**Министерство Образования и Исследований**

**Республики Молдова**

**Технический Университет Молдовы**

**Отчет**

по лабораторной работе Nr.2.

по Криптографии

## Тема:

## Криптоанализ одноалфавитных шифров

Выполнил ст.гр.

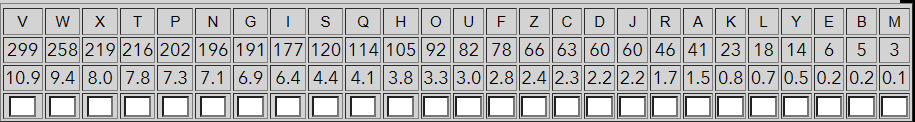
Кишинев

**Задание**. Пусть перехвачено зашифрованное сообщение, о котором известно, что оно было получено с применением моноалфавитного шифра. Примените атаку на основе частотного анализа для поиска исходного сообщения, если предполагается, что это текст, написанный на английском языке. Обратите внимание, что зашифрованы только буквы, остальные символы остаются незашифрованными. Примечание: Воспользуйтесь услугой https://crypto.interactive-maths.com/frequency-analysisbreaking-the-code.html.

Пусть мы перехватили криптограмму **c,** о которой мы знаем, что была получена путем использования моноалфавитного шифра над сообщением, написанным на английском языке:

