

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

Technical University of Moldova

Department of Software and Automation Engineering

**REPORT**

Laboratory work No. 2

**Discipline**: Cryptography and Security

Elaborated: FAF-221, Chichioi Iuliana

Checked: asist. univ.,Nirca Dumitru

Chișinău 2024

## Topic: Mono-alphabetic Cipher

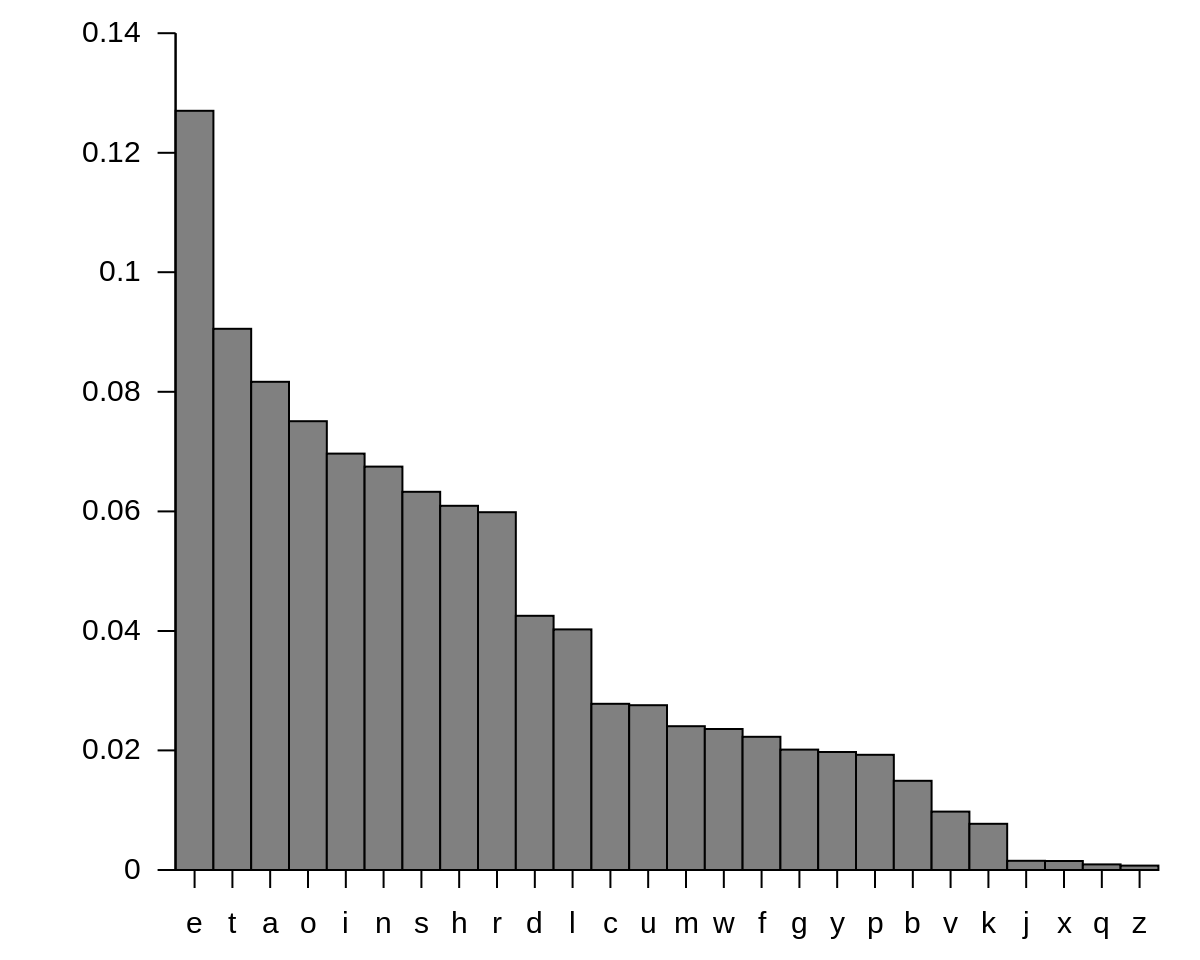
## Tasks:

1. An encrypted message was intercepted that is known to have been obtained using a mono-alphabetic cipher. Applying the frequency analysis attack to find out the original message, if it assumed to be a text written in English. Bear in mind that only letters, the other characters remain unencrypted.

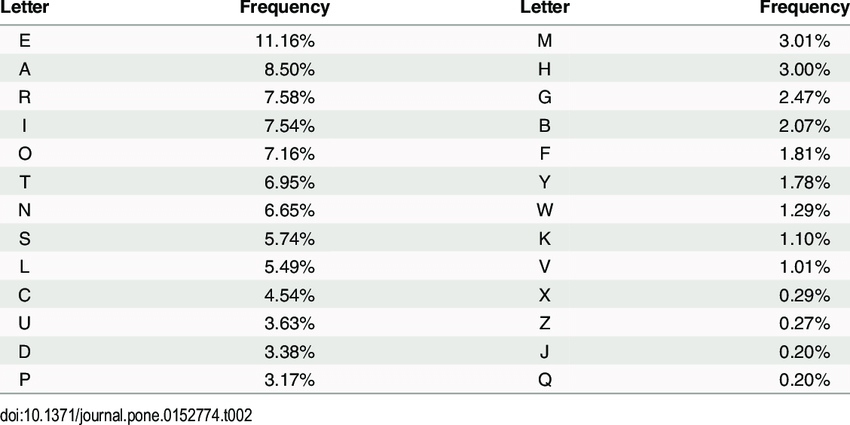
## Theoretical notes:

The vulnerability of mono-alphabetic encryption systems stems from their susceptibility to character frequency analysis. When dealing with a sufficiently lengthy encrypted text in a known language, attackers can exploit the inherent frequency patterns of letters within that language, a technique known as a frequency analysis attack. This frequency analysis is not only widely studied for cryptographic purposes but also in various other contexts.

Over time, researchers have developed distinct ordering structures to reflect the frequency of letter occurrences in multiple European and non-European languages. As a ciphertext length increases, it gradually converges towards this general frequency ordering.



