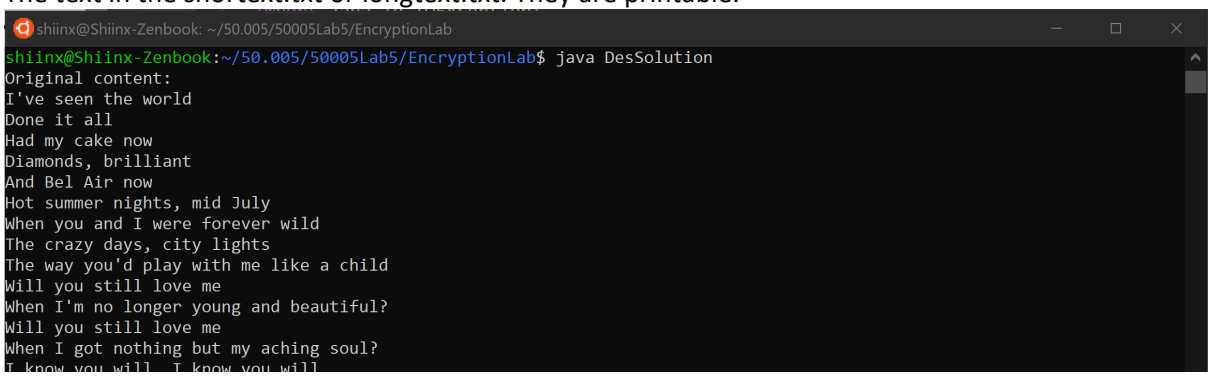
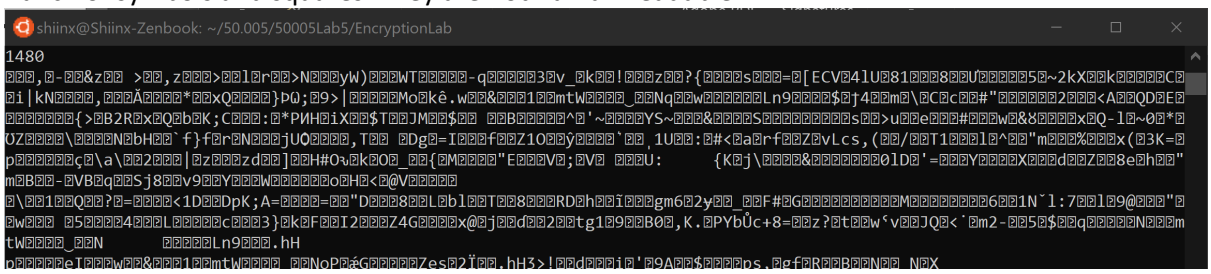
Part 1

Question 1:
The text in the shortext.txt or longtext.txt. They are printable.



Question 2:
Bunch of symbols and squares. They are not human-readable.



Question 3:
They are printable.

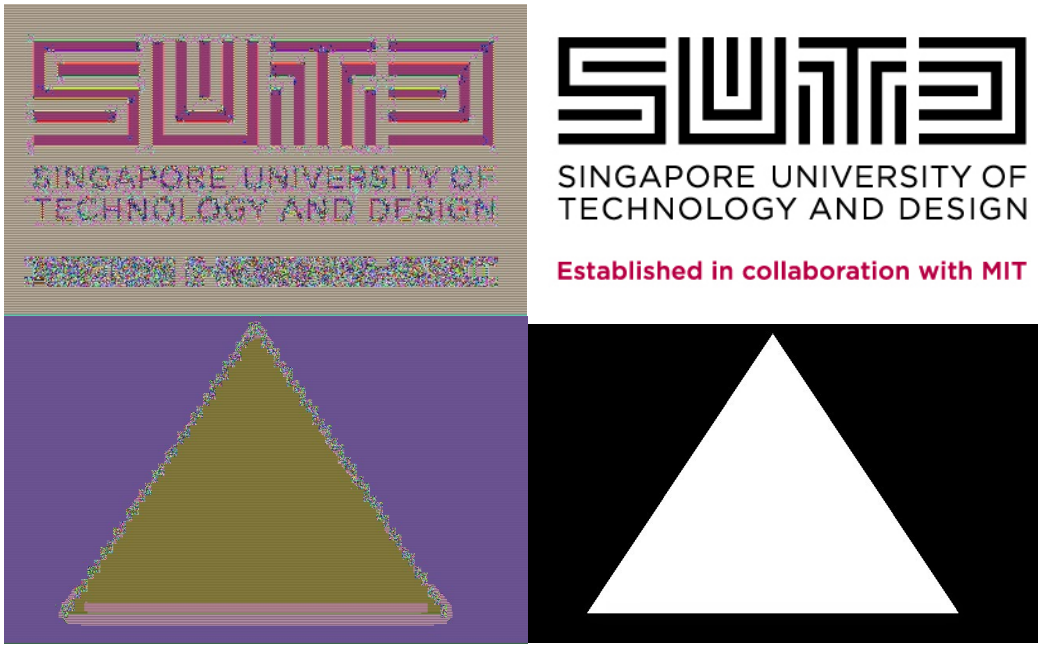
Question 4:
No. There is no secret key involved in decoding or encoding. Usually involves standard formats. It is not an encryption or decryption.

