Ministerul Educației, Culturii și Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică
Departamentul Ingineria Software și Automatică

Raport

pentru lucrare de laborator Nr. 2
la cursul "*Metode criptografice de protectie a informației*"

A efectuat: Arteom KALAMAGHIN, FAF-211
A verificat: Aureliu ZGUREANU

Chișinău - 2023

Subject: Cryptanalysis of monoalphabetic ciphers

Tasks:

Fie a fost interceptat un mesaj criptat despre care se cunoaște a fost obținut prin utilizarea unui cifru monoalfabetic. Aplicând atacul cu analiza frecvențelor de aflat mesajul original, dacă se presupune că el este un text scris în limba engleză. Țineți cont de faptul că au fost criptate doar literele, celelalte caractere rămânând necriptate.

Decipher process:

I won't provide the full text of the cryptogram here since I find no use in it and if necessary it can be found in the annotation to this laboratory work.

The frequencies of the letters in the english alphabet												
E	T	A	O	I	N	S	H	R	D	L	C	U
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8
M	W	F	G	Y	P	B	V	K	J	X	Q	Z
2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.1	0.07

The frequencies of the letters in the cryptogram												
V	W	P	T	X	N	G	I	Q	S	H	O	Z
12.9	10.0	7.6	7.1	6.8	6.7	6.1	5.9	5.2	4.4	3.7	3.0	3.0
U	D	F	C	A	J	L	R	K	B	Y	E	M
2.9	2.7	2.7	2.2	2.0	1.5	1.2	1.0	0.6	0.3	0.3	0.01	0.0

First of all let's start from analyzing the most common di- and trigraphs. In English, these are TH, HE and THE; in our text - WQ, QV and WQV; taking in account this and correlations in frequencies - I will assume that **d(V) = E**, **d(Q) = H**, **d(W) = T**.

Now the second word (*thePe*) is almost decrypted. There are the two possible decryptions: *there* and *these*, taking into consideration the frequencies my guess is - **d(P) = S**.

All around the text we may encounter *Ae* digraph being a separate word. I guess this to be *be* and it is supported by the frequency data - **d(A) = B**.

After seeking for the strongest correlations between frequencies I deduce four more conjectures: **d(X) = I**, **d(Y) = X**, **d(C) = F**, **d(I) = R**, **d(F) = Y**. After I substitute some, words start taking their shape.

While scanning the text I notice the word *systeZshNDSO* and taking into account the frequencies I consider **d(Z) to be M**, so that *systeZshNDSO* > *systemshNDSO*.

Now the first word in the text is *frNm*, has to be *from* - **d(N) = O**. The next word is *tRo*… *from these two* - **d(R) = W**.

In the third line there is a word *theoretiHTSSy*, even the autocomplete understands that this has to be theoretically: **d(H) = C**, **d(T) = A**, **d(S) = L**.

At this point, when we've successfully got the half of the alphabet, it is just a piece of cake to find all the other letters by just looking at unambiguous partially decrypted words: *fDGOameGtal* > *fundamental* - {**d(D) = U**, **d(G) = N**, **d(O) = D**)}, *UrinciUles* > *principles* - **d(U) = P**, *selectinJ* > *selecting* - **d(J) = G**, *reBuirements* > *requirements* - **d(B) = Q**, *unbreaLable* >*unbreakable* - **d(L) = K**, *oKer* > *over* - **d(K) = V**, *conEure* > *conjure* - **d(E) = J**, *selectinJ* > *selecting* - **d(J) = G**.

The only letter remaining is the one that is not encountered in the text, the least common letter in English - **d(M) = Z**.

The cipher																									
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
T	A	H	O	V	C	J	Q	X	E	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F	M

The original text:

From these two fundamental principles for selecting usable field ciphers, Kerckhoffs deduced six specific requirements: (1) the system should be, if not theoretically unbreakable, unbreakable in practice; (2) compromise of the system should not inconvenience the correspondents; (3) the key should be rememberable without notes and should be easily changeable; (4) the cryptograms should be transmissible by telegraph; (5) the apparatus or documents should be portable and operable by a sinJleperson; (6) the system should be easy, neither requiring knowledge of alonJ list of rules nor involving mental strain. These requirements still comprise the ideal which military ciphers aim at. they have been rephrased, and qualities that lie implicit have -beenmade explicit. but any modern cryptographer would be very happy if any cipher fulfilled all six.of course, it has never been possible to do that. there appears to be a certain incompatibility amonJ them that makes it impossible to institute all of them at once. The requirement that is usually sacrificed is the first. Kerckhoffs argued strongly against the notion of a field cipher that would simply resist solution long enough for the orders it transmitted to be carried out. this was not enough, he said, declaring that "the secret matter in communications sent over a distance very often retains its importance beyond the day on which it was transmitted." he was on the side of the angels, but a practical field cipher that is unbreakable was not possible in his day, nor is it today, and so military cryptography has settled for field ciphers that delay but do not defeat cryptanalysis. Perhaps the most startling requirement, at first glance, was the second. Kerckhoffs explained that by "system" he meant "the material part of the system; tableaux, code books, or whatever mechanical apparatus may be necessary," and not "the key proper." Kerckhoffs here makes for the first time the distinction, now basic to cryptology, between the general system and the specific key. why must the general system "not require secrecy," as, for example, a codebook requires it? Why must it be "a process that. . . our neighbors can even copy and adopt"? because, Kerckhoffs said, "it is not necessary to conjure up imaginary phantoms and to suspect the incorruptibility of employees or subalterns to understand that, if a system requiring secrecy were in the hands of too large a number of individuals, it could be compromised at each engagement in which one or another of them took part." This has proved to be true, and kerckhoffs' second requirement has become widely accepted under a form that is sometimes called the fundamental assumption of military cryptography: that the enemy knows the general system. but he must still be unable to solve messages in it without knowing the specific key. in its modern formulation, the Kerckhoffs doctrine states that secrecy must reside solely in the keys.had Kerckhoffs merely published his perceptions of the problems facing post-telegraph cryptography and his prescriptions for resolving them, he would have assured a place for himself in the pantheon of cryptology. but he did more. He contributed a technique of cryptanalysis that is of supreme importance today. called "superimposition," it constitutes the most general solution for polyalphabetic substitution systems. With few exceptions, it lays no restrictions on the type or length keys, as does the kasiski method, nor on the alphabets, which may be interrelated or entirely independent. it wants only several messages in the same key. The cryptanalyst must align these one above the other so that letters enciphered with the same key letter will fall into a single column. In the simplest case, that of a running key (a very long continuous text used as a key, as a novel) that restarts with each message, he can do this simply by placing all the first letters in the first column, all the second letters in the next column, and so on.

Conclusion:

In conclusion, this laboratory work has provided me with an intriguing glimpse into the world of monolingual encryption, showcasing the historical significance of classical ciphers like frequency-based decryption, which are both fascinating and relatively easy to grasp, albeit outdated in modern cryptography. As I successfully decrypted messages, I not only deepened my understanding of cryptographic techniques but also sharpened my analytical and problem-solving skills, highlighting the enduring relevance of these fundamental skills in the ever-evolving field of cybersecurity. This experience serves as a captivating reminder of how cryptography has evolved over time, with classical ciphers offering valuable insights into its rich history and serving as stepping stones to explore more advanced encryption methods in our digital age.