**Ministerul Educaţiei și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**



*Laboratory work 2*

Subject: Criptanaliza cifrurilor monoalfabetice

Done by: Sirețanu Andreia-Cristina

st. gr. FAF-211

Verified by: Mitu Cătălin

Chişinău - 2023

**Subiectul:** Cifrurilor monoalfabetice

**Sarcini:**

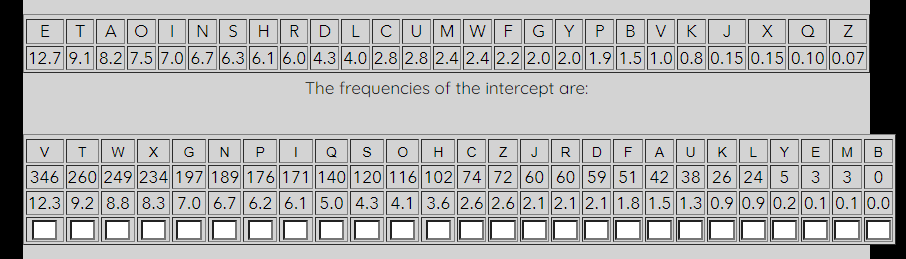
Fie a fost interceptat un mesaj criptat despre care se cunoaște a fost obținut prin utilizarea unui cifru monoalfabetic. Aplicând atacul cu analiza frecvențelor de aflat mesajul original, dacă se presupune că el este un text scris în limba engleză. Țineți cont de faptul că au fost criptate doar literele,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

Notă: utilizați serviciul <https://crypto.interactive-maths.com/frequency-analysis-breaking-thecode.html>

