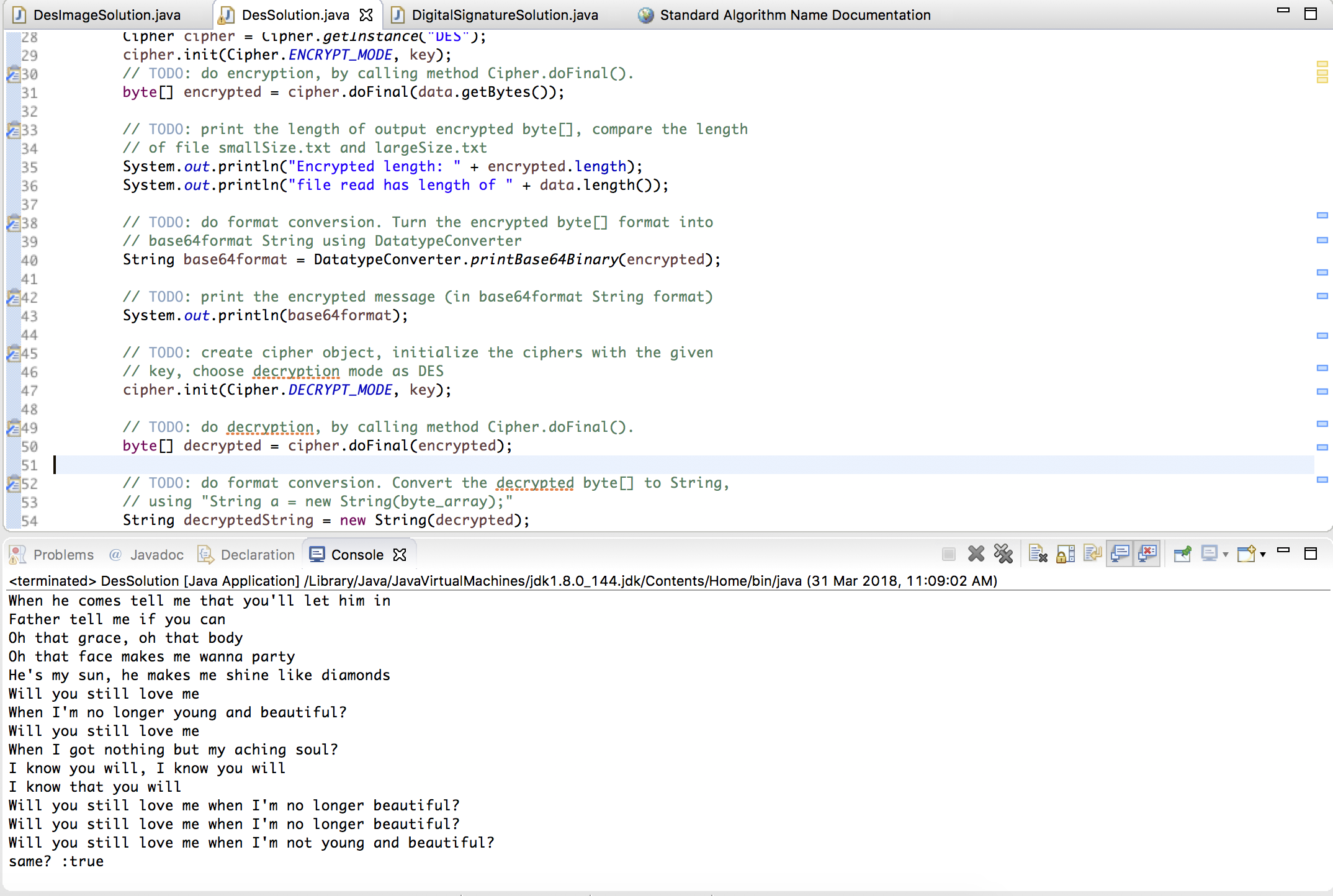
Task 1



Q1: The files are printable because they are still in plaintext.

Q2: I see gibberish. It is not printable.

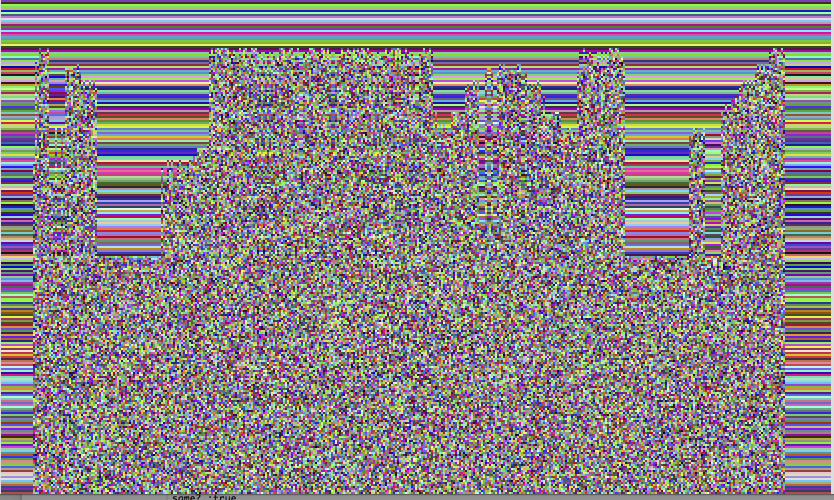
Q3: Base64 encoded data is generally printable.