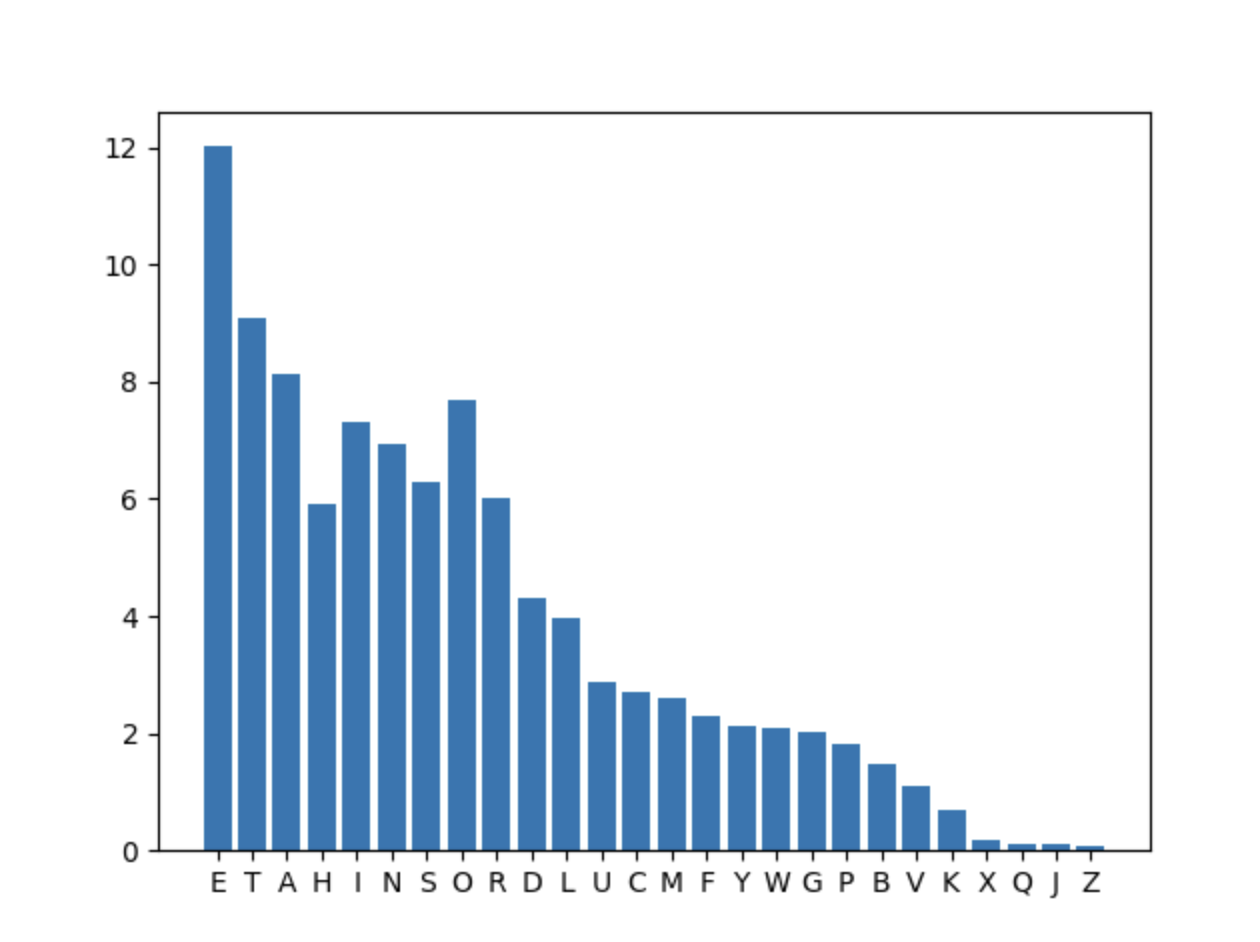
**Fig.1**: English letter frequency



**Fig.2**: English letter frequency(Table)

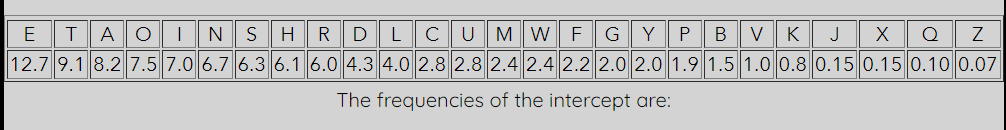
**Implementation(Var. Nr.5)**

I have a cryptogram c = *Ixkviatgl Udasxhtwxng Gn. 22, rixwwvg xg 1920 rqvg Cixvoztg rtp28, zdpw av ivjtiovo tp wqv znpw xzuniwtgw pxgjsv udasxhtwxng xghifuwnsnjf. Xw wnnl wqv phxvghv xgwn t gvr rniso. Vgwxwsvo Wqv Xgovy ncHnxghxovghv tgo Xwp Tuusxhtwxngp xg Hifuwnjituqf, xw ovphixavo wqvpnsdwxng nc wrn hnzusxhtwvo hxuqvi pfpwvzp. Cixvoztg, qnrvkvi, rtp svppxgwvivpwvo xg uinkxgj wqvxi kdsgvitaxsxwf wqtg qv rtp xg dpxgj wqvz tp tkvqxhsv cni gvr zvwqnop nc hifuwtgtsfpxp.Xg xwXwuvizxwwvo qxz wn ivhngpwidhw t uixztif hxuqvi tsuqtavw rxwqndw qtkxgjwn jdvpp tw t pxgjsv ustxgwvyw svwwvi. Adw wqv nwqvi rtp uincndgo. Wqv ivpdswp htg ngsf av ovphixavo tp Uinzvwqvtg, cniCixvoztg'p pwinlv nc jvgxdp xgpuxivo wqv gdzvindp, ktixvo, tgo kxwtspwtwxpwxhts wnnsp wqtw tiv xgoxpuvgptasv wn wqv hifuwnsnjf nc wnotf.Avcniv Cixvoztg, hifuwnsnjf vlvo ndw tg vyxpwvghv tp t pwdof dgwnxwpvsc, tp tg xpnstwvo uqvgnzvgng, gvxwqvi aniinrxgj cinz gnihngwixadwxgj wn nwqvi anoxvp nc lgnrsvojv. Civbdvghf hndgwp, sxgjdxpwxhhqtithwvixpwxhp, Ltpxplx vytzxgtwxngp—tss rviv uvhdsxti tgo utiwxhdsti wnhifuwnsnjf. Xw orvsw t ivhsdpv xg wqv rniso nc phxvghv. Cixvoztg svohifuwnsnjf ndw nc wqxp sngvsf rxsovigvpp tgo xgwn wqv ainto ixhq onztxg ncpwtwxpwxhp. Qv hnggvhwvo hifuwnsnjf wn ztwqvztwxhp. Wqv pvgpv ncvyutgoxgj qnixmngp zdpw qtkv ivpvzasvo wqtw cvsw af hqvzxpwp rqvgCixvoixhq Rnqsvi pfgwqvpxmvo divt, ovzngpwitwxgj wqtw sxcv uinhvppvpnuvitwv dgovi rvsslgnrg hqvzxhts strp tgo tiv wqvivcniv pdaevhw wnvyuvixzvgwtwxng tgo hngwins, tgo svtoxgj wn wnotf'p ktpw pwixovp xgaxnhqvzxpwif. Rqvg Cixvoztg pdapdzvo hifuwtgtsfpxp dgovi pwtwxpwxhp, qv sxlvrxpv csdgj rxov wqv onni wn tgtiztzvgwtixdz wn rqxhq hifuwnsnjf qto gvkvi avcniv qto thhvpp. Xwprvtungp—zvtpdivp nc hvgwits wvgovghf tgo oxpuvipxng, nc cxw tgoplvrgvpp, nc uinataxsxwf tgo ptzusxgj tgo pxjgxcxhtghv—rviv xovtssfctpqxngvo wn ovts rxwq wqv pwtwxpwxhts avqtkxni nc svwwvip tgo rniop.Hifuwtgtsfpwp, pvxmxgj wqvz rxwq tsthixwf, qtkv rxvsovo wqvz rxwqgnwtasv pdhhvpp vkvi pxghv.Wqxp xp rqf Cixvoztg qtp ptxo, xg snnlxgj athl nkvi qxp htivvi, wqtwWqv Xgovy nc Hnxghxovghv rtp qxp jivtwvpw pxgjsv hivtwxng. Xw tsngv rndsoqtkv rng qxz qxp ivudwtwxng. Adw xg cthw xw rtp ngsf wqv avjxggxgj. Qv tgo Zip. Cixvoztg bdxw Ixkviatgl