**Etapele efectuării sarcinilor:**

1. Folosind site-ul de mai sus, pentru început, am aflat frecvențele literelor in textul dat în varianta 22. Textul: RQXSV QVIAVIW FTIOSVF ZTF AV WQV AVPW LGNRG HIFUWNSNJXPW,DGHNGWVPWTASF WQV JIVTWVPW XP RXSSXTZ CIVOVIXHL CIXVOZTG. DGSXLV QXPHNGWVZUNITIF, QXP VZXGVGHV XP ODV ZNPW VZUQTWXHTSSF WN RQTW QV OXO.XGOVVO, WRN ZNIV OXPPXZXSTI ZVG XG T PXGJSV CXVSO HTG PHTIHVSF AVXZTJXGVO. RQVIV FTIOSVF RTP ITAVSTXPXTG, NDWJNXGJ, PDUVICXHXTS, CIVV TGOVTPF RXWQ WQV OVWTXSP NC T JNNO PWNIF, TGO VKVI IVTOF CNI WQV ZTXG HQTGHV,CIXVOZTG WVGOVO WNRTIO XGWINKVIPXNG, OVUWQ NC PWDOF, UVIPNGTS PVHDIXWF,WXZXOXWF, OVOXHTWXNG, TGO THHDITHF, GXHVWF, TGO KTSXOXWF NC RNIL. OVPUXWVWQV IVSTWXKV OITAGVPP NC WQVPV UVIPNGTS WITXWP—NI UVIQTUP AVHTDPV NCWQVZ, CIXVOZTG'P WQVNIVWXHTS HNGWIXADWXNGP TGO QXP UITHWXHTS TWWTXGZVGWPVYHVVO WQNPV NC TGF NWQVI HIFUWNSNJXPW. FTIOSVF'P HTIVVI RTP SXLV TGTZTMXGJ PLFINHLVW WQTW VYUSNOVP XG CTGWTPWXH UTWWVIGP TJTXGPW WQVQVTKVGP. CIXVOZTG'P RTP SXLV WQV PDG.QV RTP ANIG RNSCV CIXVOZTG NG PVUWVZAVI 24, 1891, XG LXPQXGVK,IDPPXT, WQV NSOVPW PNG TGO PVHNGO HQXSO NC CIVOVIXHL TGO INPT CIXVOZTG.QXP CTWQVI, T IDZTGXTG RQN PUNLV VXJQW STGJDTJVP TGO RNILVO TP TGXGWVIUIVWVI CNI WQV IDPPXTG UNPW NCCXHV, VZXJITWVO WN TZVIXHT XG 1892, TW RQXHQ WXZV QXP PNG'P GTZV RTP HQTGJVO WN RXSSXTZ. WQV CTZXSF PVWWSVOXG UXWWPADIJQ, RQVIV QXP CTWQVI ZTGTJVO T PVRXGJ ZTHQXGV TJVGHF.RXSSXTZ JITODTWVO XG 1909 TP NGV NC WQV WVG QNGNI PWDOVGWP XG T HSTPP NC300 TW UXWWPADIJQ HVGWITS QXJQ PHQNNS; QV WQVG RVGW WN RNIL TP HQXVCHSVIL XG WQV VIXV HXWF XING RNILP, T CXIZ WQTW PNSO PWVTZ VGJXGVP. TANDWWQTW WXZV WQV ATHL-WN-WQV-CTIZ ZNKVZVGW HTSSVO WN HXWF ANFP, TGO XG WQVCTSS NC 1910, CIXVOZTG TGO WQIVV CIXVGOP VGINSSVO XG ZXHQXJTGTJIXHDSWDITS HNSSVJV, RQNPV HQXVC TWWITHWXNG RTP WQTW XW RTP WDXWXNG-CIVV.ADW CIXVOZTG PNNG OXPHNKVIVO WQTW CTIZXGJ QVSO SXWWSV XGWVIVPW CNI QXZ.QV RTP TG XGKVGWXKV FNDGJ CVSSNR RQN SXLVO WN CXY WQXGJP TGO QTO RIXWWVGPNZV PHXVGHV CXHWXNG CNI QXP QXJQ-PHQNNS UTUVI; QV RTP ITUXOSF HNZXGJ WNWQV HNGHSDPXNG WQTW QV SXLVO PHXVGHV. TW WQV VGO NC WQV WVIZ QV SVTIGVOWQTW WDXWXNG RTP TSPN CIVV XG T PHXVGWXCXH CXVSO TSSXVO WN TJIXHDSWDIV—JVGVWXHP—TW NGV NC WQV XKF SVTJDV DGXKVIPXWXVP, HNIGVSS. QV ANIINRVOWITXG CTIV TGO TIIXKVO XG XWQTHT, GVR FNIL, XG CVAIDTIF, 1911, RQVIV QVJNW T ENA RTXWXGJ NG WTASVP. TCWVI HNZZVGHVZVGW XG CVAIDTIF NC 1914, QVTWWVGOVO JITODTWV PHQNNS, ZTGTJXGJ WN CTSS XG SNKV WRXHV, NGHV RXWQ TAIDGVWWV, NGHV RXWQ WQV ASNGOV OTDJQWVI NC T ZNKXV-QNDPV NRGVI. RQXSVQV RTP WQVIV, T RVTSWQF WVYWXSV ZVIHQTGW, JVNIJV CTAFTG, RQNZTXGWTXGVO STANITWNIXVP XG THNDPWXHP, HQVZXPWIF, JVGVWXHP, TGO HIFU-WNSNJF (WN WIF WN UINKV WQTW ATHNG RINWV PQTLVPUVTIV'P USTFP) NG QXP 500-THIV VPWTWV, IXKVIATGL, TW JVGVKT, XSSXGNXP, OVHXOVO WQTW QV GVVOVO TJVGVWXHXPW WN XZUINKV WQV JITXGP TGO SXKVPWNHL NG QXP CTIZ. QV TUUSXVO WNHNIGVSS CNI T "RNDSO-AV-VI," GNW TG "TP-XP-VI," TGO QXIVO CIXVOZTG, WNAVJXG EDGV 1, 1915.CTAFTG RTP T ZTG NC GN CNIZTS VODHTWXNG ADW NC XGWVSSXJVGHV TGOVGVIJF. QV QTO T JIVTW OVPXIV WN AV "PNZVANOF," TGO WQTW OVPXIVZNWXKTWVO QXP PDAPXOXMXGJ WQV ATHNGXTG PWDOXVP: UINNC NC WQXPIVKNSDWXNGTIF WQVPXP RNDSO HNKVI XWP UTWING TP RVSS TP XWP THWDTSOXPHNKVIVIP RXWQ JSNIF. QV QXZPVSC IVTO SXWWSV, ADW QV TAPNIAVO VGNDJQCINZ WQNPV TINDGO QXZ WN ZTLV QXP WTSL NG TSZNPW TGF PDAEVHW PNDGOXZUIVPPXKV—TW SVTPW PDUVICXHXTSSF. QV RTP TDWNHITWXH, GVKVI TSSNRXGJ QXPPWTCC WN OXPTJIVV RXWQ QXZ, ADW NWQVIRXPV GNW DGUSVTPTGW PN SNGJ TPVZUSNFVVP IVHNJGXMVO WQTW QV RTP ANPP. T HTIOXGTS TIWXHSV NC CTXWQ RXWQQXZ RTP WQTW T RVSS-VYVHDWVO PTSVP HTZUTXJG HNDSO UDW THINPP TSZNPWTGFWQXGJ.

