NTNU

Kunnskap for en bedre verden

DEPARTMENT OF COMPUTER SCIENCE

TTM4135 - APPLIED CRYPTOGRAPHY AND NETWORK SECURITY

Practical Assignment

Author:
Adrian Langseth

February, 2021

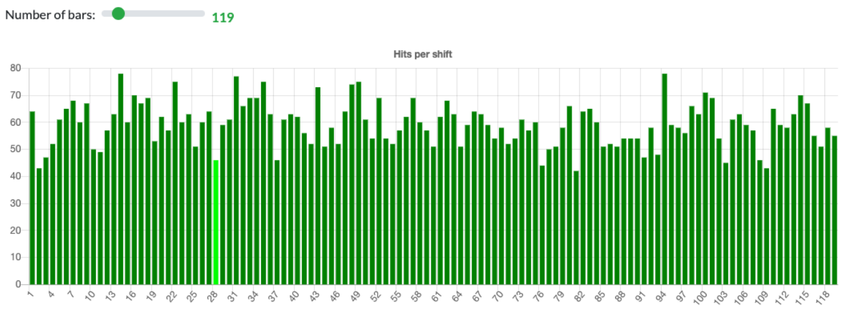


Figure 1: Autocorrelation on the text 0

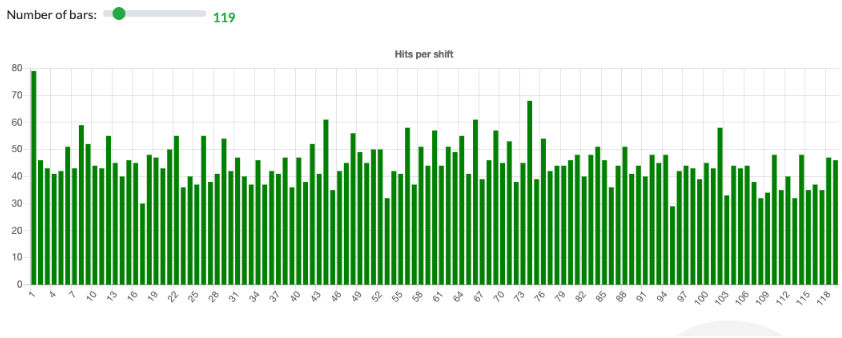


Figure 2: Autocorrelation on the text 1

Vigenére Analysis

Autocorrelation

Text 0

Examining the autocorrelation on text 0 illustrated in Figure 1, one can not see a clear repeating pattern in the autocorrelation.

Text 1

Examining the autocorrelation on text 1 illustrated in Figure 2, one can not see a clear repeating pattern in the autocorrelation.

Text 2

As we see in the autocorrelation seen in Figure 3, a clear repeating pattern is shown in the maximums with an interval of 7. This implies that it would be beneficial to investigate a vinegere cipher of length 7. Examining this possibility in the vigenere analysis tool, with a key length of 7, we find the key to be **GRBPWFM**.

This result in the following generated plaintext: *SO THAT SHE COULD NOT FINISH THE SENTENCE; BUT HER LIP QUIVERED. BUT IT SEEMED THAT MRS. DALLOWAY WAS ABLE TO UNDERSTAND WITHOUT WORDS. ”I KNOW,” SHE SAID, ACTUALLY PUTTING ONE ARM ROUND RACHEL’S SHOULDER. ”WHEN I WAS YOUR AGE I WANTED TOO. NO ONE UNDERSTOOD UNTIL I MET RICHARD. HE GAVE ME ALL I WANTED. HE’S MAN AND WOMAN AS WELL.” HER EYES RESTED UPON MR. DALLOWAY, LEANING UPON THE RAIL, STILL TALKING. ”DON’T THINK I SAY THAT BECAUSE I’M HIS WIFE–I SEE*