Question 5:
Yes.

Question 6:
Yes, smalltext.txt is 1480, longtext.txt is 17360. In this case, the difference in size of encrypted byte array depended on input and padding hence, larger input file larger array.

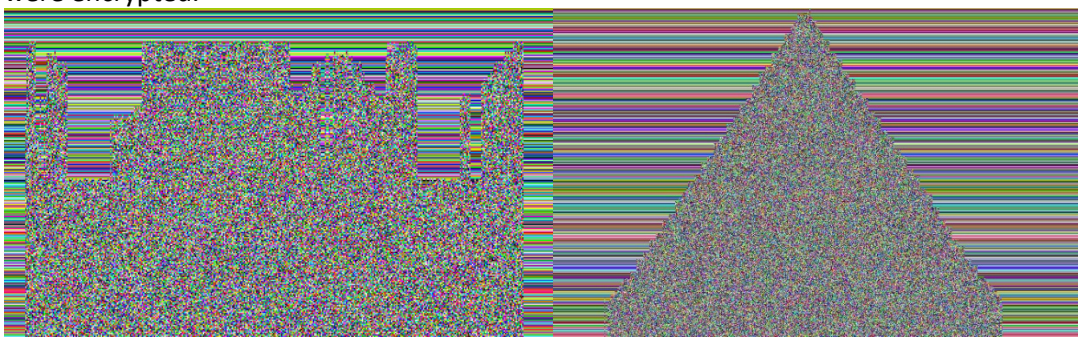
Part 2

Question 1:
The outlines are similar. It is mostly identifiable. Most of the letters in the image are still identifiable. Shapes are easily identifiable.



Question 2:
ECB, electronic codebook, encrypts identical plaintext blocks into identical cipher blocks which means that although the color of the image changed, the “pattern” of it doesn’t.

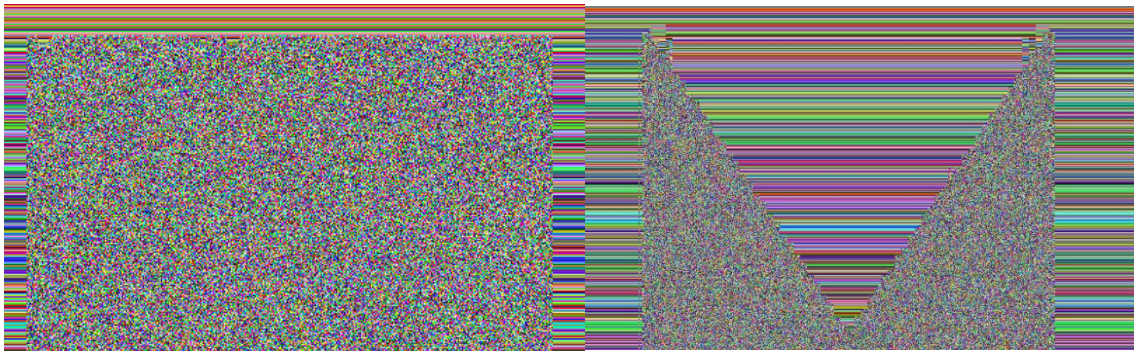
Question 3:
The background that is a single color is now colored stripes and the outline of SUTD can no longer be seen. However, the outline of the triangle can still be seen.
CBC, cipher block chaining, encrypts by XORing each block of plaintext with the previous ciphertext block before encrypting. Hence, the text to be encrypted also depends on the previous blocks that were encrypted.



Question 4:
There are weird gaps. It might be because if read from top to bottom, the first few are constant patterns of black and white, resulting in somewhat similar ciphertext. The 'S' & 'D' consist mainly of horizontal lines (hence straight line), whereas the U consist mostly of vertical lines(hence fuzzy).

If taken from bottom to top, therefore instead of getting previous cipher text from on top, it is now getting it from below, which would change the image shown.

The triangle image is an upside down & inverted version of the top to bottom version.



Part 3

Question 1:
16 for shorttext.txt
16 for longtext.txt
They are the same.

Question 2:
Both are the same size, 128. Output size is dependent on the key and not the input text. Hence, since both are signed with keys of same size, 1024 bit, they will give the same output size.

Console output for Part 3 shorttext.txt

Console output for Part 3 longtext.txt