3.Historical algorithms:

1. **What can we say about multiple encryption in the context of historical algorithms (consider their different classes)? How does this affect the ability to decrypt a ciphertext? The answer to this question is illustrated by the result of an experiment conducted in Cryptool.**
   According to my observations on algorithms such as Hill,Playfair polyalphabetic etc. are not really secure that we can trust because they known as a common algorithms that others knew and able to easily crack it. So in my opinion it might not be the perfect protection choice but multiple encryption makes it a bit more safety but not at all. It just extends the time to crack it.

2. **How many different keys are there in the classical substitution algorithm?**

   There are 26! = $2^{88.4}$ possible number which is about 88bits. But according to my research this cipher isn't really enough and can be easily broken

3. **What is the space (number) of keys in polyalphabetic algorithms?**
   A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The vigenere cipher is best-known example with a 26-letter alphabet and period d the key space contains 26! x 26d-1 possible keys. This is approximately 1032 keys for a period of length 5 and 1053 keys for a period of length 20. Its depends on the cipher keys for example there is 25 possible keys in Caesar ciphers which is 25! x 25d-1.

4. **How many different keys are there in PlayFair and Hill algorithm?**
   There is 25 letters(reduced) in PlayFair algorithm spread on a 5x5 square, that's 25! Keys. And there are $\mathbf{26^{n2}}$ possible matrices of dimension or 4.7n^2 upper bound on the key size of the Hill algorithm cipher using nxn which can contain only numbers from 0 to 26.

Hill is more difficult to be crack than PlayFair.

5. **What does the number of keys in transposition algorithm depend on?**

   its constitutes a permutation of the plaintext. In transposition cipher, in order to decipher it, the recipient has to work out the column lengths by dividing by the message length by the key length. (Length).

6. **Which of the selected algorithms do you consider the strongest, why?**

   According to my research **transposition** algorithm are not highly secure because they do not change the letters in the plaintext or even cover freq. And **polyalphabetic** is the repeating nature of its key. If a cryptanalyst correctly guesses the key's length n, the cipher text can be treated as n interleaved Caesar ciphers, which can easily be broken individually.

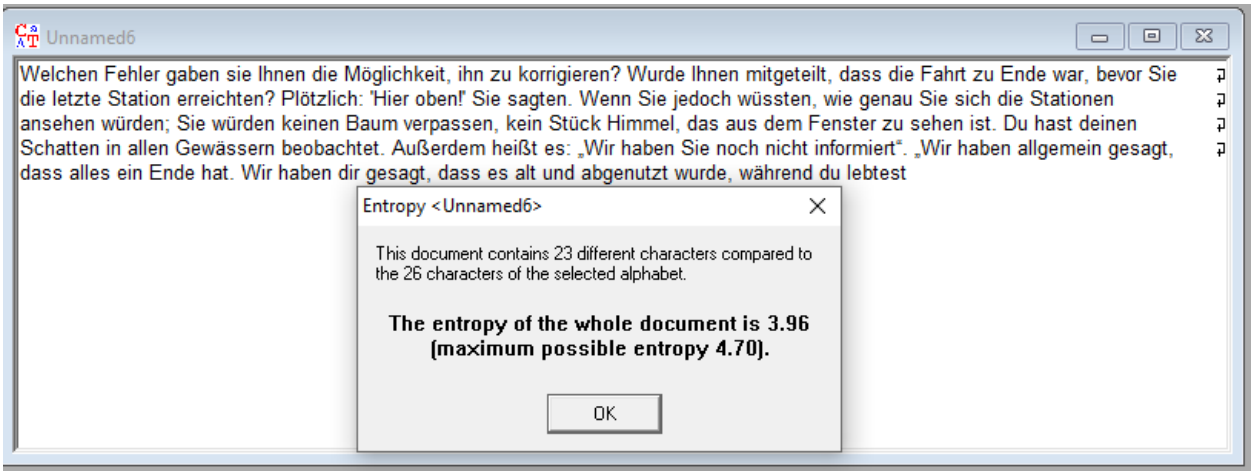
   Also **classical cipher** used historically but it has fallen into disuse.However they are also generally very simple to break with modern technology. Furthermore Hill cipher is harder to crack than playfair cipher.

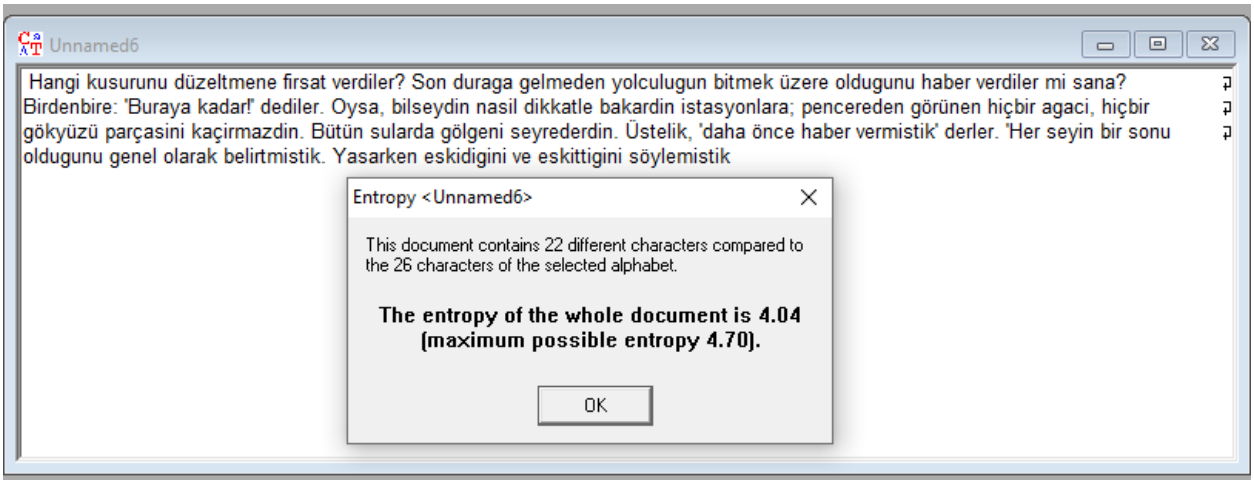
   Thus in my opinion the strongest algorithm is the **Hill algorithm** anymore. İts one of the most widely used cryptographic algorithm and widely applied in various cryptographic studies to decrypt data.

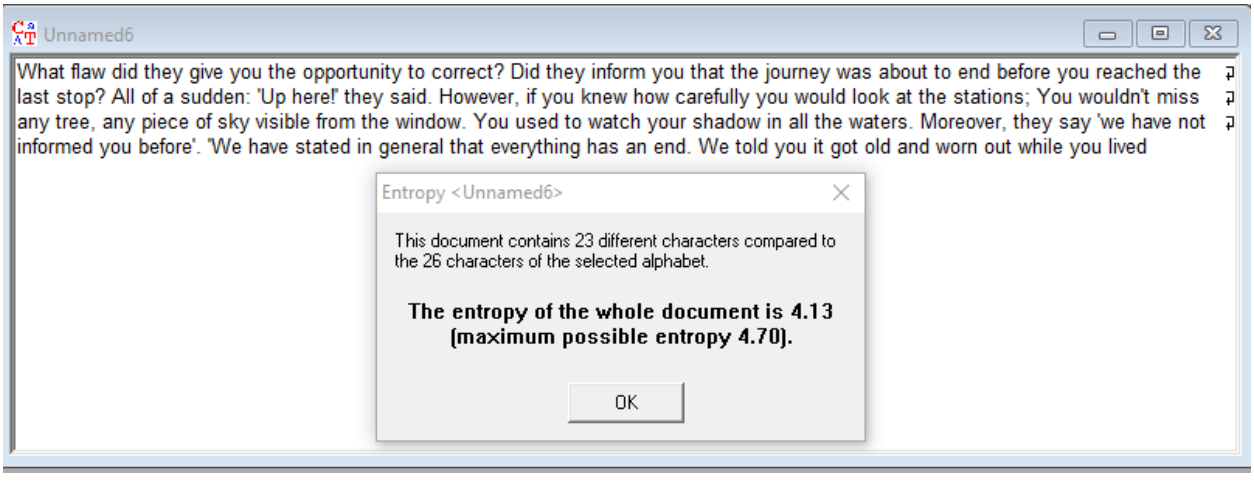
4. Property analysis of available algorithms.

1. Compare the entropy values of plaintexts for different languages (English, Polish, German, French, Italian, Spanish, ...)

I used turkish poem to analyse.

