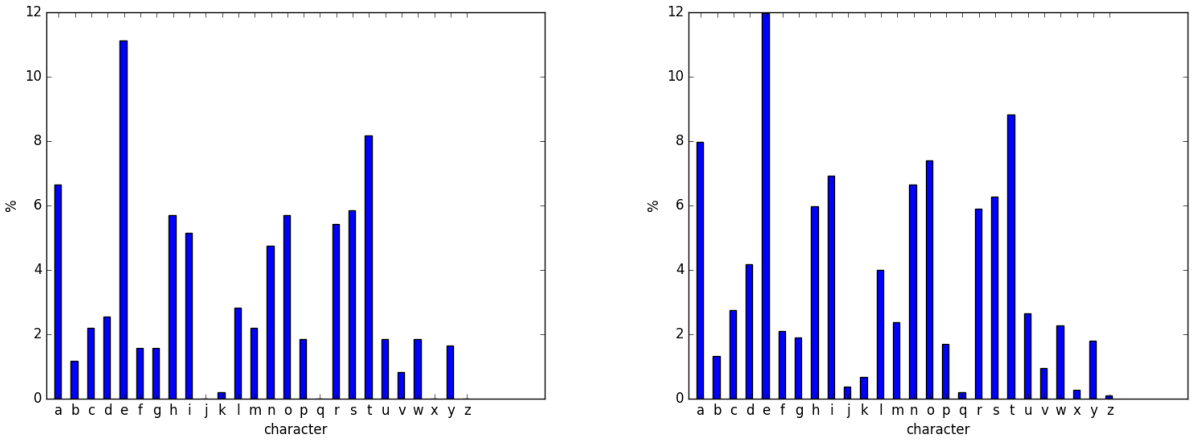
1 Analyse the ciphertext histograms

Below I have plotted the histograms for each file and figured out their corresponding cipher.

1.1 File 0.txt - Transposition

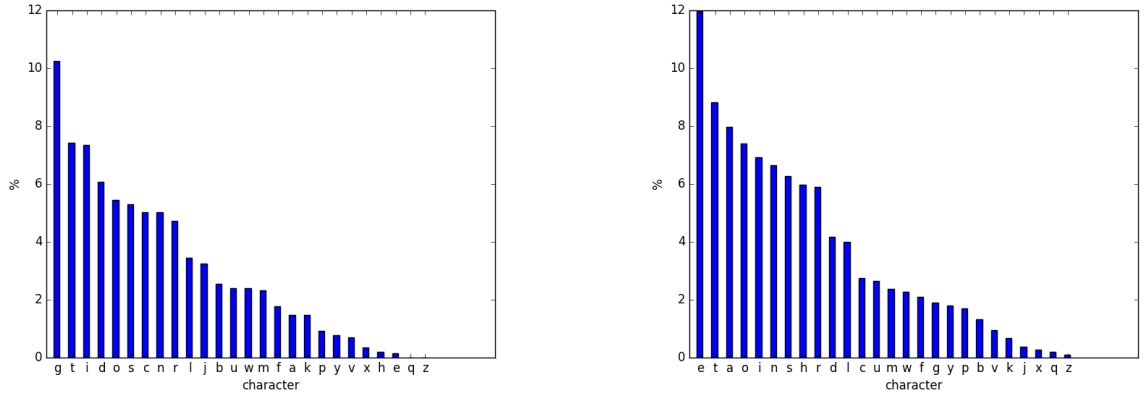


(a) Ciphertext (b) English

Figure 1: Histograms for the transposition cipher

The character frequency in the ciphertext is the same as that of a standard english text. This points to a transposition cipher, which preserves the character frequency in the encrypted text

1.2 File 1.txt - Random simple substitution



(a) Ciphertext (b) English

Figure 2: Histograms for the substitution cipher

If we sort the histograms by frequency and compare it with a sorted version of the english language, we can see that same frequencies appear, just at other characters. This points to a simple substitution cipher.

