NWEN 243 Frequency Analysis Topic Questions

David Barnett ID: 300313764

Question 1

The modified Caesar cipher from Lab 1 did not make it harder to crack using frequency analysis. Due to the algorithm is just just mapping a clear character to a cipher character, the frequency of the cipher characters can still be used to infer the clear character with frequency analysis.

Question 2

The changes that would be needed is to enter the expected keyword length. Then after that the crack would treat the vignere cipher as a poly-alphabetic cipher. Other optimization could be apply to the algorithm.

Question 3

No, even with the use of Homophones the English language would follow some rules and correlations such as common 'sh','th' and 'ion' that gives hints to the plain text.

Question 4

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

Question 5

So that cryptanalysts could not determine the words length from the cipher text