gvti wqv vgo nc 1920. Wqvpxwdtwxng qto avhnzv xgwnsvitasv. Ctaftg qto sdivo qxz athl tcwvi wqvrti rxwq itxpvp tgo uinzxpvp nc tapnsdwv civvonz wn uinkv ni oxpuinkvwqv vyxpwvghv nc hxuqvip xg Pqtlvpuvtiv. Adw qv qto pbdvshqvo vkviftwwvzuw wn on pn tgo qto vzatiitppvo Cixvoztg xgwn tuutivgwsfthbdxvphvgw pxsvghv tw stgwvig-psxov svhwdivp ng wqv pdaevhw. Ng Etgdtif1, 1921, Cixvoztg avjtg t pxy-zngwq hngwithw rxwq wqv Pxjgts Hniup wnovkxpv hifuwnpfpwvzp. Rqvg xw vyuxivo, qv rtp wtlvg ng wqv hxkxs-pvikxhvutfinss nc wqv Rti Ovutiwzvgw tw $4,500 t fvti.Ngv nc qxp cxipw tppxjgzvgwp rtp wn wvthq t hndipv xg zxsxwtif hnovptgo hxuqvip tw wqv Pxjgts Phqnns, wqvg tw Htzu Tscivo Ktxs, Gvr Evipvf.Cni wqxp qv rinwv t wvywannl wqtw, cni wqv cxipw wxzv, xzunpvo niovi dungwqv hqtnp nc hxuqvi pfpwvzp tgo wqvxi wvizxgnsnjf. Wqvpv qto puindwvoxg t avrxsovixgj ktixvwf, tgo rixwvip wivtwvo vthq tp xgoxkxodts tgopuvhxts htpvp. Cixvoztg pniwvo wqvz ndw ng wqv atpxp nc pwidhwdivxgpwvto nc tpuvhw, tgo pn snjxhts tgo dpvcds rtp wqxp hstppxcxhtwxng wqtw xwqtp avhnzv pwtgotio. Qv znovsvo qxp gnzvghstwdiv ng qxp htwvjnixvp, pnwqtw wqv gtzvp qv zxgwvo qtkv wqv jivtw zvixw nc ztlxgj wqv ivstwxngpavwrvvg wqv ktixndp jvgvit nc hxuqvip vkxovgw ng pxjqw. Tg vytzusv xp wqvhnzusvzvgwtif utxi "zngn-tsuqtavw" tgo "unsftsuqtavw"; wqv Civghqrviv pwxss htssxgj unsftsuqtavwxh pfpwvzp af wqv tsznpw nacdphtwnif"ondasv pdapwxwdwxng," rqxhq wvssp tapnsdwvsf gnwqxgj tw tss tandw wqvpfpwvz. Cixvoztg'p znpw xzuniwtgw hnxgtjv rtp wqv rnio"hifuwtgtsfpxp," rqxhq qv ovkxpvo xg 1920 wn hsvti du t hqingxh pndihv nchngcdpxng xg hifuwnsnjf—wqv tzaxjdxwf nc wqv kvia "ovhxuqvi," wqvg dpvown zvtg anwq tdwqnixmvo tgo dgtdwqnixmvo ivodhwxngp nc t hifuwnjitz wn ustxgwvyw.Qv wxwsvo qxp annl Vsvzvgwp nc Hifuwtgtsfpxp, tgo wqv wviz qtp pnuinpuvivo wqtw wnotf xw hxihdstwvp xg jvgvits hngkviptwxng tgo uixgw*

So first we look at the frequencies as shown bellow:  


**Fig.3**: Frequency of cryptogram letters(in my case)

And we also look at this table:



**Fig.4**: Frequency of cryptogram letters

And as we see the “V” in my text has a similar appearance and the most used letter “E” so I conclude *V -> e* and also by the look of it I see that the “W” and “T” have the same percentage so I assume that *W -> t*. The my “T” letter has the same as “A” so also *T -> a*. So I get: *IXKeIAaGL UDASXHatXNG GN. 22, RIXtteG XG 1920 RQeG CIXeOZaG RaP28, ZDPt Ae IeJaIOeO aP* ***tQe*** *ZNPt*

