Comp3260 Assignment 1

Jay Rovacsek and Cody Lewis

April 9, 2018

1 c1

First the frequency graph was observed, which expressed that the cipher war produced by substitution. Next the IC was calculated giving an approximate period, d = 3. Then a kasiski of 17 characters shown that the string ‘agxyvyzmffhjkefie’ occurs in the text 3 times with the gaps 392 and 2024.

$$GCD(2024, 392) : 2024 = 5 \times 392 + 64$$

$$GCD(392, 64) : 392 = 6 \times 64 + 8$$

$$GCD(64, 8) : 64 = 8^2 + 0$$

$$\Rightarrow GCD(2024, 392) = 8$$

Hence the cipher definitely has 8 alphabets. Looking at the frequency graph with 8 alphabets shows that the cipher is Viginere as the letter frequency match the normal graph left to right, they only shift. The key is the letter a is shifted to in each alphabet, which means the key is ‘remember’.

2 c2

The frequency graphs shows that a substitution cipher was used, the IC give an approximate period, d = 10. A Kasiski at 10 gives the gaps of 287, 91.

$$GCD(287, 91) = 7$$

Hence there are definitely 7 alphabets in the cipher. Solving for the key to this cipher is very similar to the previous one, only the frequency graph is backwards meaning it is a Beauford cipher. Matching each letter to the letter in place of a in each alphabet, gives the key ‘triumph’.

3 c3

c3 was found to be a General substitution cipher with the key: ‘mcafrgyjhkdplqiutvexbzwsno’

4 c4

c4's IC indicated that it is monoalphabetic, and its frequency graph matches that of normal English, hence c4 is a Transposition cipher. The first 3 letters of the cipher text is 'hte' according to digraphs is probably the message 'the', thus the cipher is a row Transposition. Through some anagramming further through the message the words 'enigma machine was' were found. After a bit of evaluation of the pattern against ciphertext and message the key '2,1,4,6,5,4' or 'bafced' was found to decipher c4 into the message.
The key was determined to have a length of x where:

$$xmod(6) = 0$$

This was determined via Kasiski analysis performed on the ciphertext resulting in strings 'ahcmni' and 'cyretp' occuring far more often than should be expected. Analysing the inital position and repeated position the key length was estimated with more accuracy given:

$$GCD(492, 414) = 6$$