**Ministerul Educaţiei și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**



*Laboratory work 2*

Subject: Monoalphabetic script encryption

Done by: Gitlan Gabriel

st. gr. FAF-213

Verified by: Mîțu Cătălin

asist. univ.

Chişinău - 2023

**Goal:**

A message has been intercepted that is known to have been obtained through the use of a monoalphabetic cipher. By applying frequency analysis attack to discover the original message, assuming it is a text written in English, taking into account that only the letters have been encrypted, leaving the other characters unchanged.

Please use the following service:

https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html

The report will include a description of the breaking process, exactly as presented in section 2.3 in the Example of Frequency Analysis Attack.

**Variant 18**

*Xw rtp Citghv, qnrvkvi, wqtw udasxpqvo ngv nc hifuwnsnjf'p jivtwvpwannlp. St Hifuwnjituqxhzxsxwtxiv cxipw tuuvtivo tp wrn xgpwtsszvgwp xgwqv Endigts ovp Phxvghvp zxsxwtxivp xg Etgdtiftgo Cvaidtif nc 1883,avxgj ivxppdvo stwvi wqtw fvti tp t utuviathl annl af wqv endigts'pudasxpqvi. Xw xp wqv znpw hnghxpv annl ng hifuwnsnjf vkvi rixwwvg. Xwptdwqni qto wqv xgpwxghw cni wqv hifuwnjituqxh edjdsti, tgo qv hnzuivppvoxgwn 64 utjvp kxiwdtssf wqv vgwxiv lgnrg cxvso nc hifuwnsnjf, xghsdoxgjunsftsuqtavwxhp rxwq zxyvo tsuqtavwp, vghxuqvivo hnov, tgo hxuqviovkxhvp. Wqv annl xp tspn ngv nc wqv znpw phqnstisf ng hifuwnsnjf. Xwpcnnwgnwvp hxwv znpw hstppxhts tgo ztgf znovig pndihvp; hnzzvgwp pdhqtp "Wqxp xp gnw wqv ngsf qxpwnixhts ni axasxnjituqxh viini cni rqxhq wqv Tdpwixtg rixwvi zdpw av ivuinthqvo"pqnr qnr htivcdssf wqv tdwqni qtp pwdoxvo wqnpv pndihvp.Xwp tdwqni rtp anig Evtg-Jdxsstdzv-Qdaviw-Kxhwni-Citgjnxp-Tsvytgoiv-djdpwv Lvihlqnccp kng Gxvdrvgqnc ng Etgdtif 19, 1835, twGdwq, Qnsstgo. Tcwvi jvwwxgj ovjivvp xg svwwvip tgo xg phxvghv cinz wqvDgxkvipxwf nc Sxvjv, qv rtp qxivo xg 1863 tp tg xgpwidhwni xg znovigstgjdtjvp tw wqv qxjq phqnns tw Zvsdg, t stijv wnrg 25 zxsvp pndwqvtpwnc Utixp. Wqv gvyw fvti qv ztiixvo t jxis cinz wqv tivt tgo xg 1865, rqvgqv rtp 30, wqvf qto wqvxi ngsf hqxso, t otdjqwvi, Utdsxgv. Qv pwtfvo twZvsdg cni 10 fvtip, wvthqxgj Vgjsxpq tgo Jviztg.Af wqtw wxzv qv qto pqniwvgvo qxp gtzv wn Tdjdpwv Lvihlqnccp.Avtiovo, oxjgxcxvo, psnr nc puvvhq, Lvihlqnccp, ovpuxwv tg xgtaxsxwf wnztxgwtxg oxphxusxgv xg qxp hstppvp tgo pnzv vhhvgwixhxwxvp nc hqtithwvi,rtp t "svtigvo, mvtsndp, htutasv" wvthqvi rqn trnlv qxp pwdovgwp'xgwvivpw xg wqvxi rnil; qxp pduvixnip ptxo "qxp pwdovgwp sxlv qxz tgo rnilrxwq pdhhvpp." Tcwvirtio, qv rnilvo tp t uixktwv xgpwidhwni xg Utixp.Qxp adpxvpw fvtip cnssnrvo wqv udasxhtwxng nc St Hifuwnjituqxhzxsxwtxiv. T gvr xgwvigtwxngts stgjdtjv htssvo Knst-uxxl ("Rniso-Puvtl")qto avvg xgkvgwvo af t Jviztg uixvpw. Tandw 1885, xw htdjqw ng xgCitghv tgo cstpqvo rxwq vyuivpp-witxg puvvo tss nkvi wqv hndgwif, gnwngsf tzngj xgwvssvhwdtsp adw tzngj tss hstppvp; xw rtp vkvg qvtio xg wqvpwivvwp. Cinz Citghv xw itoxtwvo wqindjqndw wqv rniso. Wqv znpw thwxkvuinutjtgoxpw nc Knstuxxl rtp Tdjdpwv Lvihlqnccp, rqn, tw wqv pvhngoKnstuxxl hngjivpp xg Zdgxhq xg 1887, rtp thhstxzvo oxivhwni ("Oxsvlvs,"xg Knstuxxl) nc wqv Xgwvigtwxngts Thtovzf nc Knstuxxl. Adw tw wqv wqxiohngjivpp, qvso tw Utixp xg Ztf nc 1889, rxwq Lvihlqnccp uivpxoxgj, hixwxhtswvgpxngp rxwqxg wqv znkvzvgw zndgwvo tgo cxgtssf ainlv xw tutiw.Lvihlqnccp rtp hidpqvo af wqv hnsstupv nc tg xgwvigtwxngts oivtz wqtwqto pvvzvo pn gvvocds tgo pn hviwtxg. Qv hivtwvo gnwqxgj vspv tgo, ngTdjdpw 9, 1903, oxvo rqxsv ng kthtwxng xg Prxwmvistgo.Adw qxp hifuwnsnjxh xovtp pwxss gndixpq. Cni Lvihlqnccp pndjqw tgprvipwn wqv uinasvzp wqidpw dung hifuwnsnjf af gvr hngoxwxngp. "Xw xpgvhvpptif wn oxpwxgjdxpq htivcdssf avwrvvg t pfpwvz nc vghxuqvizvgwvgkxpxngvo cni t znzvgwtif vyhqtgjv nc svwwvip avwrvvg pvkvits xpnstwvouvnusv tgo t zvwqno nc hifuwnjituqf xgwvgovo wn jnkvig wqv hniivpungovghvavwrvvg oxccvivgw tizf hqxvcp cni tg dgsxzxwvo wxzv," qv rinwv. Xg wqtwngv pvgwvghv, Lvihlqnccp oxccvivgwxtwvp uiv-wvsvjituqf zxsxwtifhnzzdgxhtwxngp cinz unpw-. Wqv pvgwvghv xp uivjgtgw rxwq znpw nc wqvivbdxivzvgwp wqtw qtkv hnzv wn av ovztgovo nc pfpwvzp nc zxsxwtifhifuwnjituqf, ivbdxivzvgwp pdhq tp pxzusxhxwf, ivsxtaxsxwf, ituxoxwf, tgopn ng. Wqxp hsvti ivhnjgxwxng nc wqv gvr niovi hngpwxwdwvp Lvihlqnccp' cxipwjivtw hngwixadwxng wn hifuwnsnjf.Wqv pvhngo rtp wn ivtccxiz xg t znovig hngwvyw wqv uixghxusv wqtw ngsfhifuwtgtsfpwp htg lgnr wqv pvhdixwf nc t hxuqvi pfpwvz. Xw xp wqv cniz ncedojzvgw rqxhq xp pwxss dpvo.*