*XZUNItaGt PXGJSe UDASXHatXNG XGHIFUtNSNJF.* ***Xt*** *tNNL tQe PHXeGHe XGtN a GeR RNISO. eGtXtSeO*

***tQe*** *XGOeY NCHNXGHXOeGHe aGO XtP aUUSXHatXNGP XG HIFUtNJIaUQF,* ***Xt*** *OePHIXAeO tQePNSDtXNG*

*NC tRN HNZUSXHateO HXUQeI PFPteZP. CIXeOZaG, QNReKeI, RaP SePPXGteIePteO XG UINKXGJ tQeXI*

*KDSGeIaAXSXtF tQaG Qe RaP XG DPXGJ tQeZ aP aKeQXHSe CNI GeR ZetQNOP NC HIFUtaGaSFPXP.XG* ***Xt****,*

*CIXeOZaG OeKXPeO tRN GeR teHQGXBDeP. NGe RaP AIXSSXaGt. XtUeIZXtteO QXZ tN IeHNGPtIDHt a*

*UIXZaIF HXUQeI aSUQaAet RXtQNDt QaKXGJtN JDePP at a PXGJSe USaXGteYt SetteI. ADt tQe NtQeI*

*RaP UINCNDGO. CNI tQeCXIPt tXZe XG HIFUtNSNJF, CIXeOZaG tIeateO a CIeBDeGHF OXPtIXADtXNG aP*

*aGeGtXtF, aP a HDIKe RQNPe PeKeIaS UNXGtP ReIe HaDPaSSF IeSateO, GNt aP EDPta HNSSeHtXNG NC*

*XGOXKXODaS SetteIP tQat QaUUeG tN PtaGO XG a HeItaXG NIOeICNI GNGHaDPaS (QXPtNIXHaS) IeaPNGP,*

*aGO tN tQXP HDIKe Qe aUUSXeO PtatXPtXHaSHNGHeUtP****. tQe*** *IePDStP HaG NGSF Ae OePHIXAeO aP*

*UINZetQeaG, CNICIXeOZaG'P PtINLe NC JeGXDP XGPUXIeO* ***tQe*** *GDZeINDP, KaIXeO, aGO*

*KXtaSPtatXPtXHaS tNNSP tQat aIe XGOXPUeGPaASe tN* ***tQe*** *HIFUtNSNJF NC tNOaF.AeCNIe CIXeOZaG,*

*HIFUtNSNJF eLeO NDt aG eYXPteGHe aP a PtDOF DGtNXtPeSC, aP aG XPNSateO UQeGNZeGNG, GeXtQeI*

*ANIINRXGJ CINZ GNIHNGtIXADtXGJ tN NtQeI ANOXeP NC LGNRSeOJe. CIeBDeGHF HNDGtP,*

*SXGJDXPtXHHQaIaHteIXPtXHP, LaPXPLX eYaZXGatXNGP—aSS ReIe UeHDSXaI aGO UaItXHDSaI*

*tNHIFUtNSNJF.* ***Xt*** *OReSt a IeHSDPe XG tQe RNISO NC PHXeGHe. CIXeOZaG SeOHIFUtNSNJF NDt NC tQXP*

*SNGeSF RXSOeIGePP aGO XGtN* ***tQe*** *AINaO IXHQ ONZaXG NCPtatXPtXHP. Qe HNGGeHteO HIFUtNSNJF tN*

*ZatQeZatXHP. tQe PeGPe NCeYUaGOXGJ QNIXMNGP ZDPt QaKe IePeZASeO tQat CeSt AF HQeZXPtP*

*RQeGCIXeOIXHQ RNQSeI PFGtQePXMeO DIea, OeZNGPtIatXGJ tQat SXCe UINHePPePNUeIate DGOeI ReSSLGNRG HQeZXHaS SaRP aGO aIe tQeIeCNIe PDAEeHt tNeYUeIXZeGtatXNG aGO HNGtINS, aGO SeaOXGJ tN*

*tNOaF'P KaPt PtIXOeP XGAXNHQeZXPtIF. RQeG CIXeOZaG PDAPDZeO HIFUtaGaSFPXP DGOeI*

*PtatXPtXHP, Qe SXLeRXPe CSDGJ RXOe tQe ONNI tN aGaIZaZeGtaIXDZ tN RQXHQ HIFUtNSNJF QaO GeKeI*

*AeCNIe QaO aHHePP. XtPReaUNGP—ZeaPDIeP NC HeGtIaS teGOeGHF aGO OXPUeIPXNG, NC CXt*

*aGOPLeRGePP, NC UINAaAXSXtF aGO PaZUSXGJ aGO PXJGXCXHaGHe—ReIe XOeaSSFCaPQXNGeO tN OeaS RXtQ*

*tQe PtatXPtXHaS AeQaKXNI NC SetteIP aGO RNIOP.HIFUtaGaSFPtP, PeXMXGJ tQeZ RXtQ aSaHIXtF,*

*QaKe RXeSOeO tQeZ RXtQGNtaASe PDHHePP eKeI PXGHe.tQXP XP RQF CIXeOZaG QaP PaXO, XG SNNLXGJ*

*AaHL NKeI QXP HaIeeI, tQattQe XGOeY NC HNXGHXOeGHe RaP QXP JIeatePt PXGJSe HIeatXNG. Xt aSNGe*

*RNDSOQaKe RNG QXZ QXP IeUDtatXNG. ADt XG CaHt Xt RaP NGSF tQe AeJXGGXGJ. Qe aGO ZIP. CIXeOZaG*

*BDXt IXKeIAaGL GeaI tQe eGO NC 1920. tQePXtDatXNG QaO AeHNZe XGtNSeIaASe. CaAFaG QaO SDIeO QXZ*

*AaHL aCteI tQeRaI RXtQ IaXPeP aGO UINZXPeP NC aAPNSDte CIeeONZ tN UINKe NI OXPUINKetQe*

*eYXPteGHe NC HXUQeIP XG PQaLePUeaIe. ADt Qe QaO PBDeSHQeO eKeIFatteZUt tN ON PN aGO QaO*

