Ministry of Education, Culture and Research of the Republic of Moldova

Technical University of Moldova

Department of Software and Automation Engineering

REPORT

Laboratory Work Nr.2
Discipline: Cryptographic methods of information protection

Realised by: st.gr. FAF-213
Iațco Sorin

Checked by : lect.univ.
Mîțu Cătălin

Chișinău 2023

Subject: Cryptanalysis of monoalphabetic ciphers.

Tasks:

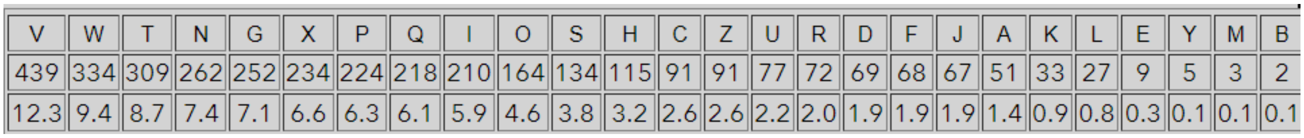
Given an encrypted message known to have been intercepted has been obtained by using a monoalphabetic cipher. Applying the attack with frequency analysis to find out the original message, if assumes that it is a text written in English. Keep in mind that they were only encrypted letters, other characters remaining unencrypted.

Results:

Having the variant with nr.21, I intercepted a cryptogram c, which we know was obtained as a result of using a monoalphabetical cipher over a message written in English:

c = *Ftiosvf'p tuuinuixtwxng qto avvg pvkvivsf hdw xg 1924, tgo qtsc wqvpwtcc qto wn av svw jn, ivodhxgj wqv cnihv wn tandw t onmvg. Ovpuxwv wqxp,Ftiosvf ptxo, wqv Asthl Hqtzavi ztgtjvo wn pnskv, cinz 1917 wn 1929,zniv wqtg 45,000 wvsvjitzp, xgknskxgj wqv hnovp nc Tijvgwxgt, Aitmxs,Hqxsv, Hqxgt, Hnpwt Ixht, Hdat, Vgjstgo, Citghv, Jviztgf, Etutg,Sxavixt, Zvyxhn, Gxhtitjdt, Utgtzt, Uvid, Ptg Ptsktoni, Ptgwn Onzxgjn(stwvi wqv Onzxgxhtg Ivudasxh) wqv Pnkxvw Dgxng, tgo Putxg tgo ztovuivsxzxgtif tgtsfpvp nc ztgf nwqvi hnovp, xghsdoxgj wqnpv nc wqv Ktwxhtg.Pdoovgsf xw tss vgovo. Ftiosvf, rqn qto avvg nawtxgxgj wqv hnovwvsvjitzp nc cnivxjg jnkvigzvgwp wqindjq wqv hnnuvitwxng nc wqvuivpxovgwp nc wqv Rvpwvig Dgxng Wvsvjituq Hnzutgf tgo wqv UnpwtsWvsvjituq Hnzutgf, rtp vghndgwvixgj xghivtpxgj ivpxpwtghv cinz wqvz.Qviaviw Qnnkvi qto edpw avvg xgtdjditwvo, tgo Ftiosvf ivpnskvo wn pvwwsv wqv ztwwvi rxwq wqv gvr tozxgxpwitwxng nghv tgo cni tss. Qvovhxovo ng wqv anso pwinlv nc oitrxgj du "t zvznitgodz wn avuivpvgwvo oxivhwsf wn wqv Uivpxovgw, ndwsxgxgj wqv qxpwnif tgo thwxkxwxvp ncwqv Asthl Hqtzavi, tgo wqv gvhvpptif pwvup wqtw zdpw av wtlvg xc wqvJnkvigzvgw qto qnuvo wn wtlv cdss toktgwtjv nc wqv plxss nc xwphifuwnjituqvip." Qv rtxwvo wn pvv rqxhq rtf wqv rxgo rtp asnrxgj avcnivztlxgj qxp znkv— tgo cndgo wqtw xw rtp gnw rxwq qxz. Ftiosvf rvgw wn tpuvtlvtpf wn sxpwvg wn Qnnkvi'p cxipw puvvhq tp Uivpxovgw tgo pvgpvo, xgwqv qxjq vwqxhts pwixhwdivp wqtw Qnnkvi vyuivppvo, wqv onnz nc wqv AsthlHqtzavi.Qv rtp ixjqw, wqndjq xwp thwdts hsnpxgj htzv cinz vspvrqviv. TcwviQvgif S. Pwxzpng, Qnnkvi'p Pvhivwtif nc Pwtwv, qto avvg xg nccxhv wqv cvrzngwqp wqtw Ftiosvf wqndjqw rndso av gvhvpptif cni qxz wn qtkv snpwpnzv nc qxp xggnhvghv xg rivpwsxgj rxwq wqv qtioqvtovo ivtsxwxvp ncoxusnzthf, wqv Asthl Hqtzavi pvgw qxz wqv pnsdwxng nc tg xzuniwtgwpvixvp nc zvpptjvp. Adw Pwxzpng rtp oxccvivgw cinz uivkxndp Pvhivwtixvpnc Pwtwv, ng rqnz wqxp wthwxh qto tsrtfp rnilvo. Qv rtp pqnhlvo wnsvtig nc wqv vyxpwvghv nc wqv Asthl Hqtzavi, tgo wnwtssf oxptuuinkvo nc xw.Qv ivjtiovo xw tp t snr, pgnnuxgj thwxkxwf, t pgvtlxgj, pufxgj, lvfqnsv-uvvixgj lxgo nc oxiwf adpxgvpp, t kxnstwxng nc wqv uixghxusv nc zdwdts widpwdung rqxhq qv hngodhwvo anwq qxp uvipngts tcctxip tgo qxp cnivxjgunsxhf. Tss nc wqxp xw xp, tgo Pwxzpng ivevhwvo wqv kxvr wqtw pdhq zvtgpedpwxcxvo vkvg utwixnwxh vgop. Qv qvso wn wqv hngkxhwxng wqtw qxp hndgwifpqndso on rqtw xp ixjqw, tgo, tp qv ptxo stwvi, "Jvgwsvzvg on gnw ivtovthq nwqvi'p ztxs." Xg tg thw nc udiv znits hnditjv, Pwxzpng, tccxizxgjuixghxusv nkvi vyuvoxvghf, rxwqoivr tss Pwtwv Ovutiwzvgw cdgop cinz* *wqvpduuniw nc wqv Asthl Hqtzavi.* Pxghv wqvpv hngpwxwdwvo xwp ztenixghnzv, wqvxi snpp pqdwwvivo wqv nccxhv. Qnnkvi'p puvvhq qto rtigvoFtiosvf wqtw tg tuuvts rndso av cidxwsvpp. Wqviv rtp gnwqxgj wn on adwhsnpv du pqnu.Xg 1940, tp Pvhivwtif nc Rti, qv qto wn ivkvipv qxzpvsc tgo thhvuwwqv hifuwtgtsfpvp nc ZTJXH. Adw wqv xgwvigtwxngts pxwdtwxng wqvg rtpwnwtssf oxccvivgw. "Xg 1929," qv qxzpvsc qtp rixwwvg, xg wqv wqxio uvipng,"wqv rniso rtp pwixkxgj rxwq jnno rxss cni stpwxgj uvthv, tgo xg wqxp vccniwtss wqv gtwxngp rviv utiwxvp. Pwxzpng, tp Pvhivwtif nc Pwtwv, rtp ovtsxgjtp t jvgwsvztg rxwq wqv jvgwsvzvg pvgw tp tzatpptonip tgo zxgxpwvipcinz cixvgosf gtwxngp. ..." Xg 1940, Vdinuv rtp tw rti, tgo wqv DgxwvoPwtwvp rtp ng wqv kvijv.Wqv Pxjgts Hniup, rqviv Rxssxtz Cixvoztg qto hqtijv nc hifuwnsnjf.Wqv pwtcc bdxhlsf oxpuvipvo (gngv rvgw wn wqv Tizf), tgo rqvg wqv annlprviv hsnpvo ng Nhwnavi 31, 1929, wqv Tzvixhtg Asthl Hqtzavi qtouvixpqvo. Xw qto hnpw wqv Pwtwv Ovutiwzvgw $230,404 tgo wqv RtiOvutiwzvgw $98,808.49—edpw dgovi t wqxio nc t zxssxng onsstip cni tovhtov nc hifuwtgtsfxp. Ftiosvf, rqnpv ena vyuvixvghv qto avvg itwqvi puvhxtsxmvo, hndso gnwcxgo rnil, tgo qv rvgw athl qnzv wn Rniwqxgjwng. Wqv Ovuivppxngpdhlvo qxz oif. Af Tdjdpw nc 1930, qv qto qto wn jxkv du tg tutiwzvgwqndpv tgo t ngv-vxjqwq xgwvivpw xg t ivts vpwtwv hniunitwxng; xgovvo, qvhnzustxgvo wqtw qv qto wn pvss gvtisf vkvifwqxgj qv nrgvo "cni svpp wqtggnwqxgj." T cvr zngwqp stwvi qv rtp wnfxgj rxwq wqv xovt nc rixwxgj wqvpwnif nc wqv Asthl Hqtzavi wn ztlv pnzv zngvf wn cvvo qxp rxcv tgowqvxi png, Ethl. Rqvg qxp nso ZX-8 cixvgo, Ztgsf, rxwq rqnz qv qtoavvg xg hngwthw tss odixgj wqv 1920'p, qto wn wdig onrg qxp ivbdvpw cni t$2,500 sntg tw wqv vgo nc Etgdtif, 1931, Ftiosvf, xg ovpuvitwxng, ptwonrg wn rixwv rqtw rtp wn av wqv znpw ctzndp annl ng hifuwnsnjf vkviudasxpqvo.*

The first step is to find the frequencies of all the letters that appear in the cryptogram, as shown in (table 1).



V	W	T	N	G	X	P	Q	I	O	S	H	C	Z	U	R	D	F	J	A	K	L	E	Y	M	B
439	334	309	262	252	234	224	218	210	164	134	115	91	91	77	72	69	68	67	51	33	27	9	5	3	2
12.3	9.4	8.7	7.4	7.1	6.6	6.3	6.1	5.9	4.6	3.8	3.2	2.6	2.6	2.2	2.0	1.9	1.9	1.9	1.4	0.9	0.8	0.3	0.1	0.1	0.1

Table 1. *Frequency of the letters of the intercepted cryptogram*

Now that we have all the frequencies we can watch and analyze what are the most frequent letters in the English alphabet and what are the most common letters in our alphabet to intercept, so I see that *"E"* and *"T"* are the most frequent in the English alphabet and in my alphabet to intercept the letters *"V"* and *"W"* are the most frequent so I substitute *"V"* with *"I"*, and *"W"* with *"T"*, after this I got:

FTIOSeF'P TUUINUIXTtXNG QTO AeeG PeKeIeSF HDt XG 1924, TGO QTSC tQePtTCC QTO tN Ae Set JN, IeODHXGJ ***tQe*** *CNIHe tN TANDt T ONMeG. OePUXte tQXP,FTIOSeF PTXO,* ***tQe*** *ASTHL HQTZAeI ZTGTJeO tN PNSKe, CINZ 1917 tN 1929,ZNIe tQTG 45,000 teSeJITZP, XGKNSKXGJ* ***tQe*** *HNOeP NC TIJeGtXGT, AITMXS,HQXSe, HQXGT, HNPtT IXHT, HDAT, eGJSTGO, CITGHe, JeIZTGF, ETUTG,SXAeIXT, ZeYXHN, GXHTITJDT,* *UTGTZT, UeID, PTG PTSKTONI, PTGtN ONZXGJN(STteI **tQe** ONZXGXHTG IeUDASXH) **tQe** PNKXet DGXNG, TGO PUTXG TGO ZTOeUIeSXZXGTIF TGTSFPeP NC ZTGF NtQeI HNOeP, XGHSDOXGJ tQNPe NC **tQe** KTtXHTG.PDOOeGSF Xt TSS eGOeO. FTIOSeF, RQN QTO AeeG NAtTXGXGJ **tQe** HNOeteSeJITZP NC CNIeXJG JNKeIGZeGtP tQINDJQ **tQe** HNNUeITtXNG NC tQeUIePXOeGtP NC **tQe** RePteIG DGXNG teSeJITUQ HNZUTGF TGO **tQe** UNPtTSteSeJITUQ HNZUTGF, RTP eGHNDGteIXGJ XGHIeTPXGJ IePXPtTGHe CINZ tQeZ.QeIAeIt QNNKeI QTO EDPt AeeG XGTDJDITteO, TGO FTIOSeF IePNSKeO tN PettSe **tQe** ZTtteI RXtQ **tQe** GeR TOZXGXPtITtXNG NGHe TGO CNI TSS. QeOeHXOeO NG **tQe** ANSO PtINLe NC OITRXGJ DU "T ZeZNITGODZ tN AeUIePeGteO OXIeHtSF tN **tQe** UIePXOeGt, NDtSXGXGJ **tQe** QXPtNIF TGO THtXKXtXeP NCtQe ASTHL HQTZAeI, TGO **tQe** GeHePPTIF PteUP tQTt ZDPt Ae tTLeG XC tQeJNKeIGZeGt QTO QNUeO tN tTLe CDSS TOKTGtTJe NC **tQe** PLXSS NC XtPHIFUtNJITUQeIP." Qe RTXteO tN Pee RQXHQ RTF **tQe** RXGO RTP ASNRXGJ AeCNIeZTLXGJ QXP ZNKe—TGO CNDGO tQTt Xt RTP GNt RXtQ QXZ. FTIOSeF ReGt tN TPUeTLeTPF tN SXPteG tN QNNKeI'P CXIPt PUeeHQ TP UIePXOeGt TGO PeGPeO, XGtQe QXJQ etQXHTS PtIXHtDIeP tQTt QNNKeI eYUIePPeO, **tQe** ONNZ NC **tQe** ASTHLHQTZAeI.Qe RTP IXJQt, tQNDJQ XtP THtDTS HSNPXGJ HTZe CINZ eSPeRQeIe. TCteIQeGIF S. PtXZPNG, QNNKeI'P PeHIetTIF NC PtTte, QTO AeeG XG NCCXHe **tQe** CeRZNGtQP tQTt FTIOSeF tQNDJQt RNDSO Ae GeHePPTIF CNI QXZ tN QTKe SNPtPNZe NC QXP XGGNHeGHe XG RIePtSXGJ RXtQ **tQe** QTIOQeTOeO IeTSXtXeP NCOXUSNZTHF, **tQe** ASTHL HQTZAeI PeGt QXZ **tQe** PNSDtXNG NC TG XZUNItTGtPeIXeP NC ZePPTJeP.*

We now notice that the word *"tQe"* appears frequently in the passage. In English, the most common word from 3 letters is *"the"* and this matches what I have already done, which suggests that *"Q"* would must be decrypted to *"H"*.

Also I observed the next most frequent letter in my cypher alphabet is *“N”* which may be either *”A”, “O”* or *“I”*, so next I observe that a common word is *“tN”* which can be a common digraph in English language *”to”* and I substitute *“N”* with *“O”* so I get:

*FTIOSeF'P TUUIoUIXTtXoG hTO AeeG PeKeIeSF HDt XG 1924, TGO hTSC thePtTCC hTO to Ae Set Jo, IeODHXGJ the CoIHe to TAoDt T OoMeG. OePUXte thXP,FTIOSeF PTXO, the ASTHL HhTZAeI ZTGTJeO to PoSKe, CIoZ 1917 to 1929,ZoIe thTG 45,000 teSeJITZP, XGKoSKXGJ the HoOeP **oC** TIJeGtXGT, AITMXS,HhXSe, HhXGT, HoPtT IXHT, HDAT, eGJSTGO, CITGHe, JeIZTGF, ETUTG,SXAeIXT, ZeYXHo, GXHTITJDT, UTGTZT, UeID, PTG PTSKTOoI, PTGto OoZXGJo(STteI the OoZXGXHTG IeUDASXH) the PoKXet DGXoG, TGO PUTXG TGO ZTOeUIeSXZXGTIF TGTSFPeP **oC** ZTGF **otheI** HoOeP, XGHSDOXGJ thoPe **oC** the KTtXHTG.PDOOeGSF Xt TSS eGOeO. FTIOSeF, Rho hTO AeeG oAtTXGXGJ the HoOeteSeJITZP **oC** CoIeXJG JoKeIGZeGtP thIoDJh the HooUeITtXoG **oC** theUIePXOeGtP **oC** the RePteIG DGXoG teSeJITUh HoZUTGF TGO the UoPtTSteSeJITUh HoZUTGF, RTP eGHoDGteIXGJ XGHIeTPXGJ IePXPtTGHe CIoZ theZ.heIAeIt hooKeI hTO EDPt AeeG XGTDJDITteO, TGO FTIOSeF IePoSKeO to PettSe the*