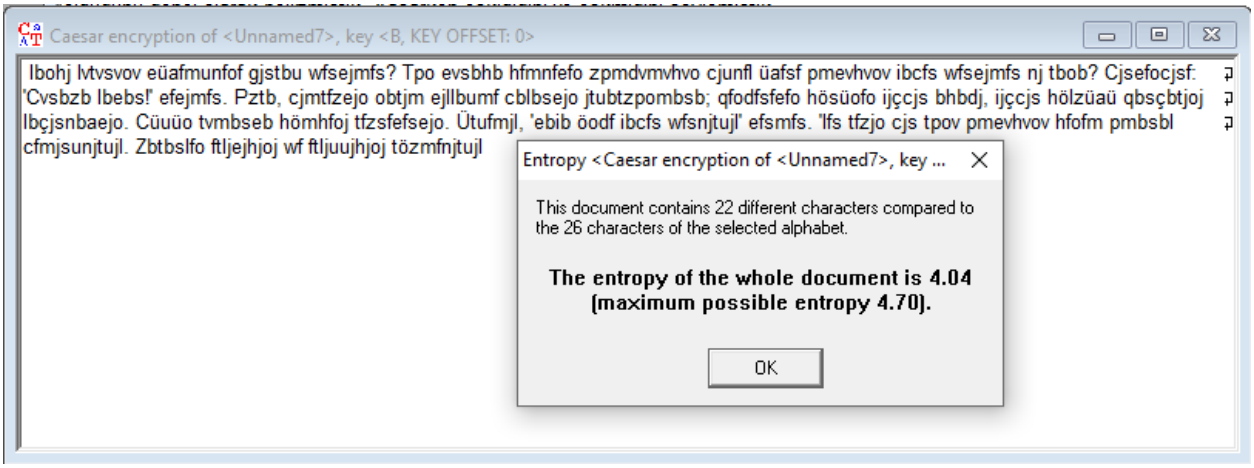

Unnamed6
Welchen Fehler gaben sie Ihnen die Möglichkeit, ihn zu korrigieren? Wurde Ihnen mitgeteilt, dass die Fahrt zu Ende war, bevor Sie die letzte Station erreichten? Plötzlich: 'Hier oben!' Sie sagten. Wenn Sie jedoch wüssten, wie genau Sie sich die Stationen ansehen würden; Sie würden keinen Baum verpassen, kein Stück Himmel, das aus dem Fenster zu sehen ist. Du hast deinen Schatten in allen Gewässern beobachtet. Außerdem heißt es: „Wir haben Sie noch nicht informiert". „Wir haben allgemein gesagt, dass alles ein Ende hat. Wir haben dir gesagt, dass es alt und abgenutzt wurde, während du lebtest
Entropy <Unnamed6>
This document contains 23 different characters compared to the 26 characters of the selected alphabet.
The entropy of the whole document is 3.96 (maximum possible entropy 4.70).
OK


Unnamed6
Hangi kusurunu düzeltmene firsat verdiler? Son duraga gelmeden yolculugun bitmek üzere oldugunu haber verdiler mi sana? Birdenbire: 'Buraya kadar!' dediler. Oysa, bilseydin nasil dikkatle bakardin istasyonlara; pencereden görünen hiçbir agaci, hiçbir gökyüzü parçasini kaçirmazdin. Bütün sularda gölgeni seyrederdin. Üstelik, 'daha önce haber vermistik' derler. 'Her seyin bir sonu oldugunu genel olarak belirtmistik. Yasarken eskidigini ve eskittigini söylemistik
Entropy <Unnamed6>
This document contains 22 different characters compared to the 26 characters of the selected alphabet.
The entropy of the whole document is 4.04 (maximum possible entropy 4.70).
OK

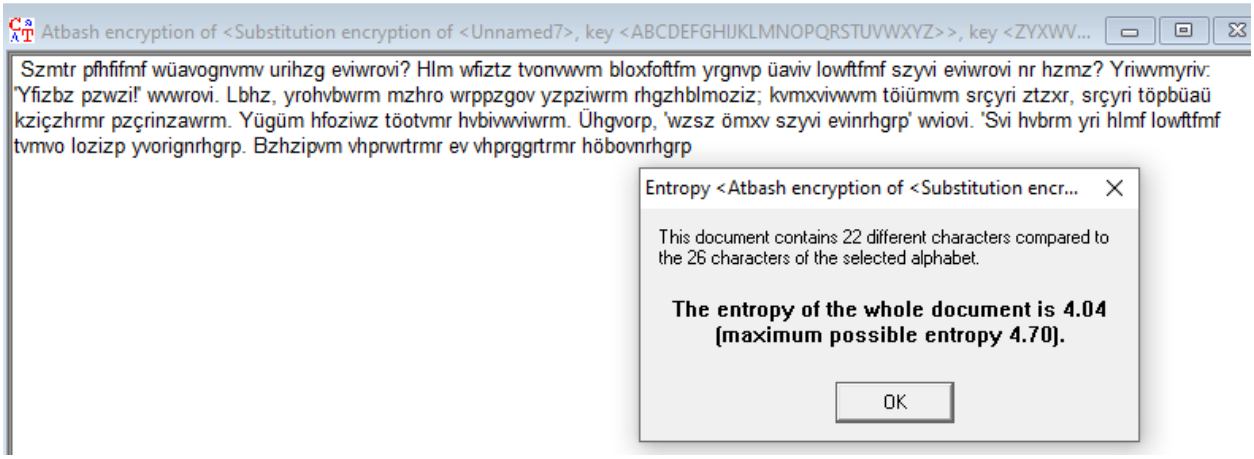

Unnamed6
What flaw did they give you the opportunity to correct? Did they inform you that the journey was about to end before you reached the last stop? All of a sudden: 'Up here!' they said. However, if you knew how carefully you would look at the stations; You wouldn't miss any tree, any piece of sky visible from the window. You used to watch your shadow in all the waters. Moreover, they say 'we have not informed you before'. 'We have stated in general that everything has an end. We told you it got old and worn out while you lived
Entropy <Unnamed6>
This document contains 23 different characters compared to the 26 characters of the selected alphabet.
The entropy of the whole document is 4.13 (maximum possible entropy 4.70).
OK