*eZAaIIaPPeO CIXeOZaG XGtN aUUaIeGtSFaHBDXePHeGt PXSeGHe at SaGteIG-PSXOe SeHtDIeP NG tQe*

*PDAEeHt. NG EaGDaIF1, 1921, CIXeOZaG AeJaG a PXY-ZNGtQ HNGtIaHt RXtQ tQe PXJGaS HNIUP*

*tNOeKXPe HIFUtNPFPteZP. RQeG* ***Xt*** *eYUXIeO, Qe RaP taLeG NG tQe HXKXS-PeIKXHeUaFINSS NC tQe RaI*

*OeUaItZeGt at $4,500 a FeaI.NGe NC QXP CXIPt aPPXJGZeGtP RaP tN teaHQ a HNDIPe XG ZXSXtaIF*

*HNOePaGO HXUQeIP at tQe PXJGaS PHQNNS, tQeG at HaZU aSCIeO KaXS, GeR EeIPeF.CNI tQXP Qe RINte*

*a teYtANNL tQat, CNI tQe CXIPt tXZe, XZUNPeO NIOeI DUNGtQe HQaNP NC HXUQeI PFPteZP aGO tQeXI*

*teIZXGNSNJF. tQePe QaO PUINDteOXG a AeRXSOeIXGJ KaIXetF, aGO RIXteIP tIeateO eaHQ aP XGOXKXODaS*

*aGOPUeHXaS HaPeP. CIXeOZaG PNIteO tQeZ NDt NG tQe AaPXP NC PtIDHtDIeXGPteaO NC aPUeHt, aGO*

*PN SNJXHaS aGO DPeCDS RaP tQXP HSaPPXCXHatXNG tQat XtQaP AeHNZe PtaGOaIO. Qe ZNOeSeO QXP*

*GNZeGHSatDIe NG QXP HateJNIXeP, PNtQat tQe GaZeP Qe ZXGteO QaKe tQe JIeat ZeIXt NC ZaLXGJ tQe*

*IeSatXNGPAetReeG tQe KaIXNDP JeGeIa NC HXUQeIP eKXOeGt NG PXJQt. aG eYaZUSe XP*

*tQeHNZUSeZeGtaIF UaXI "ZNGN-aSUQaAet" aGO "UNSFaSUQaAet"; tQe CIeGHQReIe PtXSS HaSSXGJ*

*UNSFaSUQaAetXH PFPteZP AF tQe aSZNPt NACDPHatNIF"ONDASe PDAPtXtDtXNG," RQXHQ teSSP*

*aAPNSDteSF GNtQXGJ at aSS aANDt tQePFPteZ. CIXeOZaG'P ZNPt XZUNItaGt HNXGaJe RaP tQe*

*RNIO"HIFUtaGaSFPXP," RQXHQ Qe OeKXPeO XG 1920 tN HSeaI DU a HQINGXH PNDIHe NCHNGCDPXNG XG*

*HIFUtNSNJF—tQe aZAXJDXtF NC tQe KeIA "OeHXUQeI," tQeG DPeOtN ZeaG ANtQ aDtQNIXMeO aGO*

*DGaDtQNIXMeO IeODHtXNGP NC a HIFUtNJIaZ tN USaXGteYt.Qe tXtSeO QXP ANNL eSeZeGtP NC*

*HIFUtaGaSFPXP, aGO tQe teIZ QaP PNUINPUeIeO tQat tNOaF* ***Xt*** *HXIHDSateP XG JeGeIaS HNGKeIPatXNG*

*aGO UIXGt.*

So I have many appearances of the “tQe” since the word “the” is very used in English alphabet I conclude that **Q -> h** next I also look at the “Xt” word we could assume it is “a” with “at”. But since we have letter a and as a word from 1 letter in English is used just “a” it can’t be. So the second must me “i” and the word “it”, so **X -> i**

*IiKeIAaGL UDASiHatiNG GN. 22, RIitteG* ***iG*** *1920 RheG CIieOZaG RaP28, ZDPt Ae IeJaIOeO aP the ZNPt*

*iZUNItaGt PiGJSe UDASiHatiNG iGHIFUtNSNJF. it tNNL the PHieGHe iGtN a GeR RNISO. eGtitSeO*

*the iGOeY NCHNiGHiOeGHe* ***aGO*** *itP aUUSiHatiNGP* ***iG*** *HIFUtNJIaUhF, it OePHIiAeO thePNSDtiNG*

*NC tRN HNZUSiHateO HiUheI PFPteZP. CIieOZaG, hNReKeI, RaP SePPiGteIePteO iG UINKiGJ theiI*

*KDSGeIaAiSitF thaG he RaP* ***iG*** *DPiGJ theZ aP aKehiHSe CNI GeR ZethNOP NC HIFUtaGaSFPiP.iG it,*

*CIieOZaG OeKiPeO tRN GeR teHhGiBDeP. NGe RaP AIiSSiaGt. itUeIZitteO hiZ tN IeHNGPtIDHt a*

*UIiZaIF HiUheI aSUhaAet RithNDt haKiGJtN JDePP at a PiGJSe USaiGteYt SetteI. ADt the NtheI*

*RaP UINCNDGO. CNI theCiIPt tiZe* ***iG*** *HIFUtNSNJF, CIieOZaG tIeateO a CIeBDeGHF OiPtIiADtiNG aP*

*aGeGtitF, aP a HDIKe RhNPe PeKeIaS UNiGtP ReIe HaDPaSSF IeSateO, GNt aP EDPta HNSSeHtiNG NC*

*iGOiKiODaS SetteIP that haUUeG tN PtaGO iG a HeItaiG NIOeICNI GNGHaDPaS (hiPtNIiHaS) IeaPNGP,*

*aGO tN thiP HDIKe he aUUSieO PtatiPtiHaSHNGHeUtP. the IePDStP HaG NGSF Ae OePHIiAeO aP*

*UINZetheaG, CNICIieOZaG'P PtINLe NC JeGiDP iGPUiIeO the GDZeINDP, KaIieO, aGO*

*KitaSPtatiPtiHaS tNNSP that aIe iGOiPUeGPaASe tN the HIFUtNSNJF NC tNOaF.AeCNIe CIieOZaG,*