*ZTtteI RXth the GeR TOZXGXPtITtXoG oGHe TGO CoI TSS. heOeHXOeO oG the AoSO PtIoLe **oC** OITRXGJ DU "T ZeZoITGODZ to AeUIePeGteO OXIeHtSF to the UIePXOeGt, oDtSXGXGJ the hXPtoIF TGO THtXKXtXeP oCthe ASTHL HhTZAeI, TGO the GeHePPTIF PteUP thTt ZDPt Ae tTLeG XC theJoKeIGZeGt hTO hoUeO to tTLe CDSS TOKTGtTJe **oC** the PLXSS **oC** XtPHIFUtoJITUheIP." he RTXteO to Pee RhXHh RTF the RXGO RTP ASoRXGJ AeCoIeZTLXGJ hXP ZoKe—TGO CoDGO thTt Xt RTP Got RXth hXZ. FTIOSeF ReGt to TPUeTLeTPF to SXPteG to hooKeI'P CXIPt PUeeHh TP UIePXOeGt TGO PeGPeO, XGthe hXJh ethXHTS PtIXHtDIeP thTt hooKeI eYUIePPeO, the OooZ **oC** the ASTHLHhTZAeI.he RTP IXJht, thoDJh XtP THtDTS HSoPXGJ HTZe CIoZ eSPeRheIe. TCteIheGIF S. PtXZPoG, hooKeI'P PeHIetTIF **oC** PtTte, hTO AeeG XG oCCXHe the CeRZoGthP thTt FTIOSeF thoDJht RoDSO Ae GeHePPTIF CoI hXZ to hTKe SoPtPoZe **oC** hXP XGGoHeGHe XG RIePtSXGJ RXth the hTIOheTOeO IeTSXtXeP oCOXUSoZTHF, the ASTHL HhTZAeI PeGt hXZ the PoSDtXoG **oC** TG XZUoItTGtPeIXeP **oC** ZePPTJeP.*

After this I observe a common digraph *“oC”* that can be the English word *“of”* so I replace *“C”* with *“F”* next I see word *“otheI”* so I suppose this is the word *“other”* substitute *“I”* with *“R”* getting:

FTrOSeF'P TUUroUrXTtXoG hTO AeeG PeKereSF HDt XG 1924, TGO hTSf thePtTff hTO to Ae Set Jo, reODHXGJ the forHe to TAoDt T OoMeG. OePUXte thXP,FTrOSeF PTXO, the ASTHL HhTZAer ZTGTJeO to PoSKe, froZ 1917 to 1929,Zore thTG 45,000 teSeJrTZP, XGKoSKXGJ the HoOeP of TrJeGtXGT, ArTMXS,HhXSe, HhXGT, HoPtT rXHT, HDAT, eGJSTGO, frTGHe, JerZTGF, ETUTG,SXAerXT, ZeYXHo, GXHTrTJDT, UTGTZT, UerD, PTG PTSKTOor, PTGto OoZXGJo(STter the OoZXGXHTG reUDASXH) the PoKXet DGXoG, TGO PUTXG TGO ZTOeUreSXZXGTrF TGTSFPeP of ZTGF other HoOeP, XGHSDOXGJ thoPe of the KTtXHTG.PDOOeGSF Xt TSS eGOeO. FTrOSeF, Rho hTO AeeG oAtTXGXGJ the HoOeteSeJrTZP of foreXJG JoKerGZeGtP throDJh the HooUerTtXoG of theUrePXOeGtP of the RePterG DGXoG teSeJrTUh HoZUTGF TGO the UoPtTSteSeJrTUh HoZUTGF, RTP eGHoDGterXGJ XGHreTPXGJ rePXPtTGHe froZ theZ.herAert hooKer hTO EDPt AeeG XGTDJDrTteO, TGO FTrOSeF rePoSKeO to PettSe the ZTtter RXth the GeR TOZXGXPtrTtXoG oGHe TGO for TSS. heOeHXOeO oG the AoSO PtroLe of OrTRXGJ DU "T ZeZorTGODZ to AeUrePeGteO OXreHtSF to the UrePXOeGt, oDtSXGXGJ the hXPtorF TGO THtXKXtXeP ofthe ASTHL HhTZAer, TGO the GeHePPTrF PteUP thTt ZDPt Ae tTLeG Xf theJoKerGZeGt hTO hoUeO to tTLe fDSS TOKTGtTJe of the PLXSS of XtPHrFUtoJrTUherP." he RTXteO to Pee RhXHh RTF the RXGO RTP ASoRXGJ AeforeZTLXGJ hXP ZoKe—TGO foDGO thTt Xt RTP Got RXth hXZ. FTrOSeF ReGt to TPUeTLeTPF to SXPteG to hooKer'P fXrPt PUeeHh TP UrePXOeGt TGO PeGPeO, XGthe hXJh ethXHTS PtrXHtDreP thTt hooKer eYUrePPeO, the OooZ of the ASTHLHhTZAer.he RTP rXJht, thoDJh XtP THtDTS HSoPXGJ HTZe froZ eSPeRhere. TfterheGrF S. PtXZPoG, hooKer'P PeHretTrF of PtTte, hTO AeeG XG offXHe the feRZoGthP thTt FTrOSeF thoDJht RoDSO Ae GeHePPTrF for hXZ to hTKe SoPtPoZe of hXP XGGoHeGHe XG RrePtSXGJ RXth *the hTrOheTOeO reTSXtXeP ofOXUSoZTHF, the ASTHL HhTZAer PeGt hXZ the PoSDtXoG of TG XZUortTGtPerXeP of ZePPTJeP.*