1. Compare the entropy values of plaintext and ciphertext depending on the algorithm.

caesar

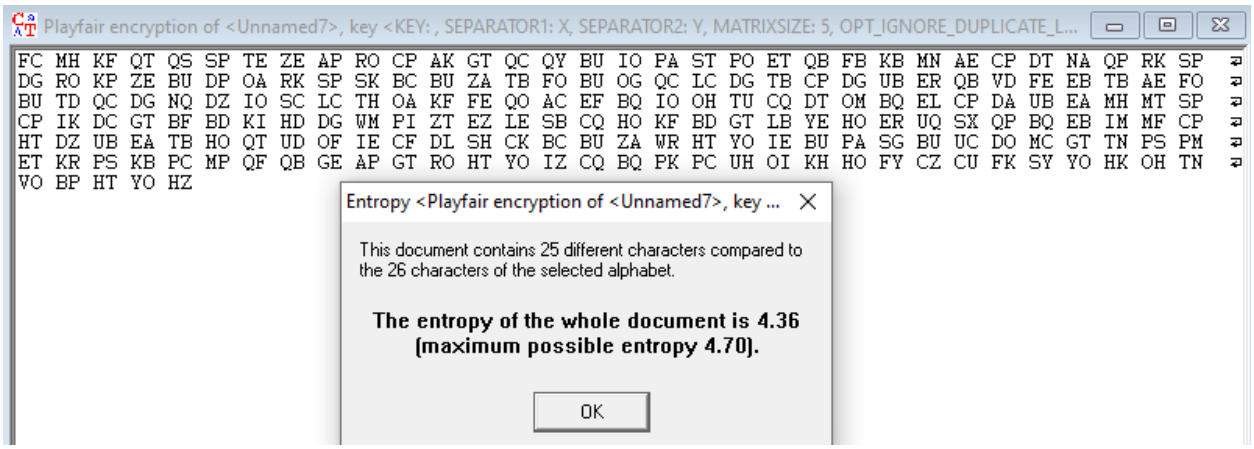


substitution



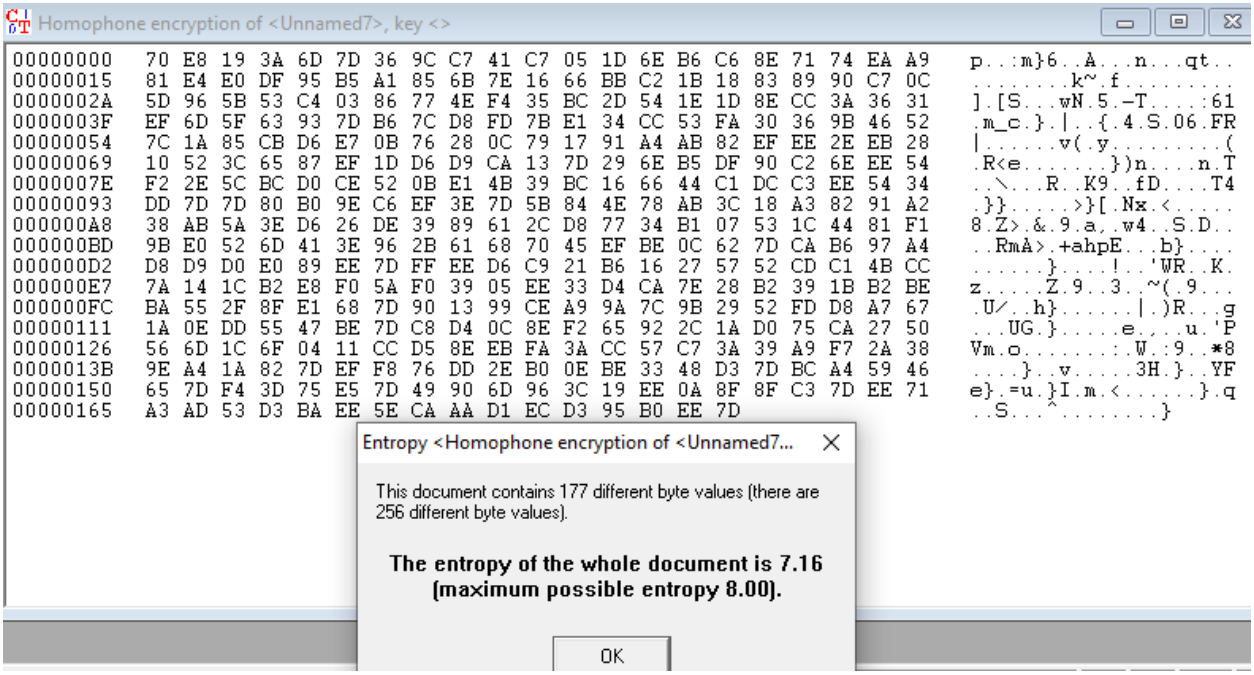
Not much difference these 2 entropy.

playfair



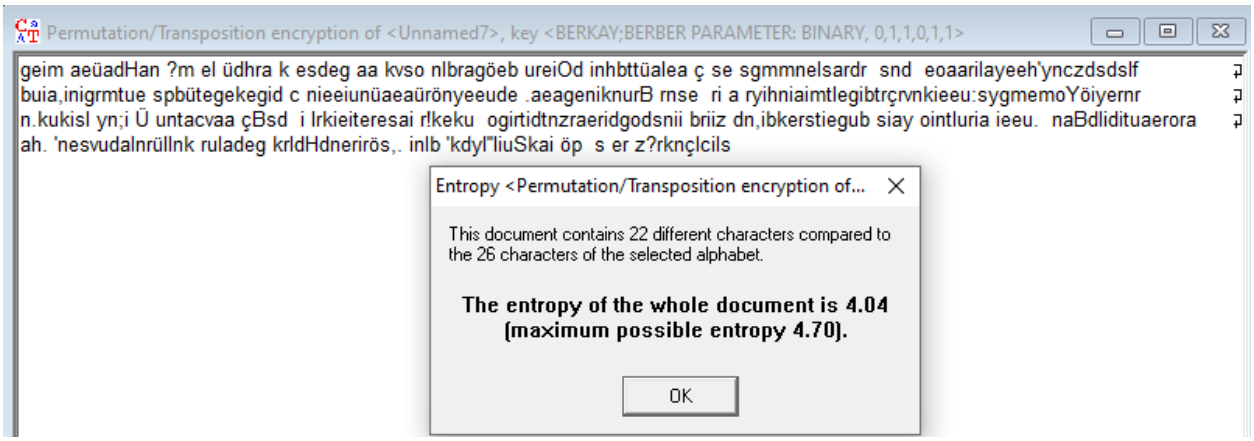
I see a bit alteration than first ones. The entropy of the document increased.

homophone



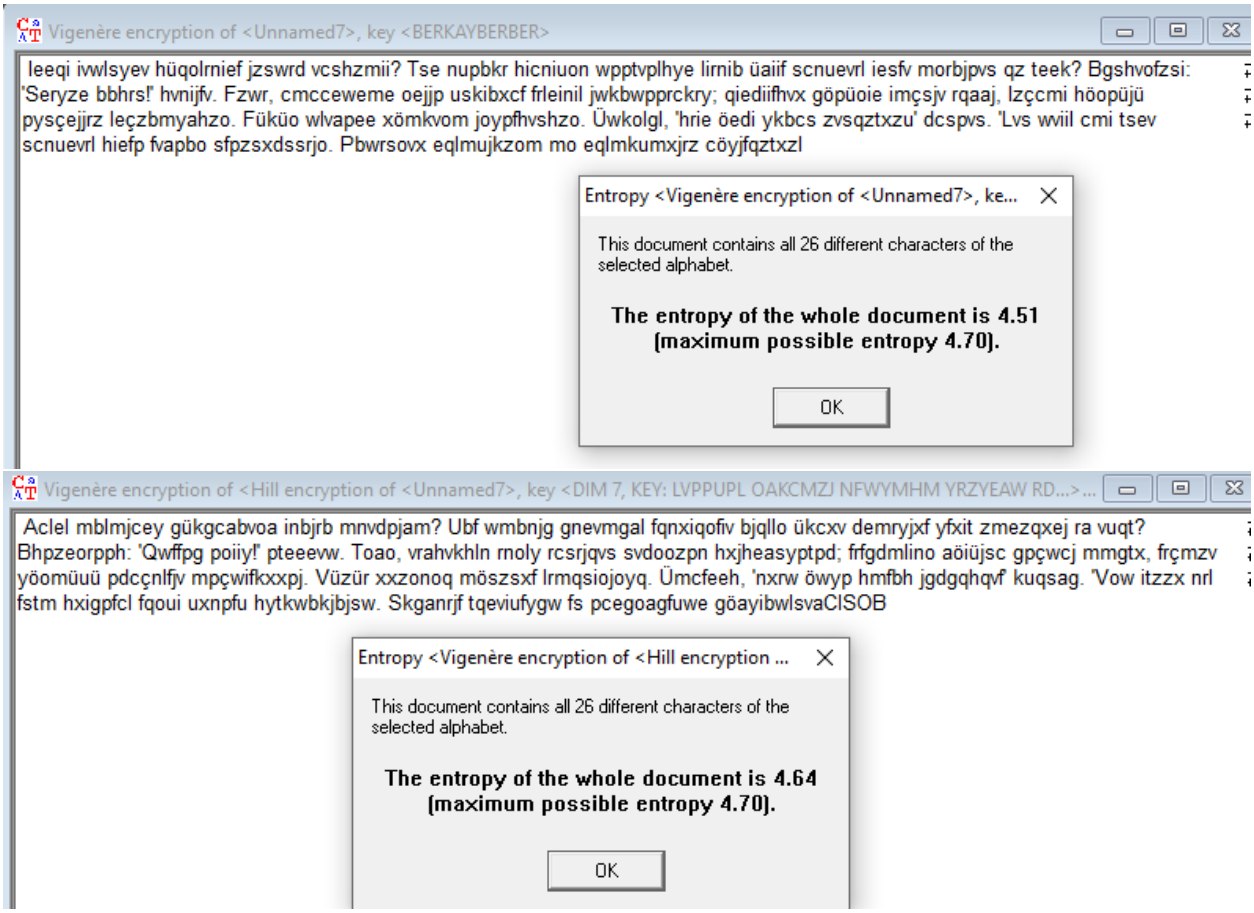
This is the only algorithm that I see this much difference compared to others. It looks complex and hard to decipher.