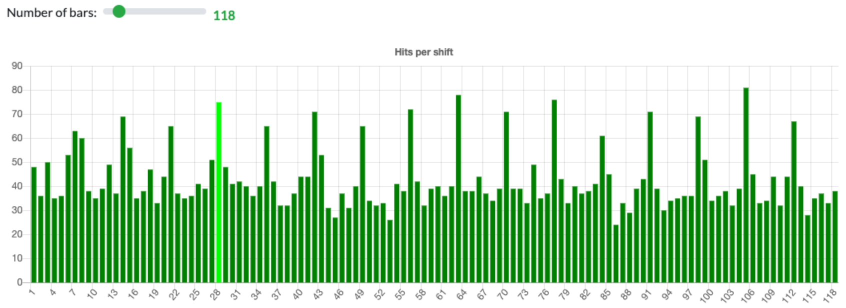


Figure 3: Autocorrelation on the text 2

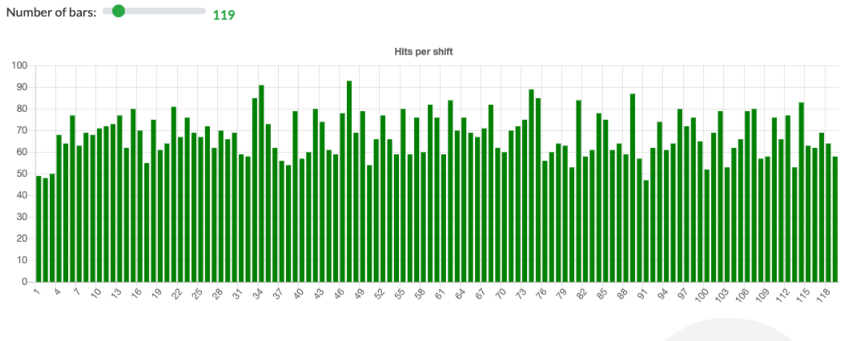


Figure 4: Autocorrelation on the text 3

HIS FAULTS MORE CLEARLY THAN I SEE ANY ONE ELSE’S. WHAT ONE WANTS IN THE PERSON ONE LIVES WITH IS THAT THEY SHOULD KEEP ONE AT ONE’S BEST. I OFTEN WONDER WHAT I’VE DONE TO BE SO HAPPY!” SHE EXCLAIMED, AND A TEAR SLID DOWN HER CHEEK. SHE WIPED IT AWAY, SQUEEZED RACHEL’S HAND, AND EXCLAIMED: ”HOW GOOD LIFE IS!” AT THAT MOMENT, STANDING OUT IN THE FRESH BREEZE, WITH THE SUN UPON THE WAVES, AND MRS. DALLOWAY’S HAND UPON HER ARM, IT SEEMED INDEED AS IF LIFE WHICH HAD BEEN UNNAMED BEFORE WAS INFINITELY WONDERFUL, AND TOO GOOD TO BE TRUE. HERE HELEN PASSED THEM, AND SEEING RACHEL ARM-IN-ARM WITH A COMPARATIVE STRANGER, LOOKING EXCITED, WAS AMUSED, BUT AT THE SAME TIME SLIGHTLY IRRITATED. BUT THEY WERE IMMEDIATELY JOINED BY RICHARD, WHO HAD ENJOYED A VERY INTERESTING TALK WITH WILLOUGHBY AND WAS IN A SOCIABLE MOOD. ”OBSERVE MY PANAMA,” HE SAID, TOUCHING THE BRIM OF HIS HAT. ”ARE YOU AWARE, MISS VINRACE, HOW MUCH CAN BE DONE TO INDUCE FINE WEATHER BY

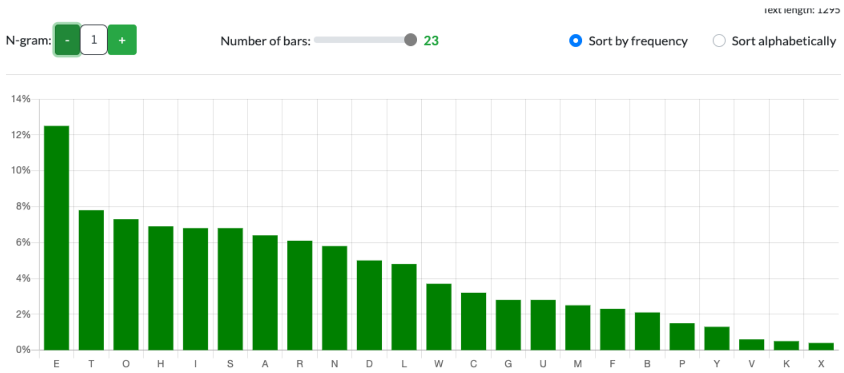
Text 3

Examining the autocorrelation on text 3 illustrated in Figure 4, one can not see a clear repeating pattern in the autocorrelation.