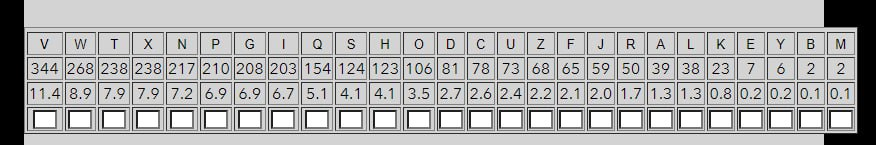
**

Figure 0: Tabel of frequency of th characters

**Figure 1: Replace V→e and T→a**

‘e’ is the most frequent letter in English dictionary, so the replacements must be started with it

****

**Figure 2: Replace Q→h and W→t**

Evident places where the word “the” can be, continuing replacement.

**Figure 3: Replace X→i and N→o**

**Figure 4: Replace P→s and G→n**

**Figure 5: Replace I→r and S→l**

**Figure 6: Replace H→c and O→d**

**Figure 7: Replace D→u and C→f**

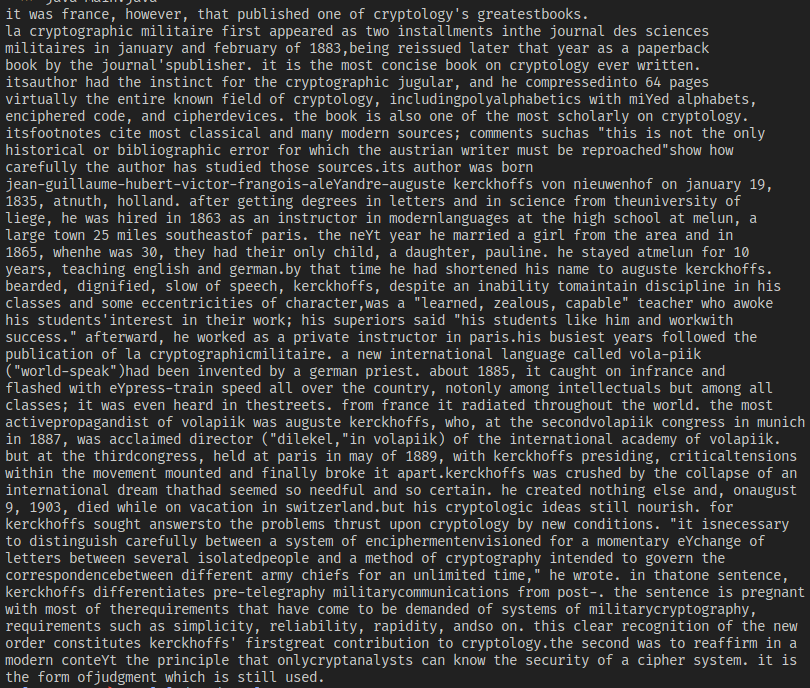
**Figure 8: Replace U→p and Z→m**

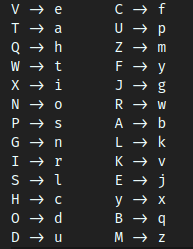
**Figure 9: Replace F→y and J→g**

**Figure 10: Replace R→w and A→b**

**Figure 11: Replace L→k and K→v**

**Figure 12: Replace E→j and X→y**

**Figure 13: Replace B→q and M→z (final result)**

****

**Figure 14: Final decryption table**

**Conclusion:**

At this laboratory work I studied how monoalphabetic decryption works and how to transform letter by letter the text to readable form. As I noticed, it was easier to find ‘a’, because it is the only letter that is single in the article. Then ‘e’, as it is the most common letter in the text and alphabet frequency. I also found the ‘t’ and ‘h’. After that, I had to pass every letter and see whether it fits in the text.