

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.



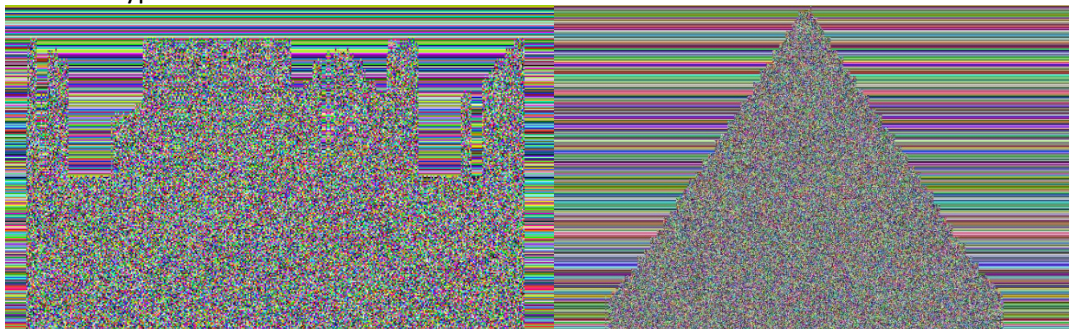
Question 2:

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.

```
shiinx@Shiinx-Zenbook: ~/50.005/50005Lab5/EncryptionLab
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?
16
128
YPfD7Jm34ZuzQMy5pCPBM64Z2Gu7kdMbApcR8Ac3xmr28uB5rLjnNNBn/cP+XRMKQDcwveB7BikDrDpABoNWItJ7Ts0j08iNKh
Ki+BTxKjhlxNKwGyHIedLCI0AXxFp3IhokZKTEg7jawnIm10cJ+Aye6UtrMpWzOuJUUrYmbIuw=
UERkP8pwz1n9gUPf+l4TyQ==
same
shiinx@Shiinx-Zenbook: ~/50.005/50005Lab5/EncryptionLab$
```

Console output for Part 3 shorttext.txt

```

shiinx@Shiinx-Zenbook: ~/50.005/50005Lab5/EncryptionLab
cavalierly must be a careless man. Neither is it a very far-fetched
inference that a man who inherits one article of such value is pretty
well provided for in other respects."

I nodded, to show that I followed his reasoning.

"It is very customary for pawnbrokers in England, when they take a
watch, to scratch the number of the ticket with a pin-point upon the
inside of the case. It is more handy than a label, as there is no risk
of the number being lost or transposed. There are no less than four
such numbers visible to my lens on the inside of this case.
Inference,--that your brother was often at low water. Secondary
inference,--that he had occasional bursts of prosperity, or he could
not have redeemed the pledge. Finally, I ask you to look at the inner
plate, which contains the key-hole. Look at the thousands of scratches
all round the hole,--marks where the key has slipped. What sober man's
key could have scored those grooves? But you will never see a
drunkard's watch without them. He winds it at night, and he leaves
these traces of his unsteady hand. Where is the mystery in all this?"

"It is as clear as daylight," I answered. "I regret the injustice
which I did you. I should have had more faith in your marvellous
faculty. May I ask whether you have any professional inquiry on foot
at present?"

"None. Hence the cocaine. I cannot live without brain-work. What else
is there to live for? Stand at the window here. Was ever such a
dreary, dismal, unprofitable world? See how the yellow fog swirls down
the street and drifts across the dun-colored houses. What could be
more hopelessly prosaic and material? What is the use of having
powers, doctor, when one has no field upon which to exert them? Crime
is commonplace, existence is commonplace, and no qualities save those
which are commonplace have any function upon earth."

I had opened my mouth to reply to this tirade, when with a crisp knock
our landlady entered, bearing a card upon the brass salver.

"A young lady for you, sir," she said, addressing my companion.

"Miss Mary Morstan," he read. "Hum! I have no recollection of the
name. Ask the young lady to step up, Mrs. Hudson. Don't go, doctor.
I should prefer that you remain."
16
128
HDK+NuuADiLUXoKirtzusXza7u4dvx52niuHsNczOZLEup+owOf79yatPcnKd/3QmKq0WFWLCeKGExayJIziVmD7pygWMP/qh
LkAETM0s5HT37QXaXZ7ZN6mG0MMFFOp807uG3lGLiRyMgyn3UirSKT+LVawvMcv+MqPN4/yfo=
oH15w3qFY1xnyNE0Z8+kTQ==
same
shiinx@Shiinx-Zenbook:~/50.005/50005Lab5/EncryptionLab$

```

Console output for Part 3 longtext.txt