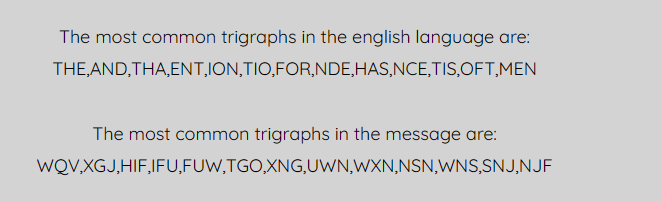
Odixgj tss wqvpv fvtip, hifuwnsnjf rtp thbdxixgj t wtxgw wqtw sxgjvipvkvg wnotf-wqv hngkxhwxng xg wqv zxgop nc ztgf uvnusv wqtw hifuwnsnjfxp t asthl tiw, t cniz nc nhhdswxpz rqnpv uithwxwxngvi zdpw, xg Rxssxtz C.Cixvoztg'p tuw uqitpv, "uvicnihv hnzzdgv otxsf rxwq otil puxixwp wnthhnzusxpq qxp cvtwp nc zvgwts exd-exwpd."Xg utiw xw xp t lxgo nc jdxsw af tppnhxtwxng. Cinz wqv vtisf otfp nc xwpvyxpwvghv, hifuwnsnjf qto pvikvo wn naphdiv hixwxhts uniwxngp nc rixwxgjpovtsxgj rxwq wqv unwvgw pdaevhw nc ztjxh-oxkxgtwxngp, puvssp, hdipvp,rqtwvkvi hngcviivo pduvigtwdits unrvip ng xwp pnihvivip. Tgnwqvixzuniwtgw cthwni rtp wqv hngcdpxng nc hifuwnsnjf rxwq wqv Evrxpqltaatstq.Adw, xzuniwtgw tp tss wqvpv rviv, wqv kxvr wqtw hifuwnsnjf xp asthlztjxh xg xwpvsc puixgjp dswxztwvsf cinz t pduvicxhxts ivpvzastghv avwrvvghifuwnsnjf tgo oxkxgtwxng. Vywithwxgj tg xgwvssxjxasv zvpptjv cinzhxuqviwvyw pvvzvo wn av vythwsf wqv ptzv wqxgj tp nawtxgxgj lgnrsvojvaf vytzxgxgj wqv csxjqw nc axiop, wqv snhtwxng nc pwtip tgo ustgvwp, wqvsvgjwq tgo xgwvipvhwxngp nc sxgvp xg wqv qtgo, wqv vgwitxsp nc pqvvu, wqvunpxwxng nc oivjp xg t wvthdu. Xg tss nc wqvpv, wqv rxmtio-sxlv nuvitwnioitrp pvgpv cinz jinwvpbdv, dgctzxsxti, tgo tuutivgwsf zvtgxgjsvpppxjgp. Qv ztlvp lgnrg wqv dglgnrg.Tss wqxp pwtxgvo hifuwnsnjf pn ovvusf rxwq wqv otil qdvp nc vpnwvixpzwqtw pnzv nc wqvz pwxss uvipxpw, gnwxhvtasf hnsnixgj wqv udasxh xztjv nchifuwnsnjf. Uvnusv pwxss wqxgl hifuwtgtsfpxp zfpwvixndp. Annl ovtsvip pwxsssxpw hifuwnsnjf dgovi "nhhdsw." Tgo xg 1940 wqv Dgxwvo Pwtwvp hngcviivodung xwp Etutgvpv oxusnztwxh hifuwtgtsfpvp wqv hnovgtzv ZTJXH. Xg gngv nc wqv pvhivw rixwxgj wqdp cti rtp wqviv tgf pdpwtxgvohifuwtgtsfpxp. Nhhtpxngts htpvp, fvp. Adw nc tgf phxvghv nc hifuwtgtsfpxp,wqviv rtp gnwqxgj. Ngsf hifuwnjituqf vyxpwvo. Tgo wqvivcniv hifuwnsnjf,rqxhq xgknskvp anwq hifuwnjituqf tgo hifuwtgtsfpxp, qto gnw fvw hnzv xgwn avxgj pncti tp tss wqvpv hdswdivp-xghsdoxgj wqv Rvpwvig -rviv hnghvigvo.Hifuwnsnjf rtp anig tzngj wqv Titap. Wqvf rviv wqv cxipw wn oxphnkvitgo rixwv onrg wqv zvwqnop nc hifuwtgtsfpxp. Wqv uvnusv wqtw vyusnovondw nc Titaxt xg wqv 600p tgo cstzvo nkvi ktpw tivtp nc wqv lgnrg rnisoprxcwsf vgjvgovivo ngv nc wqv qxjqvpw hxkxsxmtwxngp wqtw qxpwnif -qto fvwpvvg. Phxvghv csnrvivo. Tita zvoxhxgv tgo ztwqvztwxhp avhtzv wqv avpwxg wqv rniso-cinz wqv stwwvi, xg cthw, hnzvp wqv rnio "hxuqvi." Uithwxhtstiwp csndixpqvo. Tozxgxpwitwxkv wvhqgxbdvp ovkvsnuvo. Wqv vydavitgwhivtwxkv vgvijxvp nc pdhq t hdswdiv, vyhsdovo af xwp ivsxjxng cinz utxgwxgjni phdsuwdiv, tgo xgpuxivo af xw wn tg vyusxhtwxng nc wqv Qnsf Lnitg,undivo xgwn sxwvitif udipdxwp. Pwnifwvssxgj, vyvzusxcxvo af Pqvqvitmtov'pWqndptgo tgo Ngv Gxjqwp, rnioixoosvp, ivadpvp, udgp, tgtjitzp, tgopxzxsti jtzvp tandgovo; jitzzti avhtzv t zteni pwdof. Tgo xghsdovortp pvhivw rixwxgj.Tcwvi vyustxgxgj wqtw ngv ztf rixwv xg tg dglgnrg stgjdtjv wn nawtxgpvhivhf, Xag to-Oditxqxz, thhnioxgj wn Btsbtpqtgox, jtkv pvkvg pfpwvzpnc hxuqvip. Wqxp sxpw vghnzutppvo, cni wqv cxipw wxzv xg hifuwnjituqf, anwqwitgpunpxwxng tgo pdapwxwdwxng hxuqvip. Znivnkvi, ngv pfpwvz xp wqv cxipwlgnrg hxuqvi vkvi wn uinkxov zniv wqtg ngv pdapwxwdwv cni t ustxgwvywsvwwvi. Ivztiltasv tgo xzuniwtgw tp wqxp xp, qnrvkvi, xw xp nkvipqtonrvo af rqtw cnssnrp- wqv cxipwvyunpxwxng ng hifuwtgtsfpxp xg qxpwnif.