Frecvența:



*Figura 1. Frecvența literelor alfabetului englez și cea a textului dat*

2. Având frecvența literelor și cunoscând unele lucruri specifice limbii engleze (ex. O literă aparte formeză deobicei articolul “a”, iar 3 litere ămpreună, deobicei alcătuiesc aticolul “the”) am început să înlocuim primele litere și să aflăm rezultatul acestei înlocuiri.

Literele: V -> E; T=>A; W=>T; Q=>H;

Primul rezultat: RhXSe heIAeIt FaIOSeF ZaF Ae the AePt LGNRG HIFUtNSNJXPt,DGHNGtePtaASF the JIeatePt XP RXSSXaZ CIeOeIXHL CIXeOZaG. DGSXLe hXPHNGteZUNIaIF, hXP eZXGeGHe XP ODe ZNPt eZUhatXHaSSF tN Rhat he OXO.XGOeeO, tRN ZNIe OXPPXZXSaI ZeG XG a PXGJSe CXeSO HaG PHaIHeSF AeXZaJXGeO. RheIe FaIOSeF RaP

IaAeSaXPXaG, NDtJNXGJ, PDUeICXHXaS, CIee aGOeaPF RXth the OetaXSP NC a JNNO PtNIF, aGO eKeI IeaOF CNI the ZaXG HhaGHe,CIXeOZaG teGOeO tNRaIO XGtINKeIPXNG, OeUth NC PtDOF, UeIPNGaS PeHDIXtF,tXZXOXtF, OeOXHatXNG, aGO aHHDIaHF, GXHetF, aGO KaSXOXtF NC RNIL. OePUXtethe IeSatXKe OIaAGePP NC thePe UeIPNGaS tIaXtP—NI UeIhaUP AeHaDPe NCtheZ, CIXeOZaG'P theNIetXHaS HNGtIXADtXNGP aGO hXP UIaHtXHaS attaXGZeGtPeYHeeO thNPe NC aGF NtheI HIFUtNSNJXPt. FaIOSeF'P HaIeeI RaP SXLe aGaZaMXGJ PLFINHLet that eYUSNOeP XG CaGtaPtXH

UatteIGP aJaXGPt theheaKeGP. CIXeOZaG'P RaP SXLe the PDG.he RaP ANIG RNSCe CIXeOZaG NG PeUteZAeI 24, 1891, XG LXPhXGeK, IDPPXa, the NSOePt PNG aGO PeHNGO HhXSO NC CIeOeIXHL aGO INPa CIXeOZaG. hXP CatheI, a IDZaGXaG RhN PUNLe eXJht SaGJDaJeP aGO RNILeO aP aGXGteIUIeteI CNI the IDPPXaG UNPt NCCXHe, eZXJIateO tN aZeIXHa XG