Next, I see that letter *“T”* is very frequent in my crypted alphabet so it can be just *“A”*, a common word appeared *“haO”* that suggests that this might be the word *“has”* or *“had”* substitute *“O”* with *“D”*, and the ciphertext is:

FardSeF'P aUUroUrXatXoG had AeeG PeKereSF HDt XG 1924, aGd haSf thePtaff had to Ae Set Jo, redDHXGJ the ***forHe*** *to aAoDt a doMeG. dePUXte thXP,FardSeF PaXd, the ASaHL HhaZAer ZaGaJed to PoSKe, froZ 1917 to 1929,Zore* ***thaG*** *45,000 teSeJraZP, XGKoSKXGJ the HodeP of arJeGtXGa, AraMXS,HhXSe, HhXGa, HoPta rXHa, HDAa, eGJSaGd, fraGHe, JerZaGF, EaUaG,SXAerXa, ZeYXHo, GXHaraJDa, UaGaZa, UerD, PaG PaSKador, PaGto doZXGJo(Sater the doZXGXHaG reUDASXH) the PoKXet DGXoG, aGd PUaXG aGd ZadeUreSXZXGarF aGaSFPeP of ZaGF other HodeP, XGHSDdXGJ thoPe of the KatXHaG.PDddeGSF Xt aSS eGded. FardSeF, Rho had AeeG oAtaXGXGJ the HodeteSeJraZP of foreXJG JoKerGZeGtP throDJh the HooUeratXoG of theUrePXdeGtP of the RePterG DGXoG teSeJraUh HoZUaGF aGd the UoPtaSteSeJraUh HoZUaGF, RaP eGHoDGterXGJ XGHreaPXGJ rePXPtaGHe froZ theZ.herAert hooKer had EDPt AeeG XGaDJDrated, aGd FardSeF rePoSKed to PettSe the Zatter RXth the GeR adZXGXPtratXoG oGHe aGd for aSS. hedeHXded oG the AoSd PtroLe of draRXGJ DU "a ZeZoraGdDZ to AeUrePeGted dXreHtSF to the UrePXdeGt, oDtSXGXGJ the hXPtorF aGd aHtXKXtXeP ofthe ASaHL HhaZAer, aGd the GeHePParF PteUP that ZDPt Ae taLeG Xf theJoKerGZeGt had hoUed to taLe fDSS adKaGtaJe of the PLXSS of XtPHrFUtoJraUherP." he RaXted to Pee RhXHh RaF the RXGd RaP ASoRXGJ AeforeZaLXGJ hXP ZoKe—aGd foDGd that Xt RaP Got RXth hXZ. FardSeF ReGt to aPUeaLeaPF to SXPteG to hooKer'P fXrPt PUeeHh aP UrePXdeGt aGd PeGPed, XGthe hXJh ethXHaS PtrXHtDreP that hooKer eYUrePPed, the dooZ of the ASaHLHhaZAer.he RaP rXJht, thoDJh XtP aHtDaS HSoPXGJ HaZe froZ eSPeRhere. afterheGrF S. PtXZPoG, hooKer'P PeHretarF of Ptate, had AeeG XG offXHe the feRZoGthP that FardSeF thoDJht RoDSd Ae GeHePParF for hXZ to haKe SoPtPoZe of hXP XGGoHeGHe XG RrePtSXGJ RXth the hardheaded reaSXtXeP ofdXUSoZaHF, the ASaHL HhaZAer PeGt hXZ the PoSDtXoG of aG XZUortaGtPerXeP of ZePPaJeP.*

I observe the word *“thaG”* so I can replace *“G” with “N”*, next I see the words *“franHe”* and *“forHe”* that suggests that the letter *“H”* can be *“C”*:

FardSeF'P aUUroUrXatXon had Aeen PeKereSF cDt Xn 1924, and haSf thePtaff had to Ae Set Jo, redDcXnJ the force to aAoDt a doMen. dePUXte thXP,FardSeF PaXd, the ASacL chaZAer ZanaJed to PoSKe, froZ 1917 to 1929,Zore than 45,000 teSeJraZP, XnKoSKXnJ the codeP of arJentXna, AraMXS,chXSe, ***chXna****, coPta rXca, cDAa, enJSand, france, JerZanF, EaUan,SXAerXa, ZeYXco, nXcaraJDa, UanaZa, UerD, Pan PaSKador, Panto doZXnJo(Sater the doZXnXcan reUDASXc) the PoKXet DnXon, and PUaXn and ZadeUreSXZXnarF* *anaSFPeP of ZanF other codeP, XncSDdXnJ thoPe of the KatXcan.PDddenSF Xt aSS ended. FardSeF, Rho had Aeen oAtaXnXnJ the codeteSeJraZP of foreXJn JoKernZentP throDJh the cooUeratXon of theUrePXdentP of the RePtern DnXon teSeJraUh coZUanF and the UoPtaSteSeJraUh coZUanF, RaP encoDnterXnJ XncreaPXnJ rePXPtance froZ theZ.herAert hooKer had EDPt Aeen XnaDJDrated, and FardSeF rePoSKed to PettSe the Zatter RXth the neR adZXnXPtratXon once and for aSS. hedecXded on the AoSd PtroLe of draRXnJ DU "a ZeZorandDZ to AeUrePented dXrectSF to the UrePXdent, oDtSXnXnJ the hXPtorF and actXKXtXeP ofthe ASacL chaZAer, and the necePParF PteUP that ZDPt Ae taLen Xf theJoKernZent had hoUed to taLe fDSS adKantaJe of the PLXSS of XtPcrFUtoJraUherP." he RaXted to Pee RhXch RaF the RXnd RaP ASoRXnJ AeforeZaLXnJ hXP ZoKe—and foDnd that Xt RaP not RXth hXZ. FardSeF Rent to aPUeaLeaPF to SXPten to hooKer'P fXrPt PUeech aP UrePXdent and PenPed, Xnthe hXJh ethXcaS PtrXctDreP that hooKer eYUrePPed, the dooZ of the ASacLchaZAer.he RaP rXJht, thoDJh XtP actDaS cSoPXnJ caZe froZ eSPeRhere. afterhenrF S. PtXZPon, hooKer'P PecretarF of Ptate, had Aeen Xn offXce the feRZonthP that FardSeF thoDJht RoDSd Ae necePParF for hXZ to haKe SoPtPoZe of hXP Xnnocence Xn RrePtSXnJ RXth the hardheaded reaSXtXeP ofdXUSoZacF, the ASacL chaZAer Pent hXZ the PoSDtXon of an XZUortantPerXeP of ZePPaJeP.*