Permutations



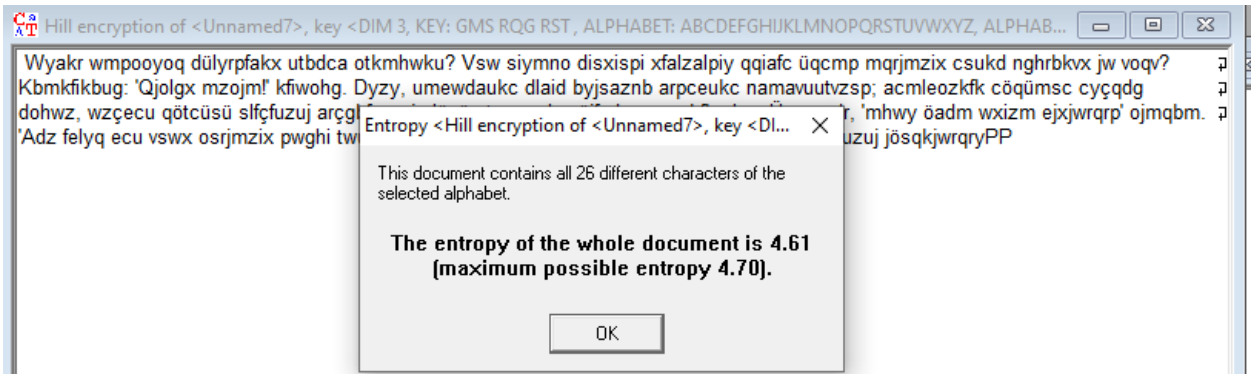
Doesn’t have surprisingly change.

Vigenere

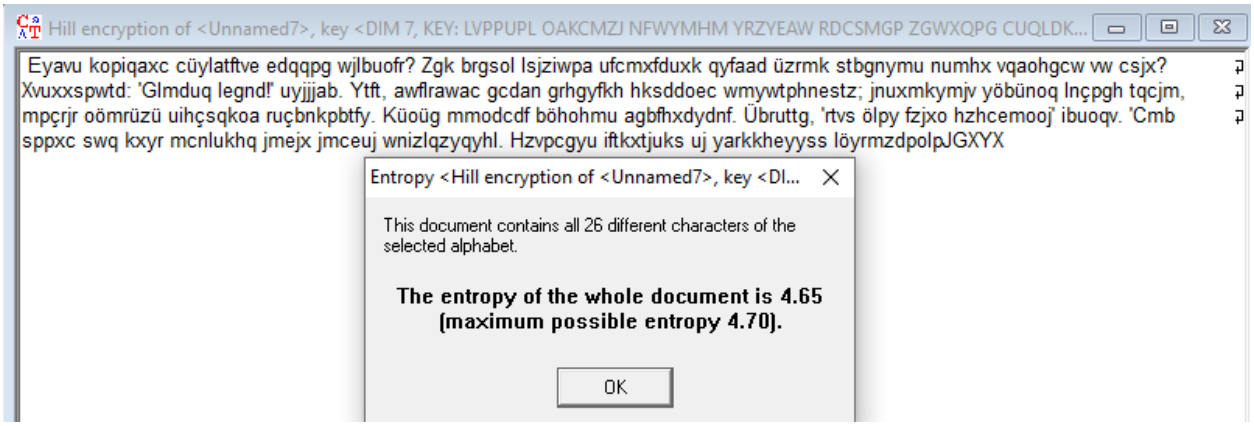


I tried to input longer key length to see the difference at the second algorithm, however it didn't effect much rather than long input key length.

Hill



3x3

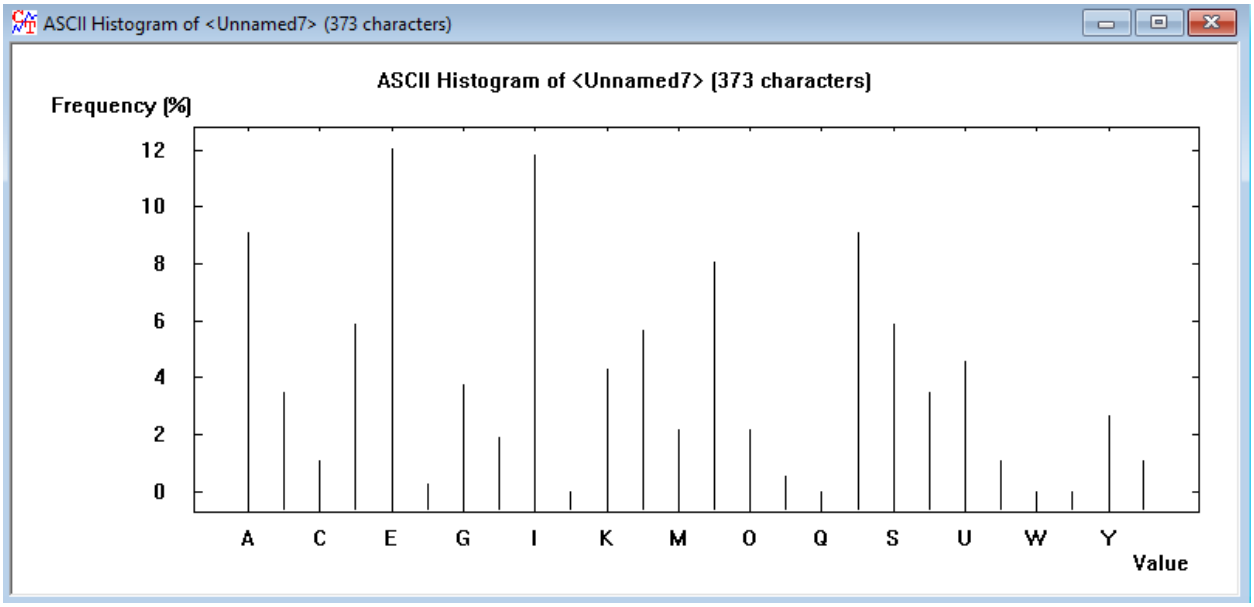


7x7

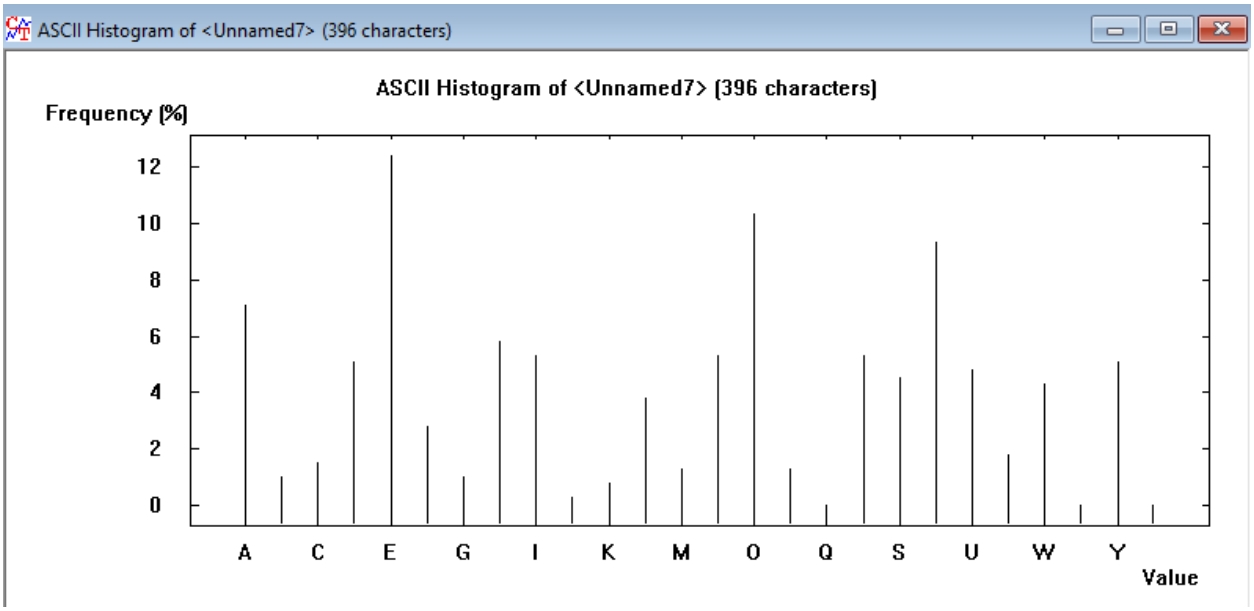
I used 3x3 matrix and 7x7 and we come across the same rate.

