Assignment 4
SEng 360

Braden Simpson
braden@uvic.ca
V00685500

1)
The intialization vector(IV) is used when encrypting multiple blocks. Without using an IV, each block is encrypted using the same key, and results in a weak encryption strategy.
This is seen in ECB(electronic codebook) block mode. Other more robust block modes such as Cipher block chaining (CBC) use the encrypted cipher text of the previous block
to be used as another element of randomness in the encryption. This is called the Initialization Vector, and when starting the encryption a randomized IV must be given, and each
successive block encryption produces the next block's IV. See the wikipedia picture to explain about IV's and CBC here.

http://upload.wikimedia.org/wikipedia/commons/d/d3/Cbc_encryption.png

2)
An example of a block mode that doesn't require an IV is ECB. That would result in a poor encryption strategy. However, entering an empty IV for a different, more robust block
mode such as CBC, would result in security problems. If the potential attacker got hold of a ciphertext message and the corresponding plaintext, then they will be able to know
when any other messages are sent with the same starting block. In terms of frequency analysis, the attacker could perform pattern analysis on the messages and find out
information about the messages making the encryption insecure.

3)
Decrypted text: Mary had a little key (It's all she could export), and all the email that she sent was opened at the Fort.
See *src.main.Part1* for the source.

4)
At the **8309032** try with key: **huUwkP9ioJqBAK2ej/5JqA==**
Decrypted text: Mary had a crypto key, she kept it in escrow, and everything that Mary said, the Feds were sure to know.
see *src.main.Part2* for the source