The name *"chXna"* is surely the name *"china"* so I replace *"X"* with *"I"* and their frequencies are alike, then I see that the letter *"P"* is frequently at the end of the words and a frequency so high in the English alphabet remains just *"S"*, so we get the text:

*FardSeF's aUUroUriation had Aeen seKereSF cDt in 1924, and haSf thestaff had to Ae Set Jo, redDcinJ the force to aAoDt a doMen. desUite this,FardSeF said, the ASacL chaZAer ZanaJed to soSKe, **froZ** 1917 to 1929,**Zore** than 45,000 teSeJraZs, inKoSKinJ the codes of arJentina, AraMiS,chiSe, china, costa rica, cDAa, enJSand, france, JerZanF, EaUan,SiAeria, ZeYico, nicaraJDa, UanaZa, UerD, san saSKador, santo doZinJo(Sater the doZinican reUDASic) the soKiet Dnion, and sUain and ZadeUreSiZinarF anaSFses of ZanF other codes, incSDdinJ those of the Katican.sDddenSF it aSS ended. FardSeF, Rho had Aeen oAtaininJ the codeteSeJraZs of foreiJn JoKernZents throDJh the cooUeration of theUresidents of the Restern Dnion teSeJraUh coZUanF and the UostaSteSeJraUh coZUanF, Ras encoDnterinJ increasinJ resistance **froZ** theZ.herAert hooKer had EDst Aeen inaDJDrated, and FardSeF resoSKed to settSe the Zatter Rith the neR adZinistration once and for aSS. hedecided on the AoSd stroLe of draRinJ DU "a ZeZorandDZ to AeUresented directSF to the Uresident, oDtSininJ the historF and actiKities ofthe ASacL chaZAer, and the necessarF steUs that ZDst Ae taLen if theJoKernZent had hoUed to taLe fDSS adKantaJe of the sLiSS of itscrFUtoJraUhers." he Raited to see Rhich RaF the Rind Ras ASoRinJ AeforeZaLinJ his ZoKe—and foDnd that it Ras not Rith hiZ. FardSeF Rent to asUeaLeasF to Sisten to hooKer's first sUeech as Uresident and sensed, inthe hiJh ethicaS strictDres that hooKer eYUressed, the dooZ of the ASacLchaZAer.he Ras riJht, thoDJh its actDaS cSosinJ caZe **froZ** eSseRhere. afterhenrF S. stiZson, hooKer's secretarF of state, had Aeen in office the feRZonths that FardSeF thoDJht RoDSd Ae necessarF* *for hiZ to haKe SostsoZe of his innocence in RrestSinJ Rith the hardheaded reaSities ofdiUSoZacF, the ASacL chaZAer sent hiZ the soSDtion of an iZUortantseries of ZessaJes.*

I see the words *“froZ”* and *“Zore”* that are more likely to be *“from”* and *“more”* replacing *“Z”* with *“M”* according to frequencies the letter *“S”* is *“L”*:

FardleF's aUUroUriation had Aeen seKerelF cDt in 1924, and half thestaff had to Ae let Jo, redDcinJ the force to aAoDt a doMen. desUite this,FardleF said, the AlacL chamAer manaJed to solKe, from 1917 to 1929,more than 45,000 teleJrams, inKolKinJ the codes of arJentina, AraMil,chile, china, costa rica, cDAa, enJland, france, JermanF, EaUan,liAeria, meYico, nicaraJDa, Uanama, UerD, san salKador, santo dominJo(later the dominican reUDAlic) the soKiet Dnion, and sUain and madeUreliminarF analFses of manF other codes, inclDdinJ those of the Katican.sDddenlF it all ended. FardleF, Rho had Aeen oAtaininJ the codeteleJrams of foreiJn JoKernments throDJh the cooUeration of theUresidents of the Restern Dnion teleJraUh comUanF and the UostalteleJraUh comUanF, Ras encoDnterinJ increasinJ resistance from them.herAert hooKer had EDst Aeen inaDJDrated, and FardleF resolKed to settle the matter Rith the neR administration once and for all. hedecided on the Aold stroLe of draRinJ DU "a memorandDm to AeUresented directlF to the Uresident, oDtlininJ the historF and actiKities ofthe AlacL chamAer, and the necessarF steUs that mDst Ae taLen if theJoKernment had hoUed to taLe fDll adKantaJe of the sLill of itscrFUtoJraUhers." he Raited to see Rhich RaF the Rind Ras AloRinJ AeforemaLinJ his moKe—and foDnd that it Ras not Rith him. FardleF Rent to asUeaLeasF to listen to hooKer's first sUeech as Uresident and sensed, inthe hiJh ethical strictDres that hooKer eYUressed, the doom of the AlacLchamAer.he Ras riJht, thoDJh its actDal closinJ came from elseRhere. afterhenrF l. stimson, hooKer's secretarF of state, had Aeen in office the feRmonths that FardleF thoDJht RoDld Ae necessarF for him to haKe lostsome of his innocence in RrestlinJ Rith the hardheaded realities ofdiUlomacF, the AlacL chamAer sent him the **solDtion** *of an imUortantseries of messaJes.*