Q4: Base64 encoding is not a cryptographic function as it only represents binary data using printable characters. It can be easily decoded.

Q5: Yes, it is the same output.

Q6: Naturally, the length of the encryption result for the larger file is longer than the smaller file. This is because there is more data to be encrypted and hence a larger array is created to store all the encrypted data.

Task 2



CBC



ECB

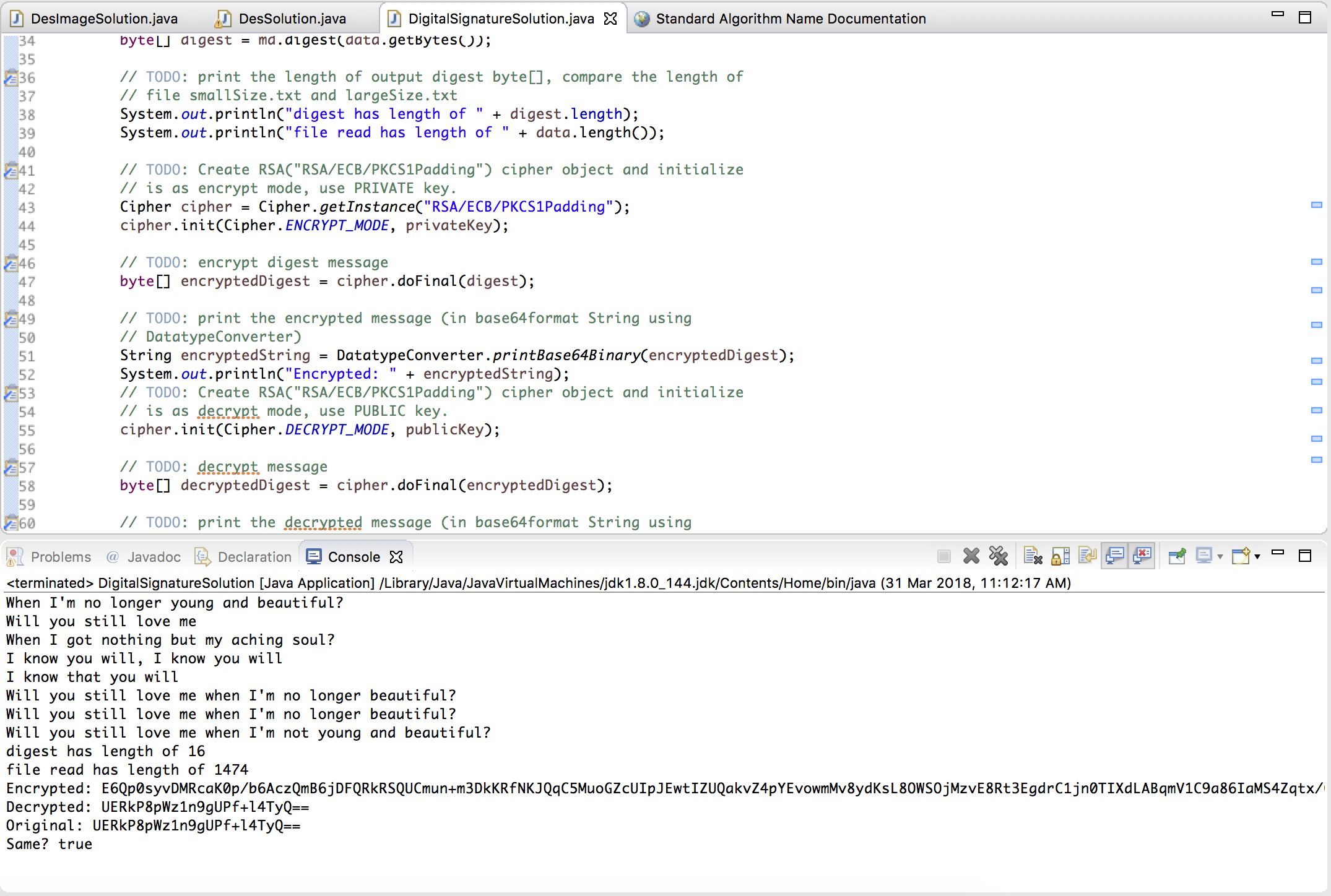
Q1. We can still identify the SUTD logo from the encrypted image. I could identify the original image from the encrypted one.

Q2. ECB encrypts each data block individually, and as identical blocks are encrypted into identical cipher blocks, it does not hide data patterns well. There is a lack of diffusion across the cipher blocks, hence the color patterns on the image are still visible.

Q3: The CBC encrypted image is not discernable and looks completely different from the original image. This is because CBC processing encrypts each data block in relation to the previous cipher block; each block is XORed with the previous cipher block before being encrypted. This way, each cipher block depends on previous blocks and does not retain any visible patterns because of this – the colors get modified heavily based on the previous encrypted colors.

Q4: When the order of fetching data is reversed, it does not affect the result too much as the CBC is done on a row by row basis; if the order is changed from top to bottom to bottom to top, there is no change as each encrypted row is independent of each other. This means that images that have a vivid shape (like the triangle) does not get encrypted well enough: the outline of the triangle is still visible.

Task 3



Q!: The message digests have the same sizes.

Q2: They both have the same sizes. A larger file does not give a longer signature, as it is not dependent on the item to be signed but rather dependent on the length of the key.