Lab 2 Qusetions:

Q1 Did the modified Caeser cypher from lab 1 make it any harder to crack using frequency analysis –
why?

A1
No,the Caeser Cypher from lab 1 is more easy to crack by using frequency analysis, because the Caeser Cypher it only using 1 key to encode, so the cypher is more regular than polyalphabetic Caeser cypher from lab 2. Therefore, you don't have to guess how many key it is. It can just use frequency analysis to break it straight away.

Q2
Outline how your code might differ, if you were attemping to crack the vignere cypher rather than a polyalphabetic cypher?

A2
I think I might write the same code for crack those two cypher, because to crack those two cypher is depends on they key length, when we knows the key length we can use frequency analysis to break easily. but for vignere cypher, the key is build in English, if they use
the simple key like "abc" names etc, we can try to crack the key first by bruteforce, if not success we can crack by using frequency after.

Q3
What is the key difference between a block cypher and a stream cypher?

A3
block cypher and stream cypher they both are symmetric key cypher, the difference between a block cypher and a stream is the block cypher will sprite the plain text into same length of block, each block is encrypted using a determined algorithm and a symmetric key. For stream cypher, encryption and decryption both use the same pseudo random stream as the key, and the plaintext data is encrypted with the key data stream at every time, and the cipher text data flow is obtained.

Q4
Decypher the following message, that was encyphered using the Vignere cypher and the keyword "HOUSE"

A4
THECH AIRMA NOFTH EFEDE RALRE SERVE BOARD SAIDY ESTER DAYTH ATATA XINCR EASEI SNEED EDNOW

Q5
What is the key difference between a cryptanalysis and a bruteforce attack?

A5
the key different between a cryptanalysis and bruteforce is the cryptanalyis refers to looking for the system design, to find a mathematical relationship, for example: according frequency analysis to crack the cryer text, but bruteforce is according to nothing, involves tring every possible combination of characters in order to find the key in order to decrypth an encrypted message.