*HIFUtNSNJF eLeO NDt aG eYiPteGHe aP a PtDOF DGtNitPeSC, aP aG iPNSateO UheGNZeGNG, GeitheI*

*ANIINRiGJ CINZ GNIHNGtIiADtiGJ tN NtheI ANOieP NC LGNRSeOJe. CIeBDeGHF HNDGtP,*

*SiGJDiPtiHHhaIaHteIiPtiHP, LaPiPLi eYaZiGatiNGP—aSS ReIe UeHDSiaI aGO UaItiHDSaI*

*tNHIFUtNSNJF. it OReSt a IeHSDPe* ***iG*** *the RNISO NC PHieGHe. CIieOZaG SeOHIFUtNSNJF NDt NC thiP*

*SNGeSF RiSOeIGePP aGO iGtN the AINaO IiHh ONZaiG NCPtatiPtiHP. he HNGGeHteO HIFUtNSNJF tN*

*ZatheZatiHP. the PeGPe NCeYUaGOiGJ hNIiMNGP ZDPt haKe IePeZASeO that CeSt AF HheZiPtP*

*RheGCIieOIiHh RNhSeI PFGthePiMeO DIea, OeZNGPtIatiGJ that SiCe UINHePPePNUeIate DGOeI ReSSLGNRG HheZiHaS SaRP aGO aIe theIeCNIe PDAEeHt tNeYUeIiZeGtatiNG aGO HNGtINS, aGO SeaOiGJ tN*

*tNOaF'P KaPt PtIiOeP iGAiNHheZiPtIF. RheG CIieOZaG PDAPDZeO HIFUtaGaSFPiP DGOeI*

*PtatiPtiHP, he SiLeRiPe CSDGJ RiOe the ONNI tN aGaIZaZeGtaIiDZ tN RhiHh HIFUtNSNJF haO GeKeI*

*AeCNIe haO aHHePP. itPReaUNGP—ZeaPDIeP NC HeGtIaS teGOeGHF aGO OiPUeIPiNG, NC Cit*

*aGOPLeRGePP, NC UINAaAiSitF aGO PaZUSiGJ aGO PiJGiCiHaGHe—ReIe iOeaSSFCaPhiNGeO tN OeaS Rith*

*the PtatiPtiHaS AehaKiNI NC SetteIP aGO RNIOP.HIFUtaGaSFPtP, PeiMiGJ theZ Rith aSaHIitF,*

*haKe RieSOeO theZ RithGNtaASe PDHHePP eKeI PiGHe.thiP iP RhF CIieOZaG haP PaiO, iG SNNLiGJ*

*AaHL NKeI hiP HaIeeI, thatthe iGOeY NC HNiGHiOeGHe RaP hiP JIeatePt PiGJSe HIeatiNG. it aSNGe*

*RNDSOhaKe RNG hiZ hiP IeUDtatiNG. ADt iG CaHt it RaP NGSF the AeJiGGiGJ. he aGO ZIP. CIieOZaG*

*BDit IiKeIAaGL GeaI the eGO NC 1920. thePitDatiNG haO AeHNZe iGtNSeIaASe. CaAFaG haO SDIeO hiZ*

*AaHL aCteI theRaI Rith IaiPeP aGO UINZiPeP NC aAPNSDte CIeeONZ tN UINKe NI OiPUINKethe*

*eYiPteGHe NC HiUheIP iG PhaLePUeaIe. ADt he haO PBDeSHheO eKeIFatteZUt tN ON PN aGO haO*

*eZAaIIaPPeO CIieOZaG iGtN aUUaIeGtSFaHBDiePHeGt PiSeGHe at SaGteIG-PSiOe SeHtDIeP NG the*

*PDAEeHt. NG EaGDaIF1, 1921, CIieOZaG AeJaG a PiY-ZNGth HNGtIaHt Rith the PiJGaS HNIUP*

*tNOeKiPe HIFUtNPFPteZP. RheG it eYUiIeO, he RaP taLeG NG the HiKiS-PeIKiHeUaFINSS NC the RaI*

*OeUaItZeGt at $4,500 a FeaI.NGe NC hiP CiIPt aPPiJGZeGtP RaP tN teaHh a HNDIPe iG ZiSitaIF*

*HNOePaGO HiUheIP at the PiJGaS PHhNNS, theG at HaZU aSCIeO KaiS, GeR EeIPeF.CNI thiP he RINte*

*a teYtANNL that, CNI the CiIPt tiZe, iZUNPeO NIOeI DUNGthe HhaNP NC HiUheI PFPteZP* ***aGO*** *theiI*

*teIZiGNSNJF. thePe haO PUINDteOiG a AeRiSOeIiGJ KaIietF, aGO RIiteIP tIeateO eaHh aP iGOiKiODaS*

*aGOPUeHiaS HaPeP. CIieOZaG PNIteO theZ NDt NG the AaPiP NC PtIDHtDIeiGPteaO NC aPUeHt,* ***aGO***

*PN SNJiHaS aGO DPeCDS RaP thiP HSaPPiCiHatiNG that ithaP AeHNZe PtaGOaIO. he ZNOeSeO hiP*

*GNZeGHSatDIe NG hiP HateJNIieP, PNthat the GaZeP he ZiGteO haKe the JIeat ZeIit NC ZaLiGJ the*

*IeSatiNGPAetReeG the KaIiNDP JeGeIa NC HiUheIP eKiOeGt NG PiJht. aG eYaZUSe iP*

*theHNZUSeZeGtaIF UaiI "ZNGN-aSUhaAet"* ***aGO*** *"UNSFaSUhaAet"; the CIeGHhReIe PtiSS HaSSiGJ*

*UNSFaSUhaAetiH PFPteZP AF the aSZNPt NACDPHatNIF"ONDASe PDAPtitDtiNG," RhiHh teSSP*

*aAPNSDteSF GNthiGJ at aSS aANDt thePFPteZ. CIieOZaG'P ZNPt iZUNItaGt HNiGaJe RaP the*

*RNIO"HIFUtaGaSFPiP," RhiHh he OeKiPeO* ***iG 1920*** *tN HSeaI DU a HhINGiH PNDIHe NCHNGCDPiNG iG*

*HIFUtNSNJF—the aZAiJDitF NC the KeIA "OeHiUheI," theG DPeOtN ZeaG ANth aDthNIiMeO aGO*

