)
CSE Class: CI03

Part 2 Output

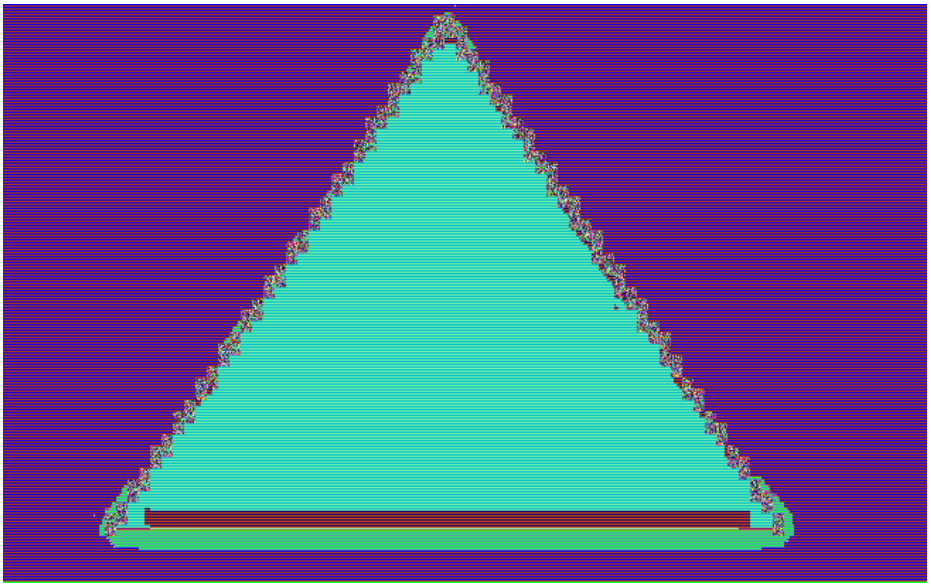
SUTD.bmp using ECB

SUTD.bmp using CBC

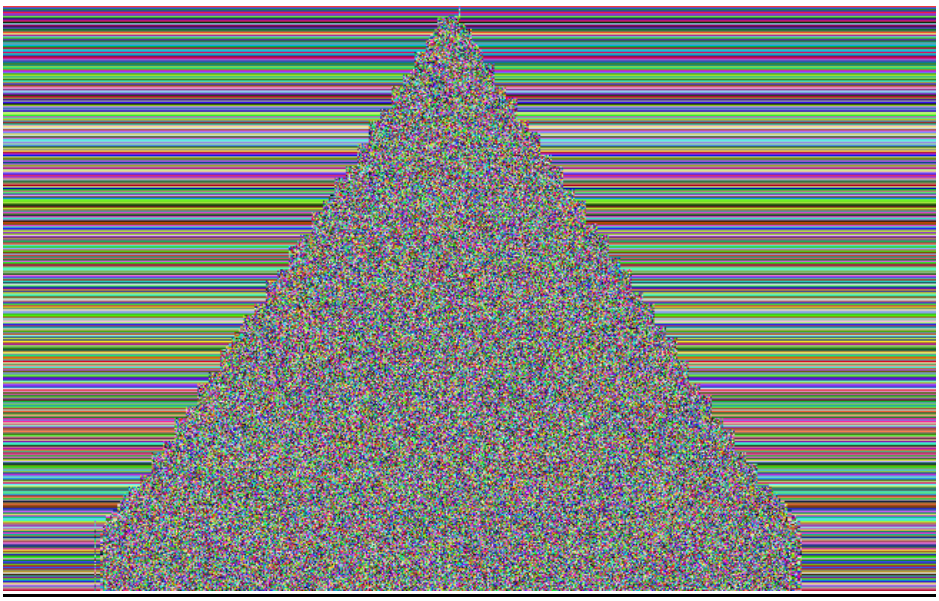


Name: Kwa Li Ying (1003833)
CSE Class: CI03

triangle.bmp using EBC



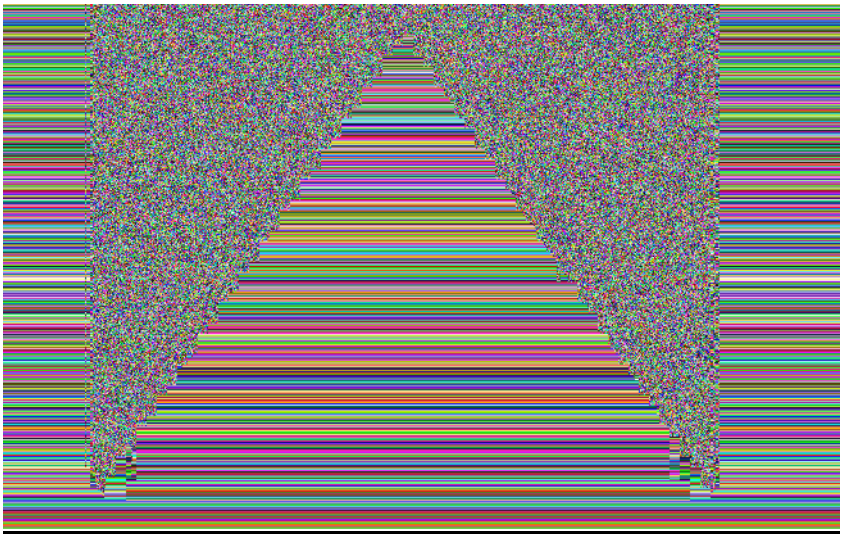
triangle.bmp using CBC



Name: Kwa Li Ying (1003833)
CSE Class: CI03

SUTD.bmp using CBC (data taken from bottom to top)

triangle.bmp using CBC (data taken from bottom to top)



Name: Kwa Li Ying (1003833)
CSE Class: CI03

Part 3

Q1: What are the sizes of the message digests that you created for the two different files? Are they the same or different?

They are the same. Each digest has a size of 16 bytes.

Q2: Compare the sizes of the signed message digests (in `byte[] encryptedBytes = eCipher.doFinal(data.getBytes());` format) for smallFile.txt and largeFile.txt. Does a larger file size give a longer signed message digest? Why or why not?

The sizes of the both signed message digests are the same. Each signed message digest is 128 bytes.

A larger file size does not give a longer signed message digest. Before RSA encryption, both are hashed to produce a message digest of fixed size (16 bytes in this case). Since the digest will have the same size despite the size of the file, the encryption will produce an encrypted byte array of fixed size. Thus the size of the file will not affect the length of the output signed message digest.

Name: Kwa Li Ying (1003833)
CSE Class: CI03

Part 3 Output

```
Original content:
I've seen the world
Done it all
Had my cake now
Diamonds, brilliant
And Bel Air now
Hot summer nights, mid July
When you and I were forever wild
The crazy days, city lights
The way you'd play with me like a child
Will you still love me
