**Sidharth Praveenkumar**

**1003647**

**Computer Systems Engineering 50.003 Lab 5 Report**

**Part 1**

Answer 1:  
Printing the plaint text contents of the file shows the actual contents of the file on the console. It is segmented and formatted properly due to the presence of newline characters. Yes, the files are printable.  
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?*

Answer 2:  
The ciphertext/output after encrypting the smallfile is not human readable, because this is actually the hash code of the byte array and contains special characters as well as alphanumeric characters. Yes, it is printable.  
Content: [B@11028347

Answer 3:  
Yes, it is printable and readable. But the base64 text is meaningless as it contains an unordered sequence of special characters and alphanumeric characters.  
Content: 

Answer 4:  
Base64 encoding is not a cryptographic operation. In general, encoding is only a way to change the scheme of a format of data into another and will provide deterministic outputs and has no factor of security involved. Data can be encoded from one format to another by anyone. A cryptographic operation has a security factor involved that allows only specific people with the correct “key” to decipher the given data.

Answer 5:  
Yes. the decrypted string output is the same as the original contents of the file.   
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?*

Answer 6:  
The length of the encrypted byte format output is larger for the large file. Thus, yes, a larger file does give a larger encrypted byte array (17360 for the large file and 1480 for the short file). However, when you print the byte array itself, you get similar outputs ([B@11028347 and [B@1055e4af) because these are the hash codes of the byte array representation.

**Part 2**

Answer 1:  
The similarities exist such that the outline and the contents are still readable by the human eye; ie: we can still identify the contents of the image. The only thing that appears to be different are the pixels as the colours are completely distorted and unlike the original one. But the overall scheme and structure of the image still look like the original image.

Answer 2:  
These similarities exist because while encrypting using the ECB mode, same blocks (every 8 bytes) are always outputted as the same block of encrypted text. Because of this, regions of the image that share the same RGB value (or repetitive patterns in that image) will look similar even after the encryption because ECB yields the same output for all those regions.

Answer 3:  
When encrypting the image using CBC mode, the image is completely unrecognizable, unlike when it was done using ECB mode. In CBC mode, each block of plaintext is XORed with the previous cipher text block before being encrypted. This eliminates the possibility of same block yielding same encrypted text and makes it difficult to catch the repetitive patterns that may occur in the image.

Answer 4:

While using CBC, the SUTD content of the image is not visible because the way this algorithm fucntions does not allow for same encrypted byte for the repeated patterns. While doing it from top to bottom for the triangle, we see that the triangle is inverted and then the noise is applied on the image, because the pixels at y are now at (len-y), making it vertically shifted.

**Task 3**

Answer 1:  
The sizes of the digests for the long and short text files are the same (16). The lengths are the same, regardless of the size of the input because md5 algorithm has a compression function that is responsible for compressing the input, such that a domain extender can map the hash function across any length input.

Answer 2:  
Both the files give the same size signed message digest(128). This is because the input that is encrypted is always of same length (as discussed in previous answer, digests always output a fixed length sequence), so the output that is the encrypted digest will also contain equal lengths. This is true because through Task 1, we observed that larger the input to be encrypted, larger is the encrypted text. So, the only way that two encrypted digests are of equal length are if the inputs are the same length, and that is given true with length 16 as in answer 1.