ELEC6242 Cryptography Coursework

Sam Jones

March 8, 2021

Contents

1 Outline **1**

2 Cipher 1 **2**
2.1 Solution for Cipher 1 2
2.2 Cipher 1 Cryptanalysis 2

3 Cipher 2 **3**
3.1 Solution for Cipher 2 3
3.2 Cipher 2 Cryptanalysis 3

4 Cipher 3 **4**
4.1 Solution for Cipher 3 4
4.2 Cipher 3 Cryptanalysis 4

5 Appendices **5**
5.1 Appendix A 5
5.2 Appendix B 5
5.3 Appendix C 5

1 Outline

2 Cipher 1

2.1 Solution for Cipher 1

BEGIN Once a laboratory novelty grown only on silicon, the NASA team now grows these forests of vertical carbon tubes on commonly used spacecraft materials, such as titanium, copper and stainless steel. Tiny gaps between the tubes collect and trap light, while the carbon absorbs the photons, preventing them from reflecting off surfaces. Because only a small fraction of light reflects off the coating, the human eye and sensitive detectors see the material as black.

Key: zyxiwvutsrqponkmljhgfedcba

2.2 Cipher 1 Cryptanalysis

I began by attempting to determine the type of encryption which had been used to produce this cipher. My first step in doing this was to calculate the Index of Coincidence for the cipher text, which I did using an online tool. The result was 0.06576, very close to the value for english text of 0.0677. On this basis I made the assumption that this is a monoalphabetic cipher. This cipher includes punctuation and a mixture of upper and lower case letters, which suggests that this is a substitution cipher rather than a permutation cipher, however the casing and punctuation could also have been arbitrarily inserted after encryption in order to lead me to a false assumption, so I also ranked the frequency of individual letters in the cipher text and compared this ranking to the corresponding ranking for average english text. They were drastically different, which would not be the case if a permutation cipher had been used. Based on these findings, I moved ahead with the assumption that a monoalphabetic substitution cipher had been used.

To give myself a starting point which would hopefully have some correct letters, I assumed that each letter in the cipher alphabet replaced the letter in the plaintext alphabet with the same position in the frequency ranking of english text that this letter had in the frequency ranking for the cipher text. For example, under this assumption the three most common letters in the cipher text, V H and Z, are decrypted to the three most common letters in english text, E T and A, respectively. This produced the decryption key *xwqdpvytosjginkmrzlfuebhca*, which when applied to the cipher text produced text which was clearly not the plaintext, but did include some notable features.

3 Cipher 2

3.1 Solution for Cipher 2

3.2 Cipher 2 Cryptanalysis

4 Cipher 3

4.1 Solution for Cipher 3

4.2 Cipher 3 Cryptanalysis

5 Appendices

5.1 Appendix A

5.2 Appendix B

5.3 Appendix C