3. Compare histograms of plaintexts for selected 3 different languages

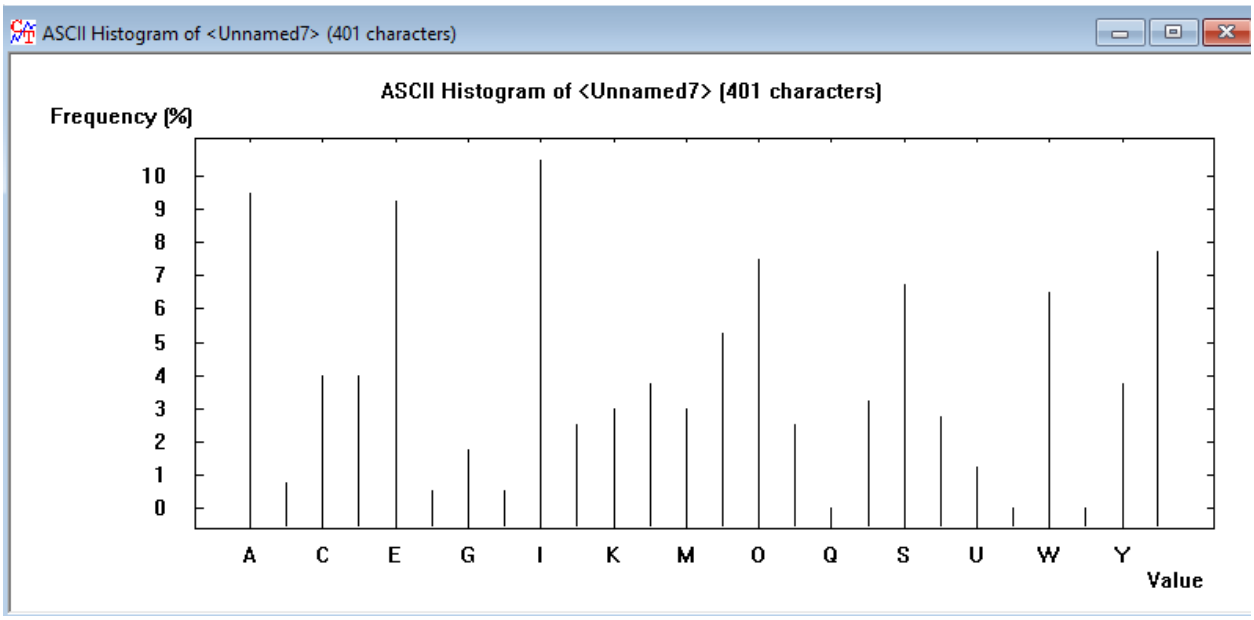
Turkish



English

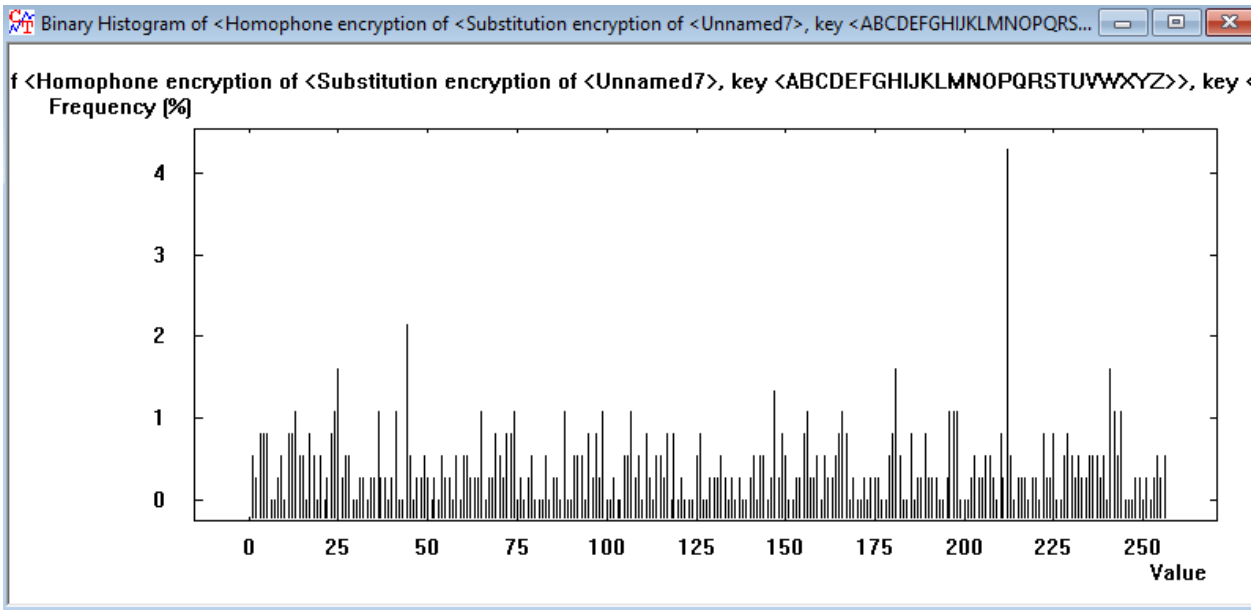


Polish

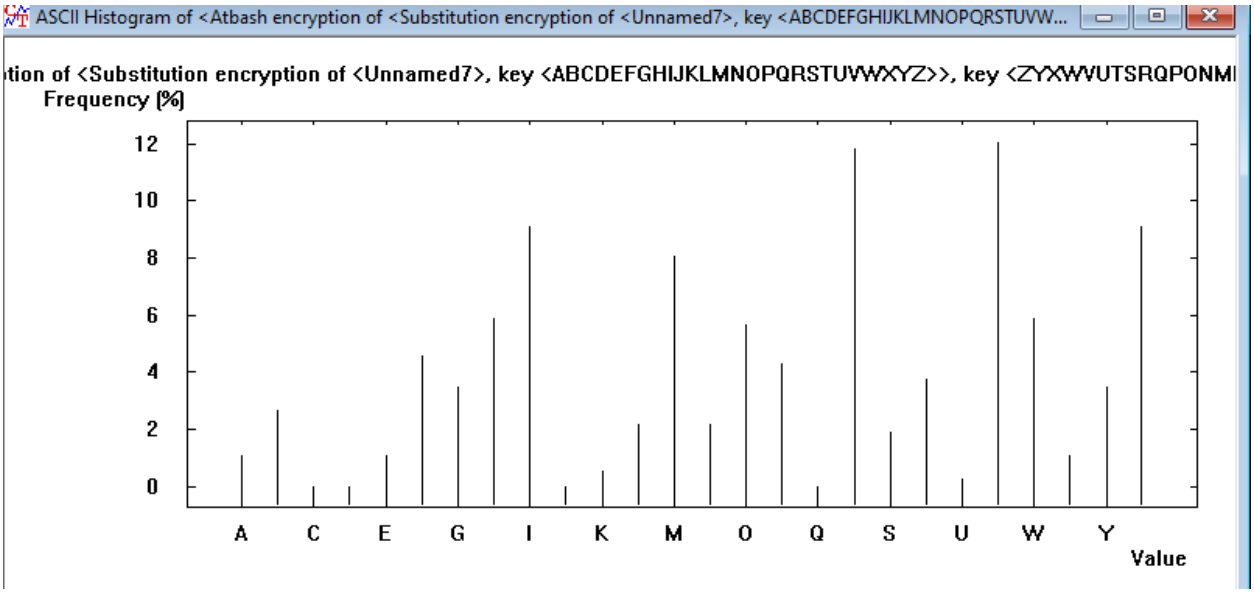


I have used the same text by translating it to different languages. And I have come across similar graph except on more similarities on frequency between the Polish and Turkish one.

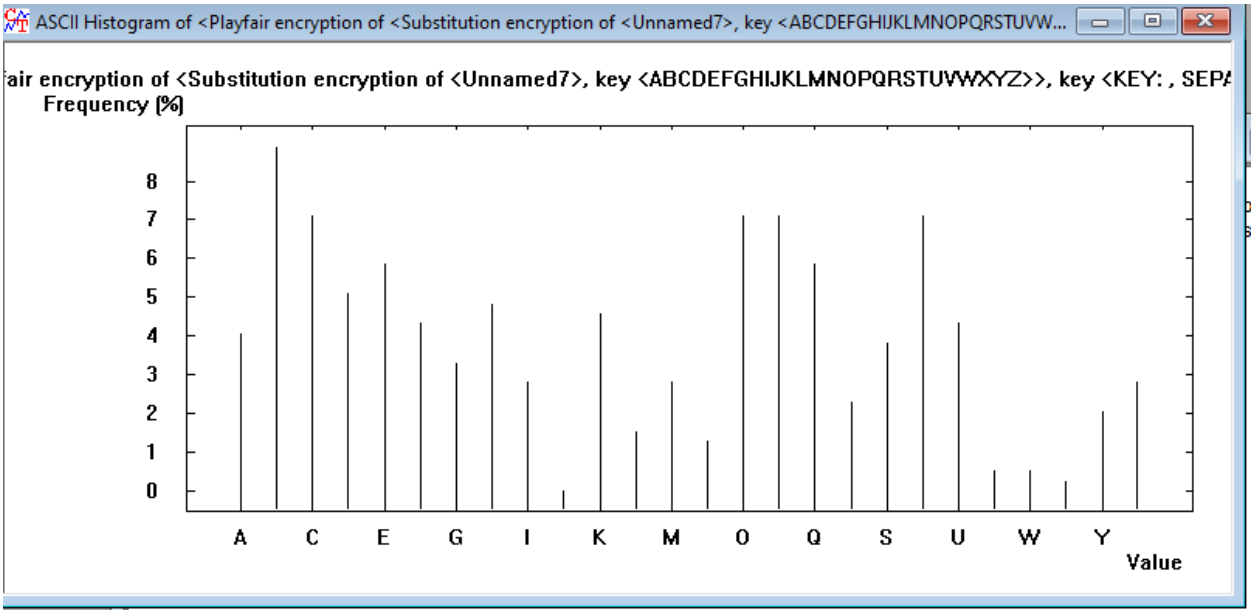
4. Compare histograms of plaintext and ciphertext depending on the algorithm.(Homophone, Substituton, Playfair)