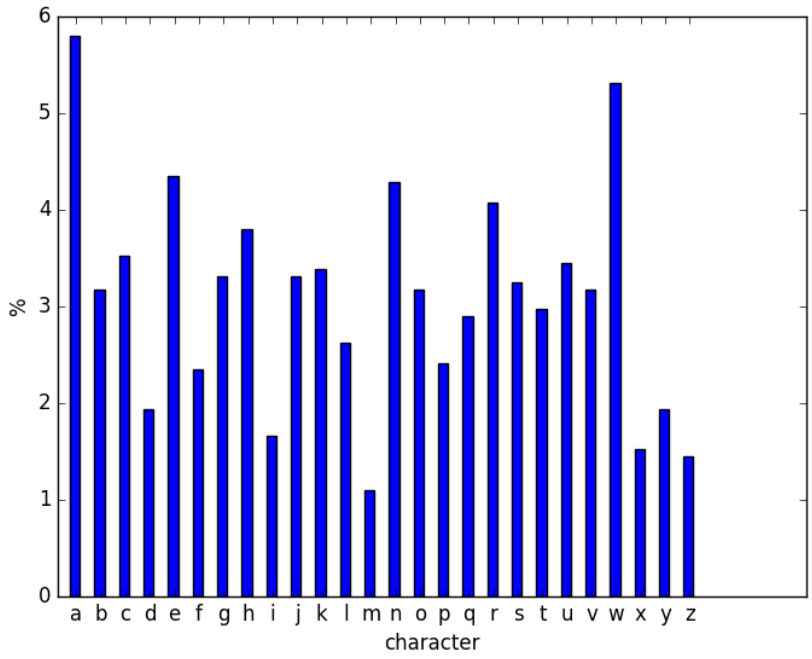


Figure 3: Histogram of the Vigenère cipher

1.3 File 3.txt - Vigenère

This histogram is much more smoothed out than the histograms for the previous ciphers. This points to polyalphabetic substituion, which could be either the Vigenère or the Hill cipher. However, plotting the autocorrelation of the ciphertext yields Figure ??, which shows us that this is the Vigenère cipher with period 7.