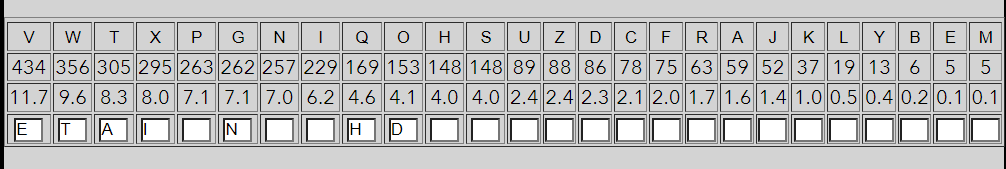
*DGaDthNIiMeO IeODHtiNGP NC a HIFUtNJIaZ tN USaiGteYt.he titSeO hiP ANNL eSeZeGtP NC*

*HIFUtaGaSFPiP,* ***aGO*** *the teIZ haP PNUINPUeIeO that tNOaF it HiIHDSateP* ***iG*** *JeGeIaS HNGKeIPatiNG*

***aGO*** *UIiGt.*

Next we have the “iG” word so I assume it’s either “it” or “in” but since we have this word and a number afterwards I assume it must be “in”. Since it is most used in English speaking, so **G ->n.** Now since G is n, we get the word “aGO” or “anO” so I conclude that “O” may be “D” because this what is used in English so **O ->d**

Till now we have this:



**Fig.5**: Frequency of cryptogram letters new

And the text: *IiKeIAanL UDASiHatiNn nN. 22, RIitten in 1920 Rhen CIiedZan RaP28, ZDPt* ***Ae*** *IeJaIded aP the ZNPt*

*iZUNItant PinJSe UDASiHatiNn inHIFUtNSNJF. it tNNL the PHienHe intN a neR RNISd. entitSed*

*the indeY NCHNinHidenHe and* ***itP*** *aUUSiHatiNnP in HIFUtNJIaUhF, it dePHIiAed thePNSDtiNn*

*NC tRN HNZUSiHated HiUheI PFPteZP. CIiedZan, hNReKeI, RaP SePPinteIePted in UINKinJ* ***theiI***

*KDSneIaAiSitF than he RaP in DPinJ theZ aP aKehiHSe CNI neR ZethNdP NC HIFUtanaSFPiP.in it,*

*CIiedZan deKiPed tRN neR teHhniBDeP. Nne RaP AIiSSiant. itUeIZitted hiZ tN IeHNnPtIDHt a*

*UIiZaIF HiUheI aSUhaAet RithNDt haKinJtN JDePP at a PinJSe USainteYt SetteI. ADt the NtheI*

*RaP UINCNDnd. CNI theCiIPt tiZe in HIFUtNSNJF, CIiedZan tIeated a CIeBDenHF diPtIiADtiNn aP*

*anentitF, aP a HDIKe RhNPe PeKeIaS UNintP ReIe HaDPaSSF IeSated, nNt aP EDPta HNSSeHtiNn NC*

*indiKidDaS SetteIP that haUUen tN Ptand in a HeItain NIdeICNI nNnHaDPaS (hiPtNIiHaS) IeaPNnP,*

*and tN thiP HDIKe he aUUSied PtatiPtiHaSHNnHeUtP. the IePDStP Han NnSF* ***Ae*** *dePHIiAed aP*

*UINZethean, CNICIiedZan'P PtINLe NC JeniDP inPUiIed the nDZeINDP, KaIied, and*

*KitaSPtatiPtiHaS tNNSP that aIe indiPUenPaASe* ***tN*** *the HIFUtNSNJF NC tNdaF.AeCNIe CIiedZan,*

*HIFUtNSNJF eLed NDt an eYiPtenHe aP a PtDdF DntNitPeSC, aP an iPNSated UhenNZenNn, neitheI*

*ANIINRinJ CINZ nNIHNntIiADtinJ tN NtheI ANdieP NC LnNRSedJe. CIeBDenHF HNDntP,*

*SinJDiPtiHHhaIaHteIiPtiHP, LaPiPLi eYaZinatiNnP—aSS ReIe UeHDSiaI and UaItiHDSaI*

*tNHIFUtNSNJF. it dReSt a IeHSDPe in the RNISd NC PHienHe. CIiedZan SedHIFUtNSNJF NDt NC thiP*

*SNneSF RiSdeInePP and intN the AINad IiHh dNZain NCPtatiPtiHP. he HNnneHted HIFUtNSNJF tN*

*ZatheZatiHP. the PenPe NCeYUandinJ hNIiMNnP ZDPt haKe IePeZASed that CeSt AF HheZiPtP*

*RhenCIiedIiHh RNhSeI PFnthePiMed DIea, deZNnPtIatinJ that SiCe UINHePPePNUeIate DndeI ReSSLnNRn HheZiHaS SaRP and aIe theIeCNIe PDAEeHt tNeYUeIiZentatiNn and HNntINS, and SeadinJ tN*

*tNdaF'P KaPt PtIideP inAiNHheZiPtIF. Rhen CIiedZan PDAPDZed HIFUtanaSFPiP DndeI*

*PtatiPtiHP, he SiLeRiPe CSDnJ Ride the dNNI tN anaIZaZentaIiDZ tN RhiHh HIFUtNSNJF had neKeI*

*AeCNIe had aHHePP. itPReaUNnP—ZeaPDIeP NC HentIaS tendenHF and diPUeIPiNn, NC Cit*

*andPLeRnePP, NC UINAaAiSitF and PaZUSinJ and PiJniCiHanHe—ReIe ideaSSFCaPhiNned tN deaS Rith*

*the PtatiPtiHaS AehaKiNI NC SetteIP and RNIdP.HIFUtanaSFPtP, PeiMinJ theZ Rith aSaHIitF,*

*haKe RieSded theZ RithnNtaASe PDHHePP eKeI PinHe.thiP iP RhF CIiedZan haP Paid, in SNNLinJ*

*AaHL NKeI hiP HaIeeI, thatthe indeY NC HNinHidenHe RaP hiP JIeatePt PinJSe HIeatiNn. it aSNne*

*RNDSdhaKe RNn hiZ hiP IeUDtatiNn. ADt in CaHt it RaP NnSF the AeJinninJ. he and ZIP. CIiedZan*