When I'm no longer young and beautiful?
Will you still love me
When I got nothing but my aching soul?
I know you will, I know you will
I know that you will
Will you still love me when I'm no longer beautiful?
I've seen the world, lit it up
As my stage now
Channeling angels in the new age now
Hot summer days, rock 'n' roll
The way you play for me at your show
And all the ways I got to know
Your pretty face and electric soul
```

```
Will you still love me
When I'm no longer young and beautiful?
Will you still love me
When I got nothing but my aching soul?
I know you will, I know you will
I know that you will
Will you still love me when I'm no longer beautiful?
Dear Lord, when I get to heaven
Please let me bring my man
When he comes tell me that you'll let him in
Father tell me if you can
Oh that grace, oh that body
Oh that face makes me wanna party
He's my sun, he makes me shine like diamonds
Will you still love me
When I'm no longer young and beautiful?
Will you still love me
When I got nothing but my aching soul?
I know you will, I know you will
I know that you will
Will you still love me when I'm no longer beautiful?
Will you still love me when I'm no longer beautiful?
Will you still love me when I'm not young and beautiful?
Length of file shorttext.txt is 16 and length of file longtext.txt is 16
Size of signed message digest for shortttext.txt is 128 and size of signed message digest for longtext.txt is 128
```

```
MPi5eoOpnDJvNvVErcj8GpNScNhebsCf22SrsPBcxstUexVf1LQRjnoYLwplSY0uvwoiCCPng6rue/GcAk/JM/wSrCOGBPYHl8c2KVBrJprWuJC0RMW46W+i8YJFQJL4h0hpyKTz2+SbXfM/ASogbio/LV/oMSTdoPC2
Original digest is UERkP8pWz1n9gUPf+l4TyQ== and decrypted message is UERkP8pWz1n9gUPf+l4TyQ==

Process finished with exit code 0
```