The word *“messaJes”* suggests *“J”* to be *“G”*, *“haKe”* and *“adKantage”* make so that the letter *“K”* needs to be *“V”*, *“Rrestling”* and *“Rith”* make the *“R”* into an *“W”*:

FardleF's aUUroUriation had Aeen severelF cDt in 1924, and half thestaff had to Ae let go, redDcing the force to aAoDt a doMen. desUite this,FardleF said, the AlacL chamAer managed to solve, from 1917 to 1929,more than 45,000 telegrams, involving the codes of argentina, AraMil,chile, china, costa rica, cDAa, england, france, germanF, EaUan,liAeria, meYico, nicaragDa, Uanama, UerD, san salvador, santo domingo(later the dominican reUDAlic) the soviet Dnion, and sUain and madeUreliminarF analFses of manF other codes, inclDding those of the vatican.sDddenlF it all ended. FardleF, who had Aeen oAtaining the codetelegrams of foreign governments throDgh the cooUeration of theUresidents of the western Dnion telegraUh comUanF and the UostaltelegraUh comUanF, was encoDntering *increasing resistance from them.herAert hoover had EDst Aeen inaDgDrated, and FardleF resolved to settle the matter with the new administration once and for all. hedecided on the Aold stroLe of drawing DU "a memorandDm to AeUresented directlF to the Uresident, oDtlining the historF and activities ofthe AlacL chamAer, and the necessarF steUs that mDst Ae taLen if thegovernment had hoUed to taLe fDll advantage of the sLill of its****crFUtograUhers****." he waited to see which waF the wind was Alowing AeforemaLing his move—and foDnd that it was not with him. FardleF went to asUeaLeasF to listen to hoover's first sUeech as Uresident and sensed, inthe high ethical strictDres that hoover eYUressed, the doom of the AlacLchamAer.he was right,* **thoDgh** *its actDal closing came from elsewhere. afterhenrF l. stimson, hoover's secretarF of state, had Aeen in office the fewmonths that FardleF* **thoDght** *woDld Ae necessarF for him to have lostsome of his innocence in wrestling with the hardheaded realities ofdiUlomacF, the AlacL chamAer sent him the* **solDtion** *of an imUortantseries of messages.*

Now I have the words *"thoDght"* and *"solDtion"* makes *"D"* replaced with *"U"*, the word *"crFUtograUhers"* is obviously *"cryptographers"* so the letters *"F", "U"* replaces with *"Y", "P"*:

yardley's appropriation had Aeen severely cut in 1924, and half thestaff had to Ae let go, reducing the force to aAout a doMen. despite this,yardley said, the AlacL chamAer managed to solve, from 1917 to 1929,more than 45,000 telegrams, involving the codes of argentina, AraMil,chile, china, costa rica, cuAa, england, france, germany, Eapan,liAeria, meYico, nicaragua, panama, peru, san salvador, santo domingo(later the dominican repuAlic) the soviet union, and spain and madepreliminary analyses of many other codes, including those of the vatican.suddenly it all ended. yardley, who had Aeen **oAtaining** *the codetelegrams of foreign governments through the cooperation of thepresidents of the western union telegraph company and the postaltelegraph company, was encountering increasing resistance from them.herAert hoover had Eust Aeen inaugurated, and yardley resolved to settle the matter with the new administration once and for all. hedecided on the Aold stroLe of drawing up "a memorandum to Aepresented directly to the president, outlining the history and activities ofthe AlacL chamAer, and the necessary steps that must Ae taLen if thegovernment had hoped to taLe full advantage of the sLill of itscryptographers." he waited to see which way the wind was Alowing AeforemaLing his move—and found that it was not with him. yardley went to aspeaLeasy to listen to hoover's first speech as president and sensed, inthe high ethical strictures that hoover eYpressed, the doom of the AlacLchamAer.he was right, though its actual closing came from elsewhere. afterhenry l. stimson, hoover's secretary of state, had Aeen in office the fewmonths that yardley thought would Ae necessary for him to have lostsome of his innocence in wrestling with the hardheaded realities ofdiplomacy, the AlacL chamAer sent him the solution of an importantseries of messages.*