1892, at RhXHh tXZe hXP PNG'P GaZe RaP HhaGJeO tN RXSSXaZ. the CaZXSF PettSeOXG UXttPADIJh, RheIe hXP CatheI ZaGaJeO a PeRXGJ ZaHhXGe aJeGHF. RXSSXaZ JIaODateO XG 1909 aP NGe NC the teG hNGNI PtDOeGtP XG a HSaPP NC300 at UXttPADIJh HeGtIaS hXJh PHhNNS; he theG ReGt tN RNIL aP HhXeCHSeIL XG the eIXe HXtF XING RNILP, a CXIZ that PNSO PteaZ eGJXGeP. aANDtthat tXZe the AaHL-tN-the-CaIZ ZNKeZeGt HaSSeO tN HXtF ANFP, aGO XG theCaSS NC 1910, CIXeOZaG aGO thIee CIXeGOP eGINSSeO XG ZXHhXJaGaJIXHDStDIaS HNSSeJe, RhNPe HhXeC attIaHtXNG RaP

that Xt RaP tDXtXNG-CIee. ADt CIXeOZaG PNNG OXPHNKeIeO that CaIZXGJ heSO SXttSe XGteIePt CNI hXZ.he RaP aG XGKeGtXKe FNDGJ CeSSNR RhN SXLeO tN CXY thXGJP aGO haO RIXtteGPNZe PHXeGHe CXHtXNG CNI hXP hXJh-PHhNNS UaUeI; he RaP IaUXOSF HNZXGJ tNthe HNGHSDPXNG that he SXLeO PHXeGHe. at the eGO NC the teIZ he SeaIGeOthat tDXtXNG RaP aSPN CIee XG a PHXeGtXCXH CXeSO aSSXeO tN aJIXHDStDIe—JeGetXHP—at NGe NC the XKF SeaJDe DGXKeIPXtXeP, HNIGeSS. he ANIINReOtIaXG CaIe aGO aIIXKeO XG XthaHa, GeR FNIL, XG CeAIDaIF, 1911, RheIe heJNt a ENA RaXtXGJ NG taASeP. aCteI HNZZeGHeZeGt XG CeAIDaIF NC 1914, heatteGOeO JIaODate PHhNNS,

ZaGaJXGJ tN CaSS XG SNKe tRXHe, NGHe RXth aAIDGette, NGHe RXth the ASNGOe OaDJhteI NC a ZNKXe-hNDPe NRGeI. RhXSehe RaP theIe, a ReaSthF teYtXSe ZeIHhaGt, JeNIJe CaAFaG, RhNZaXGtaXGeO SaANIatNIXeP XG

aHNDPtXHP, HheZXPtIF, JeGetXHP, aGO HIFU-tNSNJF (tN tIF tN UINKe that AaHNG RINte PhaLePUeaIe'P USaFP) NG hXP 500-aHIe ePtate, IXKeIAaGL, at JeGeKa, XSSXGNXP, OeHXOeO that he GeeOeO aJeGetXHXPt tN XZUINKe

the JIaXGP aGO SXKePtNHL NG hXP CaIZ. he aUUSXeO tNHNIGeSS CNI a "RNDSO-Ae-eI," GNt aG "aP-XP-eI," aGO hXIeO CIXeOZaG, tNAeJXG EDGe 1, 1915.CaAFaG RaP a ZaG NC GN CNIZaS eODHatXNG ADt NC XGteSSXJeGHe

aGOeGeIJF. he haO a JIeat OePXIe tN Ae "PNZeANOF," aGO that OePXIeZNtXKateO hXP PDAPXOXMXGJ the AaHNGXaG PtDOXeP: UINNC NC thXPIeKNSDtXNGaIF thePXP RNDSO HNKeI XtP UatING aP ReSS aP XtP aHtDaSOXPHNKeIeIP RXth JSNIF. he hXZPeSC IeaO SXttSe, ADt he aAPNIAeO eGNDJhCINZ thNPe aINDGO hXZ tN ZaLe hXP taSL NG aSZNPt aGF PDAEeHt PNDGOXZUIePPXKe—at SeaPt PDUeICXHXaSSF. he RaP aDtNHIatXH, GeKeI aSSNRXGJ hXPPtaCC tN OXPaJIee RXth hXZ, ADt NtheIRXPe GNt DGUSeaPaGt PN SNGJ aPeZUSNFeeP IeHNJGXMeO that he RaP ANPP. a HaIOXGaS aItXHSe NC CaXth RXthhXZ RaP that a ReSS-eYeHDteO PaSeP HaZUaXJG HNDSO UDt aHINPP aSZNPtaGFthXGJ.

