

**Ministerul Educației și Cercetării al Republicii Moldova**  
**Universitatea Tehnică a Moldovei**  
**Facultatea Calculatoare, Informatică și Microelectronică**



## Laboratory work 2: Cryptography and Security

Elaborated:  
st. gr. FAF-211

Echim Mihail

Verified:  
asist. univ.

Aureliu ZGUREANU

Chișinău - 2023

## CRYPTOGRAPHY AND SECURITY

**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. Notă: utilizați serviciul <https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html> Raportul va conține descrierea procesului de spargere, exact la fel cum a fost prezentat în compartimentul 2.3 în Exemplu de atac prin analiza frecvențelor. Fiecare student va lua varianta în conformitate cu numărul său de ordine din lista grupei

**The Process:**

1

W ITG RXWQ TSZNPW DGAVSXVKTASV VCCXHXVGHF. WQV ATJP NC ZTXS CNI  
OVSXKVIFWQTW ZNIGXGJ WN WQV  
VZATPPXVP XG KXVGGT RVIV AINDJQW WN WQV

I noticed this trigram appearing quite often *WVQ* and after looking at the frequency comparison, it became clear that this would be deciphered to **the** [ W -> t; V -> h; Q -> e ]

E	T	A	O
12.7	9.1	8.2	7.5
V	W	T	N
380	274	227	18

2

After making the substitution, *Xt ITG RXth*, this part of the text seemed to me to indicate that X -> i; R -> w; making this **it ITG with**. Admittedly, this is a logical leap, so we'll see where this brings me

3

The most common trigraphs in the english language are:  
THE,AND,THA,ENT,ION,TIO,FOR,NDE,HAS,NCE,TIS,OFT,MEN

The most common trigraphs in the message are:  
WQV,TGO,WVI,VIP,RTP,VIV,XGJ,VWW,SVW,WWV,RXW,XWQ,WQT

After counting the trigraphs and looking over the text, I decided that *TGO* is most likely **and**.  
[T -> a; G -> n; O -> d ].

4

*it lan with ... he lead theZ*

After looking at *he lead theZ*, I wanted to make the leap that I -> l however, seeing another instance of the encoded l in *it lan with* made me think that I -> l making it ***it ran with ... he read theZ***

5

*CNr deSiKerFthat ZNrninJ tN*

After looking this text I thought that *CNr* probably means **for** and after seeing the *tN* at the end of the sentence, it made even more sense for N -> o and subsequently C -> f.

6

*at 7 a.Z. there the SetterP were*

Seeing this text made me certain that Z -> m making it **7 a.m.** Also, I noticed the word *SetterP* which would make sense to translate to **letters** making it S -> l; P -> s

7

*it ran with almost DnAelieKaAle effiHienHF*

This sentence's last word reminded me of the word **efficiency** and it makes sense in the context, so I decided to just go with it, making H -> c; F -> y

8

*it ran with almost DnAelieKaAle efficiency.*

Looking at this sentence now makes me think that *DnAelieKaAle* means **unbelievable**.  
Making it D -> u; A -> b; K -> v

9

*the baJs of mail for deliverythat morninJ to the*

I couldn't for the life of me figure out what the *J* in *baJs* could be, until I saw *morningJ*, which cemented the idea that J -> G

10

*there the letters were oUened by meltingtheir seals with a candle.*

Obviously, *oUened* -> **opened**, making it U -> p

11

*transmit to constantinople, stocLholm, and st. petersburg."*

*stocLholm* -> **stockholm**, so L -> k

12

*armenian, for eYample*

*eYample* -> **example**, so Y -> x

13

*"notEust me—you too."*

This was a little more difficult because I couldn't figure out which letters were still not accounted for. Also, the lack of spaces in certain words made it hard to decipher not knowing if it's *not Eust* or *no tUust*. But using the context of the phrase, I deduced that it means **not just**. Making it E -> j

Finally, the deciphered text:

*it ran with almost unbelievable efficiency. the bags of mail for delivery that morning to the embassies in vienna were brought to the black chamber each day at 7 a.m. there the letters were opened by melting their seals with a candle. the order of the letters in an envelope was noted and the letters given to a subdirector. he read them and ordered the important parts copied. all the employees could write rapidly, and some knew shorthand. long letters were dictated to save time, sometimes using four stenographers to a single letter. if a letter was in a language that he did not know, the subdirector gave it to a cabinet employee familiar with it. two translators were always on hand. all european languages could be read, and when a new one was needed, an official learned it. armenian, for example, took one cabinet polyglot only a few months to learn, and he was paid the usual 500 florins for his new knowledge. after copying, the letters were replaced in their envelopes in their original order and the envelopes re-sealed, using forged seals to impress the original wax. the letters were returned to the post office by 9:30 a.m. at 10 a.m., the mail that was passing through this crossroads of the continent arrived and was handled in the same way, though with less hurry because it was in transit. usually it would be back in the post by 2 p.m., though sometimes it was kept as late as 7 p.m. at 11 a.m., interceptions made by the police for purposes of political surveillance arrived. and at 4 p.m., the couriers brought the letters that the embassies were sending out that day. these were back in the stream of communications by 6:30 p.m. copied material was handed to the director of the cabinet, who excerpted information of special interest and routed it to the proper agencies, as police, army, or railway administration, and sent the mass of diplomatic material to the court. all told, the ten-man cabinet handled an average of between 80 and 100 letters a day. astonishingly, their nimble fingers hardly ever stuffed letters into the wrong packet, despite the speed with which they worked. in one of the few recorded blunders, an intercepted letter to the duke of modena was erroneously re-sealed with the closely similar signet of parma. when the duke noticed the substitution, he sent it to parma with the wry note, "not just me—you too." both states protested, but the viennese greeted them with a blank stare, a shrug, and a bland profession of ignorance. despite this, the existence of the black chamber was well known to the various delegates to the austrian court, and was even tacitly acknowledged by the austrians. when the british ambassador complained humorously that he was getting copies instead of his original correspondence, the chancellor replied coolly, "how clumsy these people are!" enciphered correspondence was subjected to the usual cryptanalytic sweating process. the viennese enjoyed remarkable success in this work. the french ambassador, who was*

*apprised of its successes from papers sold him by a masked man on a bridge, remarked in astonishment*

*that "our ciphers of 1200 [groups] hold out only a little while against the ability of the austrian decipherers." he added that though he suggested new ways of ciphering and continual changes of ciphers, "i still find myself without secure means for the secrets i have to transmit to constantinople, stockholm, and st. petersburg."*

### The Final Key

V	W	T	N	P	G	X	I	Q	S	O	H	U	Z	R	D	J	C	A	F	L	K	Y	E	B	M
e	t	a	o	s	n	i	r	h	l	d	c	p	m	w	u	g	f	b	y	k	v	x	j	?	?

The letters **B** and **M** never appeared in the cipher so we can't be sure which letters they translate to. However, the only unaccounted-for letters are **z** and **q**. So we can safely say, that they translate to them.

### Conclusion

The lack of spaces in certain words threw me off a little bit but it wasn't too much of an issue. I wonder whether it was on purpose or just weird formatting problems. I deciphered the text and learned how the frequency-based attack on ciphers works. It was honestly a ton of fun and I would love to do something similar again.