Transposition analysis

Frequency Analysis

Doing frequency analysis on text 0, we can see a frequency distribution over the characters in the text to be similar enough to the ”standard” distribution of the English alphabet, to conclude that this is the transposition cipher of the texts. This is because of the similarity indicating that the



Text length: 1295

N-gram: - 1 +

Number of bars: 23

● Sort by frequency ○ Sort alphabetically

Figure 5: Frequency analysis on the text 0

characters have not been substituted, but only transpositioned.

JCrypTool analysis

For the analysis the best fit was found to be row-wise read-in and read-out with a column length of 7. From this the key of **3-1-7-4-2-5-6** was found to give the most coherent plaintext.

Plaintext: ”**describe the white hairless blind monsters lying curled on the ridges of sand at the bottom of the sea which would explode if you brought them to the surface their sides bursting asunder and scattering entrails to the winds when released from pressure with considerable detail and with such show of knowledge that Ridley was disgusted and begged him to stop From all this Helen drew her own conclusions which were gloomy enough Pepper was a bore Rachel was an unlicked girl no doubt prolific of confidences the very first of which would be You see I don t get on with my father Willoughby as usual loved his business and built his Empire and between them all she would be considerably bored Being a woman of action however she rose and said that for her part she was going to bed At the door she glanced back instinctively at Rachel expecting that as two of the same sex they would leave the room together Rachel rose looked vaguely into Helen s face and remarked with her slight stammer I m going out to t t triumph in the wind Mrs Ambrose s worst suspicions were confirmed she went down the passage lurching from side to side and fending off the wall now with her right arm now with her left at each lurch she exclaimed emphatically Damn Chapter II G**

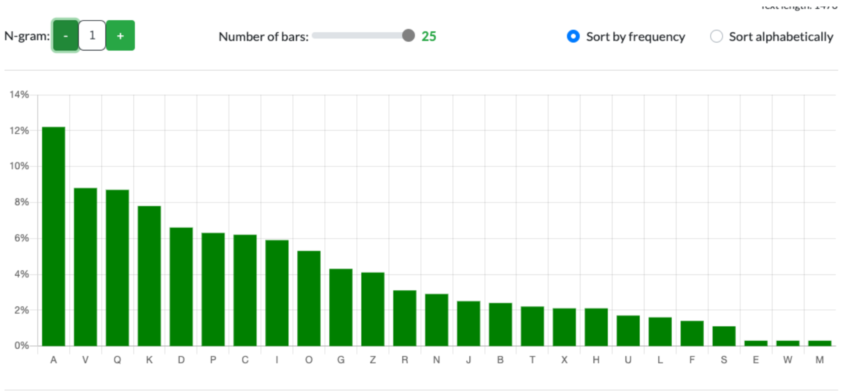
Substitution analysis

Frequency Analysis

Doing frequency analysis on text 3, we can see in Figure 6 a frequency distribution over characters in the text to be similar enough to the ”standard” distribution of the English alphabet, however with different letters. This leads me to believe text 3 is the substitution cipher. As the last text remaining, text 1, does not conform to such a distribution, I will assume text 3 to be the substitution cipher.

Finding ”the”

Note: I am assuming the large text size of 1500 provide a somewhat representative sample of the English language.



