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(X) = Y**, **d(C) = F**, **d(I) = R**. 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(N) = G**, **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**.

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	U	J	C	N	Q	X	E	L	S	Z	O	N	U	B	I	P	W	D	K	R	Y	X	M

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.