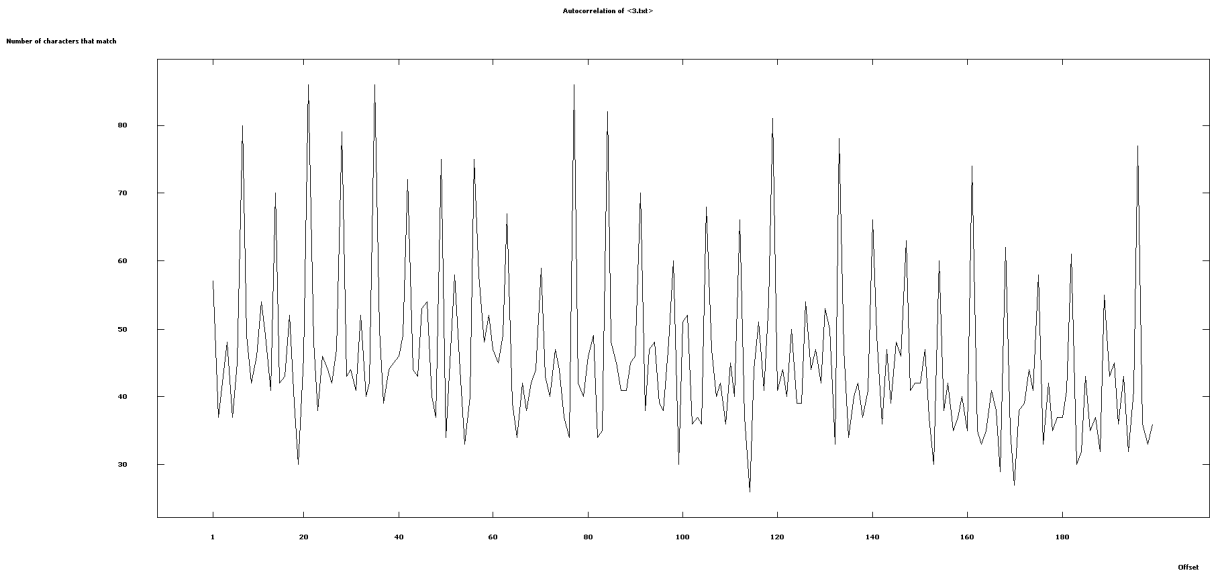


Figure 4: Autocorrelation of the Vigenère cipher

1.4 File 2.txt - 2x2 Hill cipher

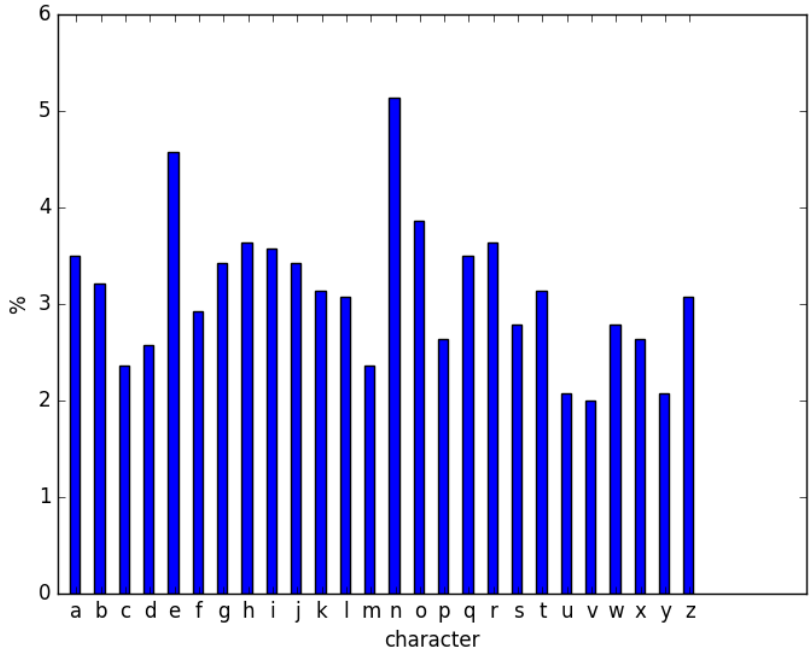


Figure 5: Histogram for the 2x2 Hill cipher

This cipher also has an even distribution, but since we have only 1 cipher left, this must be the 2x2 Hill cipher.

2 Obtaining the substitution, Vigenère, and transposition plain-texts

2.1 Random simple substitution

key: IABJGFKCDEHLMNOPQRSTUVWXYZ

plain-text: control of the sea was actually at stake. Nor did Admiral Jellicoe indulge in any false expectations concerning the future. Bad as the situation then was, he had every expectation that it would grow

2.2 Vigenère

key: WNCOJAS

plain-text: SUbMergEd fOR a PERiOd, whIle The cRew Of iTS VicTiM Was getTINg Off IN boaTs; IT Then caMe tO The SUrface, aNd The MEN pRepaRed To bOaRd The dISabled ShiP and SeaRch hER fOR vaLUableS aNd delIcacies

2.3 Transposition

key: 7165243.

plain-text: for prisoners or the ship s papers the boats crews therefore had instructions to take up a station on a bearing from which the ship s guns could most successfully rake the submarine That this manoeuvre involved great

3 Cryptoanalyse the 2x2 Hill ciphertext

key: XT LU

plain-text: of the submarine area, stopped attacking sick and wounded soldiers. Yet we still were forced to provide these unfortunates with destroyer escorts, for, had we momentarily withdrawn these protectors, the German submarines would immediately have renewed their attacks on hospital