Substution

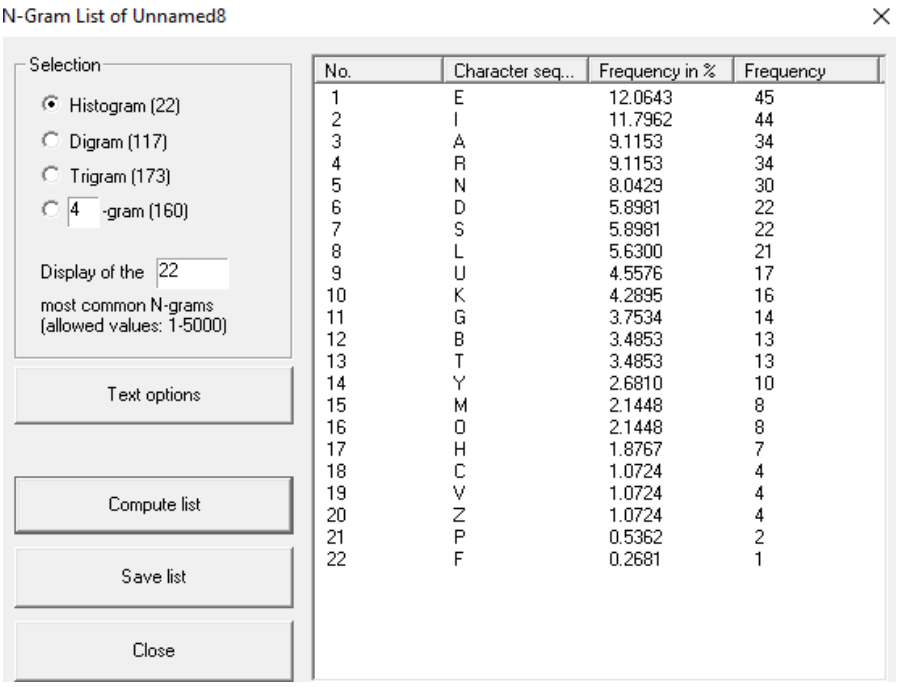


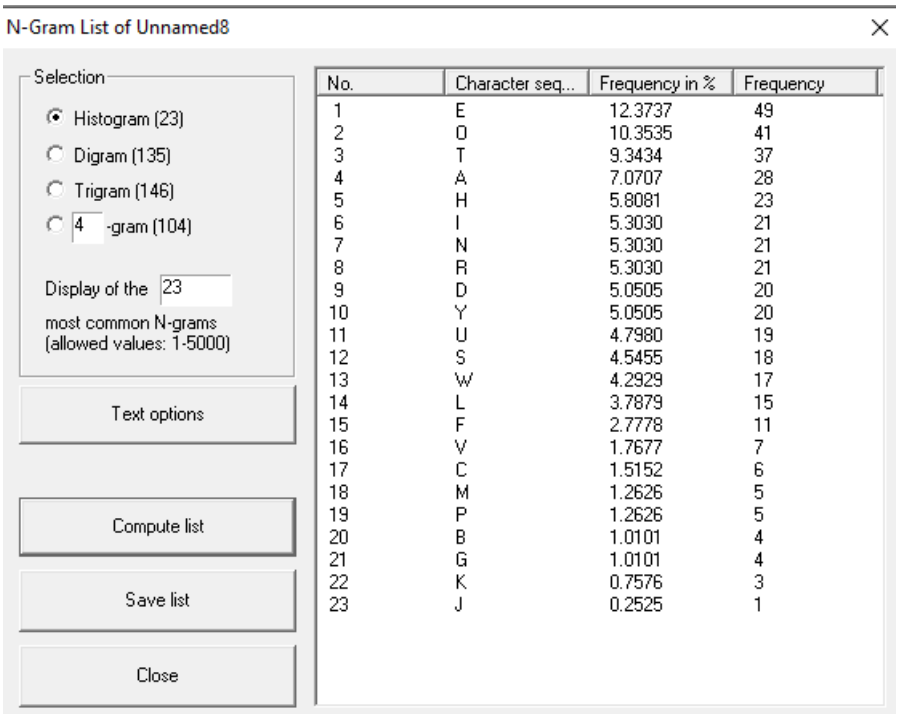
PLayFair

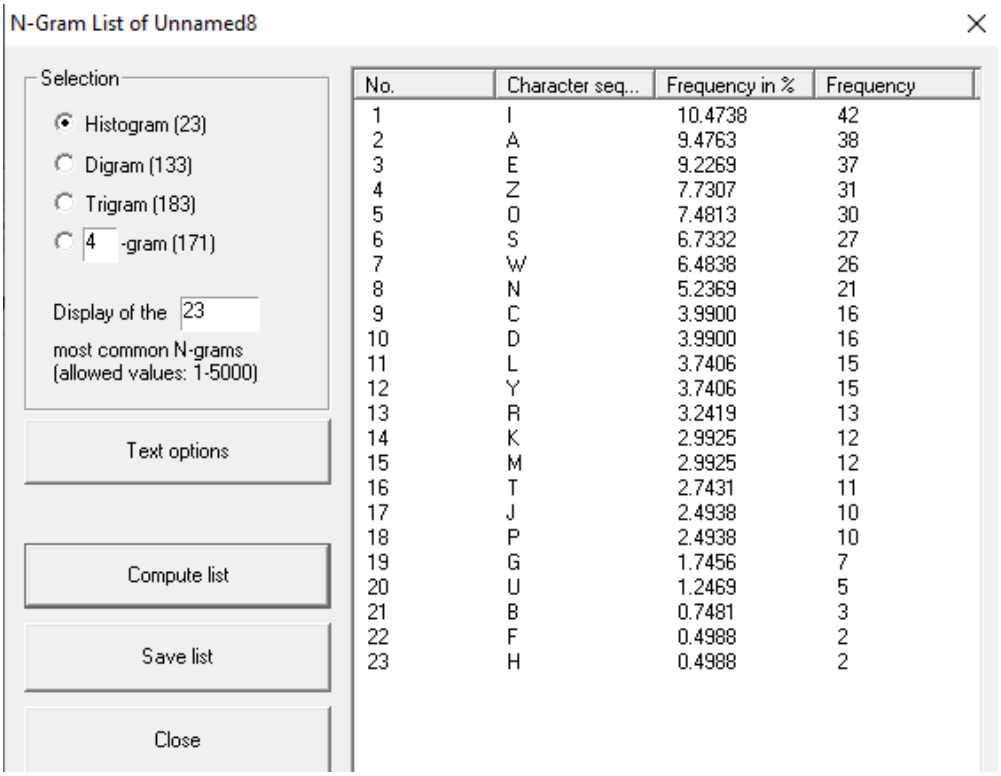


As I expected I saw the lowest rate belongs to the Homophone. And the worst is according to histograms is substituon.

