Topic Questions

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

  No, I think that crack modified Caesar cypher is easier by using frequency analysis compare to lab2.
  Because the modified Caesar cypher was use by only one key, while the polyalphabetic cypher was used probably more than one key. This means that we have to split the cyphertext into unknown numbers of sub-cyphertext, but we don't need to split the cyphertext by using frequence analysis to crack the cyphertext.

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

  When we attempt to crack a polyalphabetic, we try (0…n) numbers of key to crack the cypher text, so we passing the possible numbers of key to method in order to split cyphertext to subcyphertext.
  However, when we attempt to crack a vigenere cypher, we try the length (0…n) of key to crack the cypher text, similarly, we also need to pass the possible length of key to method in order to split cyphertext to sub-cyphertext.
  Therefore, the code difference between the two cypher is that the first case, we need to pass the number of key to "createSubtext function", the second case, we need to pass the length of key to "create Subtext" function.

- What is the key difference between a block cypher and a stream cypher?
  There are serval differences between block cypher and stream cypher by doing some research.

1. For block Cipher, encoding of the plain text is done as a fixed length block one by one. A block for example could be 64 or 128 bits, while, for stream cipher, encoding of plain text is done bit by bit. The block size here is simply one bit.
2. For block cipher, the same key is used to encrypt each of blocks, while, for stream cipher, a different key is used to encrypt each of bits.
3. For block cipher, diffusion factor: output depends on the input in a very complex method. For stream cipher, long period with no repetition
4. For block cipher, uses symmetric encryption and is not used in asymmetric encryption, while, for stream cipher, high speed and low hardware complexity.
5. For block cipher, more secure in most cases, while, for equally secure if properly designed.

- Decipher the following message, that was enciphered using the vignere cypher and the keyword “HOUSE”:
  AVYUL HWLEE UCZLL LTYVI YOFJI ZSLNI ICUJH ZOCVC LGNWV KOSLL HHULE EWHUV LOMWM ZBYWH LRHGA

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

- What is the difference between cryptanalysis and bruteforce attack?

The difference is that cryptanalysis attack a cryptographic system by referring to some relevant things to the cypher text that the cypher designers did not think of. Eg, a mathematic relation or the English frequency table we have used in this lab. These clear things make some computation faster.
However, a brute force is one that does not use any relevant materials and just try to attack the cypher heaps times until it attacks successfully.
In a word, cryptanalysis is always vulnerable to brute force attacks, but if properly designed, which make them practically impossible by arranging for the probability of success to be utterly negligible.