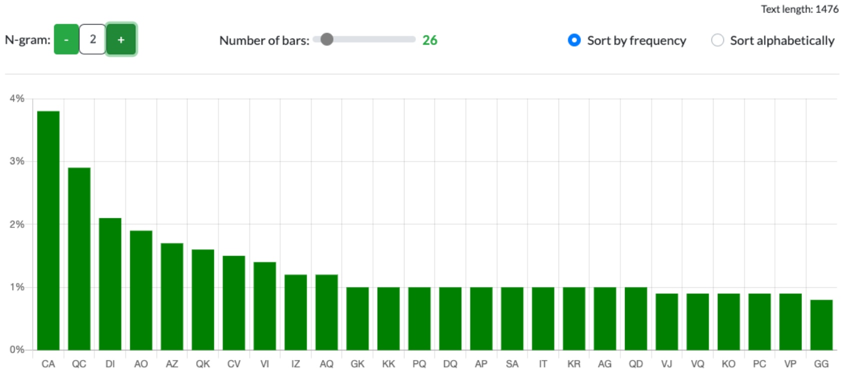
Text length: 1476

N-gram: - 1 +

Number of bars: 25

● Sort by frequency ○ Sort alphabetically

Figure 6: Frequency analysis on the text 3 on an 1-gram basis



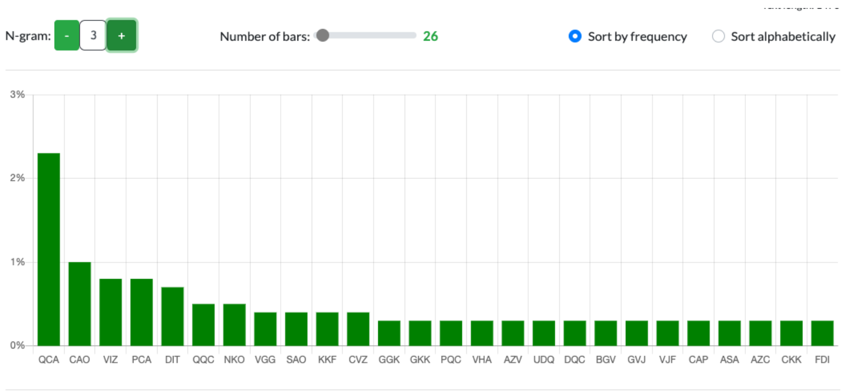
Text length: 1476

N-gram: - 2 +

Number of bars: 26

● Sort by frequency ○ Sort alphabetically

Figure 7: Frequency analysis on the text 3 on an 2-gram basis



Text length: 1476

N-gram: - 3 +

Number of bars: 26

● Sort by frequency ○ Sort alphabetically

Figure 8: Frequency analysis on the text 3 on an 3-gram basis

The characters "T", "H", and "E" roughly have a share 12%, 5.5% and 8%, respectively. Therefore we would expect the characters which have been substituted with them to be in the same approximate share. Seen in Figure 6, "A" enjoys the by far largest share, giving suspicion that this is the substitution of "E". We will remember this for further consideration in the 2-gram analysis. Based on the shares, we can suspect the substitution for "T" was one of the three letters "V", "Q" and "K", although still quite uncertain. The substitution for "H" is harder to narrow down, although the prime candidates would be those in the following cluster o "D", "P", "C", "I", and "O".

In the 2-gram distribution shown in Figure 7 we can continue to look at the two parts "TH" and "HE". As these are the two most frequent 2-gram in the English language, we will look among the higher shares. Here we see "CA", and "QC" as the top shares. If we follow our belief that "A" is the substitution for "E", it would follow that "C" may be "H". This is supported by what we saw in the 1-gram analysis. Furthermore, this would imply that "QC" corresponds to "TH" and therefore "Q" may be the substitution of "T". This is again supported by what we saw in 1-gram analysis.

The 3-gram analysis shown in Figure 8, shows "QCA" to be the outstanding shareholder. This is similar to the expected outperformance of "THE". As this supports what we found in both 1-gram and 2-gram analysis, we can safely assume "QCA" to be the substitution of "THE"

Hill Cipher

Performing the cryptanalysis with known plaintext attack suggested in the task description, I calculated the key

$$K = \begin{pmatrix} 15 & 19 \\ 2 & 17 \end{pmatrix}$$

Applying this to the Hill Cipher, the decryption resulted in the plaintext:

her skirt. He led them across a stretch of green by the river-bank and then through a grove of trees, and bade them remark the signs of human habitation, the blackened grass, the charred tree-stumps, and there, through the trees, strange wooden nests, drawn together in an arch where the trees drew apart, the village which was the goal of their journey. Stepping cautiously, they observed the women, who were squatting on the ground in triangular shapes, moving their hands, either plaiting straw or in kneading something in bowls. But when they had looked for a moment undiscovered, they were seen, and Mr. Flushing, advancing into the centre of the clearing, was engaged in talk with a lean majestic man, whose bones and hollows at once made the shapes of the Englishman's body appear ugly and unnatural. The women took no notice of the strangers, except that their hands paused for a moment and their long narrow eyes slid round and fixed upon them with the motionless inexpensive gaze of those removed from each other far far beyond the plunge of speech. Their hands moved again, but the stare continued. It followed them as they walked, as they peered into the huts where they could distinguish guns leaning in the corner, and bowls upon the floor, and stacks of rushes; in the dusk the solemn eyes of babies regarded them, and old women stared out too. As they sauntered about, the stare followed them, H