5.Compare n-grams (bi/tri/n) of plaintexts for selected 3 differentlanguages(Turkish,English,Polish)





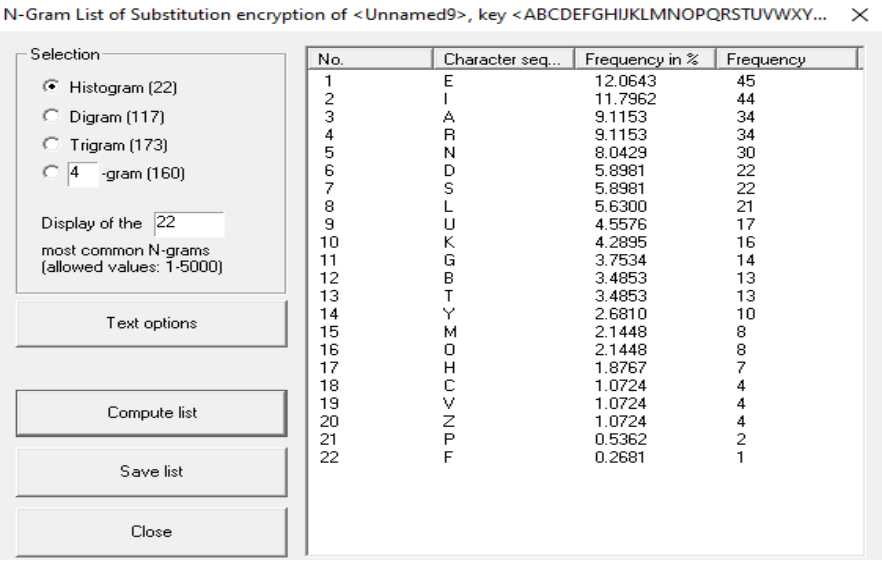


İ realize Turkısh frequency in % is averagely higher than others.

I come across better frequency rate at the Polish language which is 42 and fewer than Turkish and English.Furthermore when I compare to frequency in %, Polish is also looks better which means had a less letter complexity.

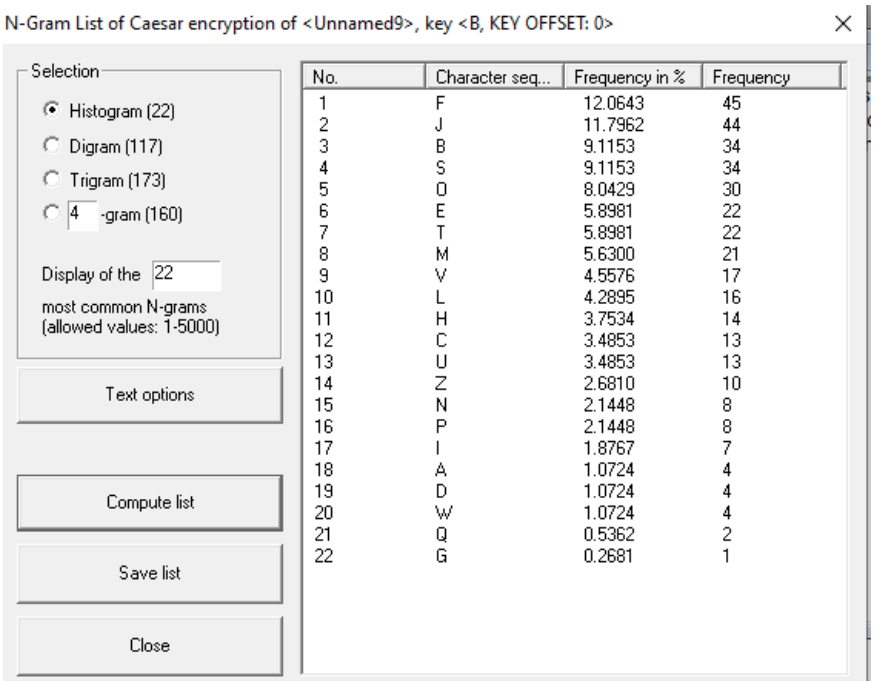
6.Compare n-games (bi/tri/n) of plaintext and ciphertext depending on the algorithm. For algorithms such as in point 2.

substituon

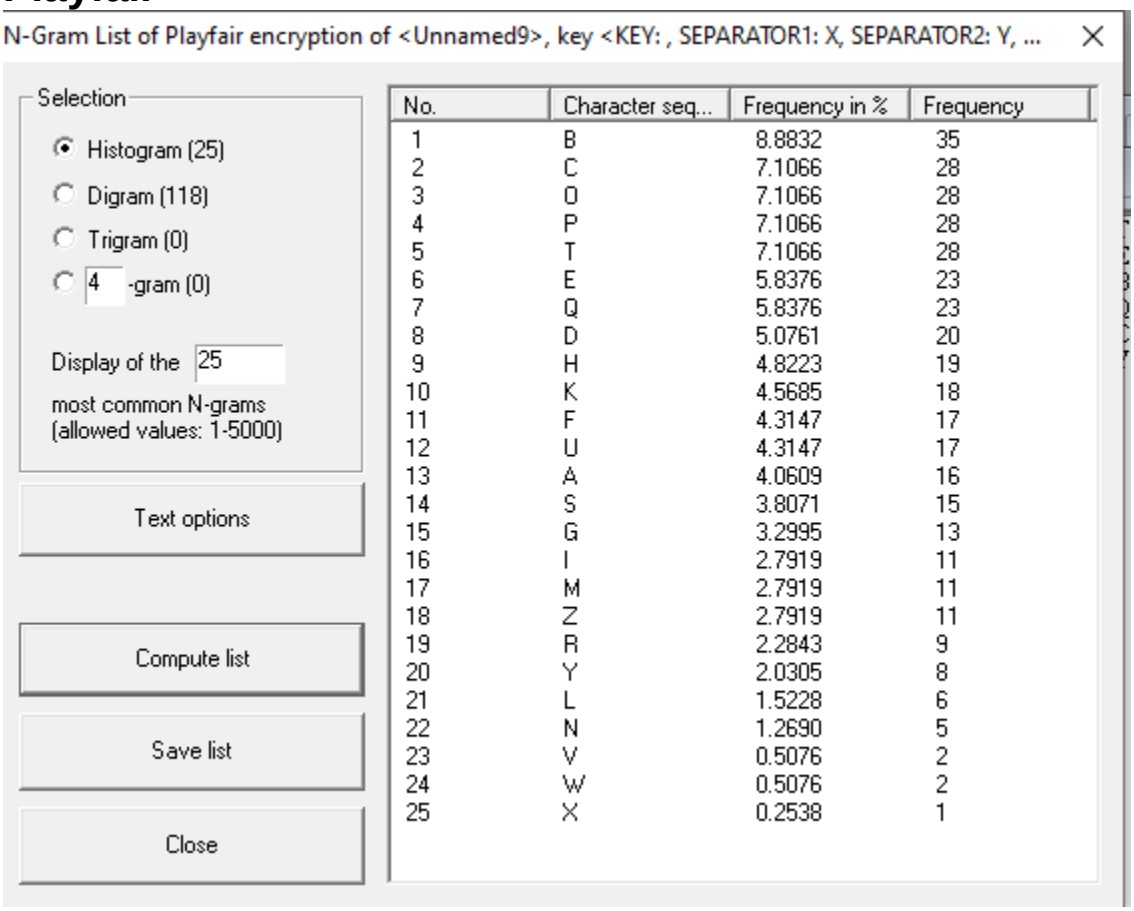


No.	Character seq...	Frequency in %	Frequency
1	E	12.0643	45
2	I	11.7962	44
3	A	9.1153	34
4	R	9.1153	34
5	N	8.0429	30
6	D	5.8981	22
7	S	5.8981	22
8	L	5.6300	21
9	U	4.5576	17
10	K	4.2895	16
11	G	3.7534	14
12	B	3.4853	13
13	T	3.4853	13
14	Y	2.6810	10
15	M	2.1448	8
16	O	2.1448	8
17	H	1.8767	7
18	C	1.0724	4
19	V	1.0724	4
20	Z	1.0724	4
21	P	0.5362	2
22	F	0.2681	1

Caesar


N-Gram List of Caesar encryption of <Unnamed9>, key <B, KEY OFFSET: 0>
Selection
Histogram (22)
Digram (117)
Trigram (173)
4 -gram (160)
Display of the 22
most common N-grams
(allowed values: 1-5000)
Text options
Compute list
Save list
Close
No. Character seq... Frequency in % Frequency
1 F 12.0643 45
2 J 11.7962 44
3 B 9.1153 34
4 S 9.1153 34
5 O 8.0429 30
6 E 5.8981 22
7 T 5.8981 22
8 M 5.6300 21
9 V 4.5576 17
10 L 4.2895 16
11 H 3.7534 14
12 C 3.4853 13
13 U 3.4853 13
14 Z 2.6810 10
15 N 2.1448 8
16 P 2.1448 8
17 I 1.8767 7
18 A 1.0724 4
19 D 1.0724 4
20 W 1.0724 4
21 Q 0.5362 2
22 G 0.2681 1

