Part 1

Question 1
I see readable texts. Yes, the files are printable.

Question 2
I see weird characters e.g. E遢[)MJn:M_B}qд
No, the file is not printable.

Question 3
Yes, it is generally printable.

Question 4
No, it is not a cryptographic operation. Encrypting is more maintaining data confidentiality and requires a secret key. Base64 encoding uses an algorithm to maintain data usability without keeping it confidential.

Question 5
Yes, the output is the same.

Question 6
Yes, the larger file has a larger encrypted byte array. Every character in the file is encrypted into another character, so a larger file having more characters will result in a larger encrypted byte array.

Part 2

Question 1
The shape and outline remains the same. Only the colours differ. Yes, the original image can be identified from the original one.

Question 2
ECB divides the data into blocks and encrypts each one separately. As a result, it does not hide data patterns well. Each individual pixel of the image might be encrypted, but the image overall is not.

Question 3
The image is indiscernible. One cannot identify the original image from it. CBC divides the data into blocks, and each block is XOR-ed with the previous cipher text block before being encrypted. This results in a largely unique encryption that does not maintain the data patterns.

Part 3

Question 1
The sizes of both message digests are both 16 bytes.

Question 2
Both files result in the same size of signed message digest. MD5 is a hash function that results in a 128-bit hash value. Since both files are hashed using MD5, the resulting message digests will both be 128-bits, or 16-bytes. Encryption maintains the message size, hence, the signed message digests are the same size.