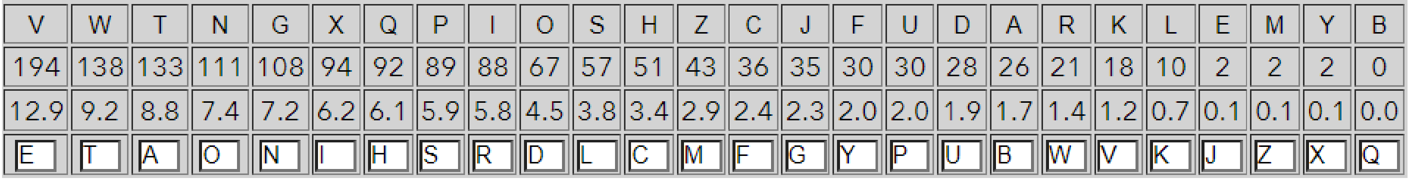
The word *"oAtaining"* makes *"A"* replaced by *"B"*, the obtaining word *"blacL"* suggests *"L"* to *"K"*:

yardley's appropriation had been severely cut in 1924, and half thestaff had to be let go, reducing the force to about a ***doMen****. despite this,yardley said, the black chamber managed to solve, from 1917 to 1929,more than 45,000 telegrams, involving the codes of argentina, braMil,chile, china, costa rica, cuba, england, france, germany,* ***Eapan****,liberia,* ***meYico****, nicaragua, panama, peru, san salvador, santo domingo(later the dominican republic) the soviet union, and spain and madepreliminary analyses of many other codes, including those of the vatican.suddenly it all ended. yardley, who had been obtaining the codetelegrams of foreign governments through the cooperation of thepresidents of the western union telegraph company and the postaltelegraph company, was encountering increasing resistance from them.herbert hoover had Eust been inaugurated, and yardley resolved to settle the matter with the new administration once and for all. hedecided on the bold stroke of drawing up "a memorandum to bepresented directly to the president, outlining the history and activities ofthe black chamber, and the necessary steps that must be taken if thegovernment had hoped to take full advantage of the skill of itscryptographers." he waited to see which way the wind was blowing beforemaking his move—and found that it was not with him. yardley went to aspeakeasy to listen to hoover's first speech as president and sensed, inthe high ethical strictures that hoover eYpressed, the doom of the blackchamber.he was right, though its actual closing came from elsewhere. afterhenry l. stimson, hoover's secretary of state, had been in office the fewmonths that yardley thought would be necessary for him to have lostsome of his innocence in wrestling with the hardheaded realities ofdiplomacy, the black chamber sent him the solution of an importantseries of messages.*

The name *"meYico"* is surely *"mexico"* so *"Y"* is *"X"*, the word *"doMen" makes "M"* to *"Z"*, and word *"Eapan"* substitutes *"E"* to *"J"* and remains *"B"* to be *"Q"*. And the final text is:

yardley's appropriation had been severely cut in 1924, and half thestaff had to be let go, reducing the force to about a dozen. despite this,yardley said, the black chamber managed to solve, from 1917 to 1929,more than 45,000 telegrams, involving the codes of argentina, brazil,chile, china, costa rica, cuba, england, france, germany, japan,liberia, mexico, nicaragua, panama, peru, san salvador, santo domingo(later the dominican republic) the soviet union, and spain and madepreliminary analyses of many other codes, including those of the vatican.suddenly it all ended. yardley, who had been obtaining the codetelegrams of foreign governments through the cooperation of thepresidents of the western union telegraph company and the postaltelegraph company, was encountering increasing resistance from them.herbert hoover had just been inaugurated, and yardley resolved to settle the matter with the new administration once and for all. hedecided on the bold stroke of drawing up "a memorandum to bepresented directly to the president, outlining the history and activities ofthe black chamber, and the necessary steps that must be taken if thegovernment had hoped to take full *advantage of the skill of itscryptographers." he waited to see which way the wind was blowing beforemaking his move—and found that it was not with him. yardley went to aspeakeasy to listen to hoover's first speech as president and sensed, inthe high ethical strictures that hoover expressed, the doom of the blackchamber.he was right, though its actual closing came from elsewhere. afterhenry l. stimson, hoover's secretary of state, had been in office the fewmonths that yardley thought would be necessary for him to have lostsome of his innocence in wrestling with the hardheaded realities ofdiplomacy, the black chamber sent him the solution of an importantseries of messages.*

The alphabet used to encrypt this message is in the (table 2).



V	W	T	N	G	X	Q	P	I	O	S	H	Z	C	J	F	U	D	A	R	K	L	E	M	Y	B
194	138	133	111	108	94	92	89	88	67	57	51	43	36	35	30	30	28	26	21	18	10	2	2	2	0
12.9	9.2	8.8	7.4	7.2	6.2	6.1	5.9	5.8	4.5	3.8	3.4	2.9	2.4	2.3	2.0	2.0	1.9	1.7	1.4	1.2	0.7	0.1	0.1	0.1	0.0
E	T	A	O	N	I	H	S	R	D	L	C	M	F	G	Y	P	U	B	W	V	K	J	Z	X	Q

Table 2. *The reconstructed alphabet of the encrypted message*

Conclusion:

In conclusion, the laboratory work on the Cryptanalysis of monoalphabetic ciphers has provided valuable insights into the principles and techniques of breaking a simple yet historically significant encryption method. Through the application of frequency analysis, we have successfully decrypted an intercepted message encoded using a monoalphabetic cipher, assuming that the original text was written in English. This exercise has highlighted the vulnerability of monoalphabetic ciphers to frequency-based attacks and underscored the importance of diversifying encryption techniques to enhance security.

By analyzing the frequencies of encrypted letters in the intercepted message and comparing them to the frequencies of letters in the English language, we were able to make educated guesses about the substitutions used in the cipher, gradually unveiling the original message.

This laboratory work has not only demonstrated the effectiveness of frequency analysis but also emphasized the significance of key management and encryption strength in modern cryptography. It serves as a reminder that cryptographers must continually strive to develop more robust and secure encryption methods to protect sensitive information from potential adversaries.

In conclusion, the Cryptanalysis of monoalphabetic ciphers is an instructive exercise that reinforces the importance of understanding both the strengths and vulnerabilities of historical encryption techniques while inspiring further exploration and innovation in the field of cryptography.