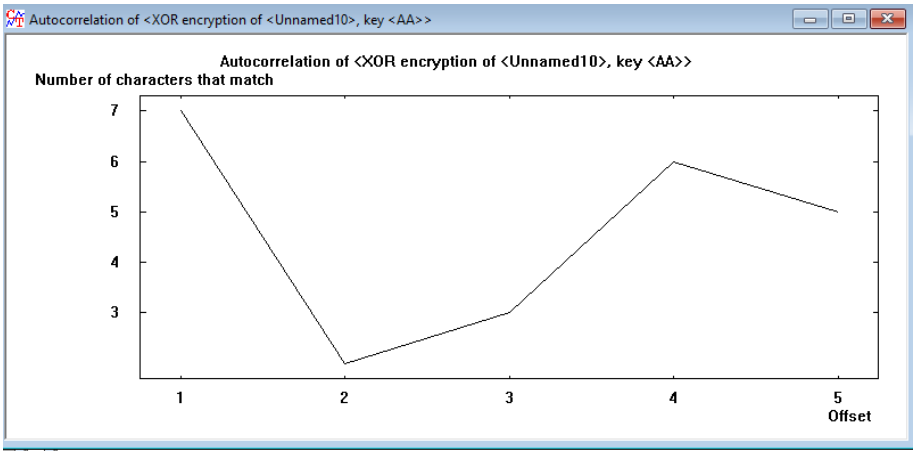
Playfair

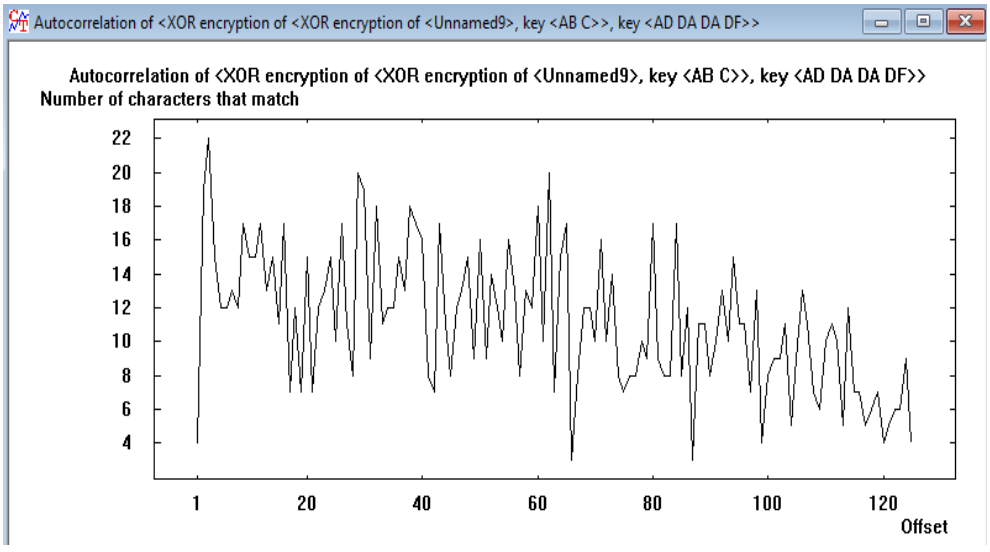

N-Gram List of Playfair encryption of <Unnamed9>, key <KEY: , SEPARATOR1: X, SEPARATOR2: Y, ...
Selection
Histogram (25)
Digram (118)
Trigram (0)
4 -gram (0)
Display of the 25
most common N-grams
(allowed values: 1-5000)
Text options
Compute list
Save list
Close
No. Character seq... Frequency in % Frequency
1 B 8.8832 35
2 C 7.1066 28
3 O 7.1066 28
4 P 7.1066 28
5 T 7.1066 28
6 E 5.8376 23
7 Q 5.8376 23
8 D 5.0761 20
9 H 4.8223 19
10 K 4.5685 18
11 F 4.3147 17
12 U 4.3147 17
13 A 4.0609 16
14 S 3.8071 15
15 G 3.2995 13
16 I 2.7919 11
17 M 2.7919 11
18 Z 2.7919 11
19 R 2.2843 9
20 Y 2.0305 8
21 L 1.5228 6
22 N 1.2690 5
23 V 0.5076 2
24 W 0.5076 2
25 X 0.2538 1

In my case that I didn’t change the language, I come across with the lowest frequency in the PlayFair which means better than Caesar and Substutıon. Also Caesar and susbtutıon almost has the same frequency.

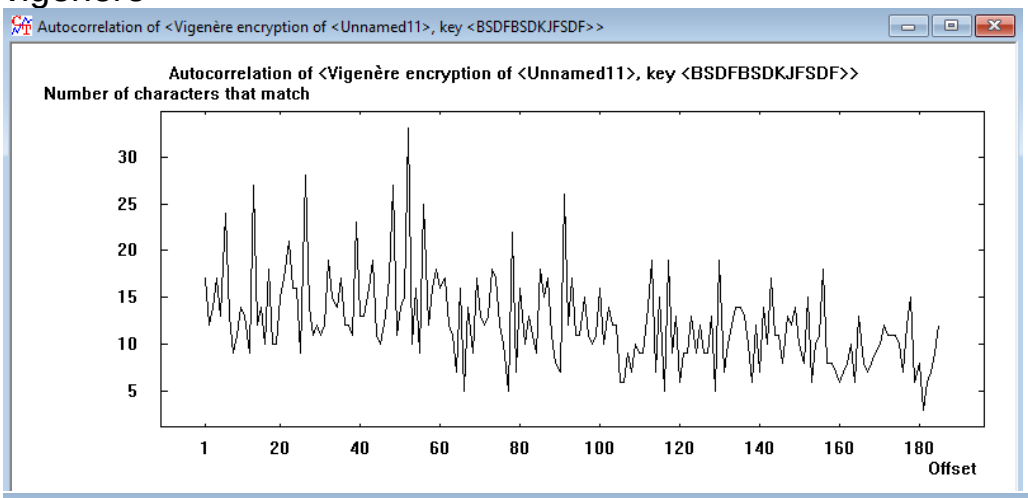
7. Analyze the autocorrelation values of the ciphertext obtained by encryption XOR and Vigenere algorithms for different password lengths.

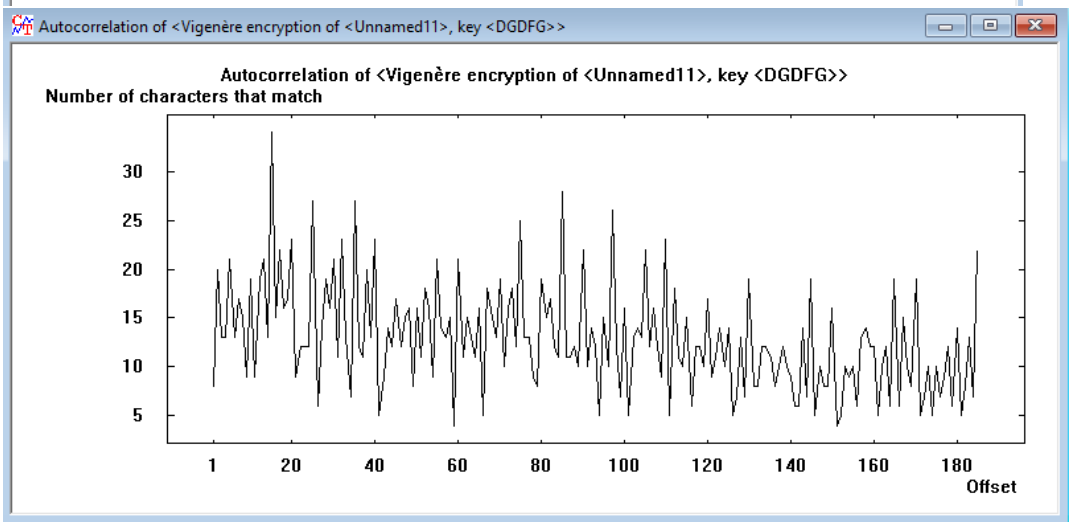
xor





vigenere





According to my examples, more keys I input table got more cramped. İts similar in both situations.

II. Questions/questions

1. **How do the observed parameters change?**
   According to my observation related to algorithms I worked on, parameters changed frequently based on a algorithm. Also given inputs are effect the results. The results were very similar to each other in some comparison but sometimes it was easy the observe the difference between them.

2. **How can the text analysis tools available in CrypTool be used to determine the encryption algorithm for a given ciphertext?**
   we can use the text analysis tools to find the most used letters in the text, than we can start decryption.

II. Questions/questions