3. Înlocuind tot așa după cea mai mare frecvență și restul literelor 3 a câte 3 și analizând cum se formează cuvintele pentru a nu crea errori am ajuns la un sfârșit a decriptării textului:

while herbert yardley may be the best known cryptologist,uncontestably the greatest is william frederick friedman. unlike hiscontemporary, his eminence is due most emphatically to what he did.indeed, two more dissimilar men in a single field can scarcely beimagined. where yardley was rabelaisian, outgoing, superficial, free andeasy with the details of a good story, and ever ready for the main chance,friedman tended toward introversion, depth of study, personal security,timidity, dedication, and accuracy, nicety, and validity of work. despitethe relative drabness of these personal traits—or perhaps because ofthem, friedman's theoretical contributions and his practical attainmentsexceed those of any other cryptologist. yardley's career was like anamazing skyrocket that explodes in fantastic patterns against theheavens. friedman's was like the sun.he was born wolfe friedman on september 24, 1891, in kishinev, russia, the oldest son and second child of frederick and rosa friedman. his father, a rumanian who spoke eight languages and worked as aninterpreter for the russian post office, emigrated to america in

1892, at which time his son's name was changed to william. the family settledin pittsburgh, where his father managed a sewing machine agency. william graduated in 1909 as one of the ten honor students in a class of300 at pittsburgh central high school; he then went to work as chiefclerk in the erie city iron works, a firm that sold steam engines. aboutthat time the back-to-the-farm movement called to city boys, and in thefall of 1910, friedman and three friends enrolled in michiganagricultural college, whose chief attraction was that it was tuition-free. but friedman soon discovered that farming held little interest for him.he was an inventive young fellow who liked to fix things and had writtensome science fiction for his high-school paper; he was rapidly coming tothe conclusion that he liked science. at the end of the term he learnedthat tuition was also free in a scientific field allied to agriculture—genetics—at one of the ivy league universities, cornell. he borrowedtrain fare and arrived in ithaca, new york, in february, 1911, where hegot a job waiting on tables. after commencement in february of 1914, heattended graduate school, managing to fall in love twice, once with abrunette, once with the blonde daughter of a movie-house owner. whilehe was there, a wealthy textile merchant, george fabyan, whomaintained laboratories in acoustics, chemistry, genetics, and cryp-tology (to try to prove that bacon wrote shakespeare's plays) on his 500-acre estate, riverbank, at geneva, illinois, decided that he needed ageneticist to improve the grains and livestock on his farm. he applied tocornell for a "would-be-er," not an "as-is-er," and hired friedman, tobegin june 1, 1915.fabyan was a man of no formal education but of intelligence

andenergy. he had a great desire to be "somebody," and that desiremotivated his subsidizing the baconian studies: proof of thisrevolutionary thesis would cover its patron as well as its actualdiscoverers with glory. he himself read little, but he absorbed enoughfrom those around him to make his talk on almost any subject soundimpressive—at least superficially. he was autocratic, never allowing hisstaff to disagree with him, but otherwise not unpleasant so long asemployees recognized that he was boss. a cardinal article of faith withhim was that a well-executed sales campaign could put across almostanything.

**Concluzie:** Folosind cifrul monoalfabetic am învățat o metodă nouă, interesantă și utilă de criptare a informației ce ma ajutat la soluționarea descifrării acestui text. Ma învățat să gândesc într-un mod abstract și logic, având multă răbdare în activitatea aceasta.