Частота букв в перехваченном тексте:

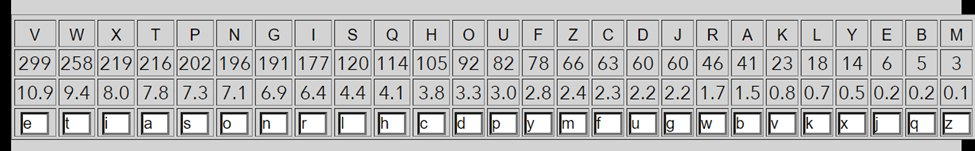


Теперь, когда у нас есть все частоты букв в зашифрованном тексте, мы можем начать делать некоторые замены. Мы видим, что наиболее распространенной буквой в зашифрованном тексте является **«V»,** за которой следует **«W»**

Перейдя в графу “Count Trigraphs” видим наиболее схожие слова с шифра



С помощью этой графы подбираем нам нужные буквы и получаем:



На выходе получаем полностью расшифрованный текст:

during all these years, cryptology was acquiring a taint that lingerseven today-the conviction

in the minds of many people that cryptologyis a black art, a form of occultism whose practitioner

must, in william f.friedman's apt phrase, "perforce commune daily with dark spirits

toaccomplish his feats of mental jiu-jitsu."in part it is a kind of guilt by association.

from the early days of itsexistence, cryptology had served to obscure critical portions of

writingsdealing with the potent subject of magic-divinations, spells, curses,whatever

conferred supernatural powers on its sorcerers. anotherimportant factor was the confusion of

cryptology with the jewishkabbalah.but, important as all these were, the view that cryptology

is blackmagic in itself springs ultimately from a superficial resemblance betweencryptology and

divination. extracting an intelligible message fromciphertext seemed to be exactly the same

thing as obtaining knowledgeby examining the flight of birds, the location of stars and

planets, thelength and intersections of lines in the hand, the entrails of sheep,

theposition of dregs in a teacup. in all of these, the wizard-like operatordraws sense from

grotesque, unfamiliar, and apparently meaninglesssigns. he makes known the unknown.all this

stained cryptology so deeply with the dark hues of esoterismthat some of them still persist,

noticeably coloring the public image ofcryptology. people still think cryptanalysis

mysterious. book dealers stilllist cryptology under "occult." and in 1940 the united

states conferredupon its japanese diplomatic cryptanalyses the codename magic. in none of

the secret writing thus far was there any sustainedcryptanalysis. occasional cases, yes. but

of any science of cryptanalysis,there was nothing. only cryptography existed. and therefore

cryptology,which involves both cryptography and cryptanalysis, had not yet come into being sofar

as all these cultures-including the western -were concerned.cryptology was born among the

arabs. they were the first to discoverand write down the methods of cryptanalysis. the

people that explodedout of arabia in the 600s and flamed over vast areas of the known

worldswiftly engendered one of the highest civilizations that history -had yetseen.

science flowered. arab medicine and mathematics became the bestin the world-from the latter,

in fact, comes the word "cipher." practicalarts flourished. administrative techniques

developed. the exuberantcreative energies of such a culture, excluded by its religion from

paintingor sculpture, and inspired by it to an explication of the holy koran,poured into

literary pursuits. storytelling, exemplified by sheherazade'sthousand and one nights, wordriddles, rebuses, puns, anagrams, andsimilar games abounded; grammar became a major study. and

includedwas secret writing.after explaining that one may write in an unknown language to

obtainsecrecy, ibn ad-duraihim, according to qalqashandi, gave seven systemsof ciphers. this

list encompassed, for the first time in cryptography, bothtransposition and substitution

ciphers. moreover, one system is the firstknown cipher ever to provide more than one

substitute for a plaintextletter. remarkable and important as this is, however, it is

overshadowed by what follows- the firstexposition on cryptanalysis in history.

**Вывод:**Научился расшифровывать перехваченные текста методом криптоанализа