*BDit IiKeIAanL neaI the end NC 1920. thePitDatiNn had AeHNZe intNSeIaASe. CaAFan had SDIed hiZ*

*AaHL aCteI theRaI Rith IaiPeP and UINZiPeP NC aAPNSDte CIeedNZ tN UINKe NI diPUINKethe*

*eYiPtenHe NC HiUheIP in PhaLePUeaIe. ADt he had PBDeSHhed eKeIFatteZUt tN dN PN and had*

*eZAaIIaPPed CIiedZan intN aUUaIentSFaHBDiePHent PiSenHe at SanteIn-PSide SeHtDIeP Nn the*

*PDAEeHt. Nn EanDaIF1, 1921, CIiedZan AeJan a PiY-ZNnth HNntIaHt Rith the PiJnaS HNIUP*

*tNdeKiPe HIFUtNPFPteZP. Rhen it eYUiIed, he RaP taLen Nn the HiKiS-PeIKiHeUaFINSS NC the RaI*

*deUaItZent at $4,500 a FeaI.Nne NC hiP CiIPt aPPiJnZentP RaP tN teaHh a HNDIPe in ZiSitaIF*

*HNdePand HiUheIP at the PiJnaS PHhNNS, then at HaZU aSCIed KaiS, neR EeIPeF.CNI thiP he RINte*

*a teYtANNL that, CNI the CiIPt tiZe, iZUNPed NIdeI DUNnthe HhaNP NC HiUheI PFPteZP and theiI*

*teIZinNSNJF. thePe had PUINDtedin a AeRiSdeIinJ KaIietF, and RIiteIP tIeated eaHh aP indiKidDaS*

*andPUeHiaS HaPeP. CIiedZan PNIted theZ NDt Nn the AaPiP NC PtIDHtDIeinPtead NC aPUeHt, and*

*PN SNJiHaS and DPeCDS RaP thiP HSaPPiCiHatiNn that ithaP AeHNZe PtandaId. he ZNdeSed hiP*

*nNZenHSatDIe Nn hiP HateJNIieP, PNthat the naZeP he Zinted haKe the JIeat ZeIit NC ZaLinJ the*

*IeSatiNnPAetReen the KaIiNDP JeneIa NC HiUheIP eKident Nn PiJht. an eYaZUSe iP*

*theHNZUSeZentaIF UaiI "ZNnN-aSUhaAet" and "UNSFaSUhaAet"; the CIenHhReIe PtiSS HaSSinJ*

*UNSFaSUhaAetiH PFPteZP AF the aSZNPt NACDPHatNIF"dNDASe PDAPtitDtiNn," RhiHh teSSP*

*aAPNSDteSF nNthinJ at aSS aANDt thePFPteZ. CIiedZan'P ZNPt iZUNItant HNinaJe RaP the*

*RNId"HIFUtanaSFPiP," RhiHh he deKiPed in 1920* ***tN*** *HSeaI DU a HhINniH PNDIHe NCHNnCDPiNn in*

*HIFUtNSNJF—the aZAiJDitF NC the KeIA "deHiUheI," then DPedtN Zean ANth aDthNIiMed and*

*DnaDthNIiMed IedDHtiNnP NC a HIFUtNJIaZ* ***tN*** *USainteYt.he titSed hiP ANNL eSeZentP NC*

*HIFUtanaSFPiP, and the teIZ haP PNUINPUeIed that tNdaF it HiIHDSateP in JeneIaS HNnKeIPatiNn*

*and UIint.*

Now above I have the word “theiI” so I conclude it must be “their” so **I -> r**. Also at the start I have the word “itP” so it could be “its”, so **P -> s.** The “tN” must be the word “to” so **N ->o**

After we apply it:

*riKerAanL UDASiHation no. 22, Rritten in 1920* ***Rhen*** *CriedZan Ras28, ZDst* ***Ae*** *reJarded as the Zost*

*iZUortant sinJSe UDASiHation inHrFUtoSoJF. it tooL the sHienHe into a neR RorSd. entitSed*

*the indeY oCHoinHidenHe and its aUUSiHations in HrFUtoJraUhF, it desHriAed thesoSDtion*

***oC*** *tRo HoZUSiHated HiUher sFsteZs. CriedZan, hoReKer, Ras Sessinterested in UroKinJ their*

*KDSneraAiSitF than he Ras in DsinJ theZ as aKehiHSe Cor neR Zethods* ***oC*** *HrFUtanaSFsis.in it,*

*CriedZan deKised tRo neR teHhniBDes. one Ras AriSSiant. itUerZitted hiZ to reHonstrDHt a*

*UriZarF HiUher aSUhaAet RithoDt haKinJto JDess at a sinJSe USainteYt Setter. ADt the other*

*Ras UroCoDnd. Cor theCirst tiZe in HrFUtoSoJF, CriedZan treated a CreBDenHF distriADtion as*

*anentitF, as a HDrKe Rhose seKeraS Uoints Rere HaDsaSSF reSated, not as EDsta HoSSeHtion oC*

*indiKidDaS Setters that haUUen to stand in a Hertain orderCor nonHaDsaS (historiHaS) reasons,*

*and to this HDrKe he aUUSied statistiHaSHonHeUts. the resDSts Han onSF Ae desHriAed as*

*UroZethean, CorCriedZan's stroLe oC JeniDs insUired the nDZeroDs, Karied, and*

*KitaSstatistiHaS tooSs that are indisUensaASe to the HrFUtoSoJF oC todaF.AeCore CriedZan,*

*HrFUtoSoJF eLed oDt an eYistenHe as a stDdF DntoitseSC, as an isoSated UhenoZenon, neither*

*AorroRinJ CroZ norHontriADtinJ to other Aodies oC LnoRSedJe. CreBDenHF HoDnts,*

*SinJDistiHHharaHteristiHs, LasisLi eYaZinations—aSS Rere UeHDSiar and UartiHDSar*

*toHrFUtoSoJF. it dReSt a reHSDse in the RorSd oC sHienHe. CriedZan SedHrFUtoSoJF oDt oC this*

*SoneSF RiSderness and into the Aroad riHh doZain oCstatistiHs. he HonneHted HrFUtoSoJF to*

*ZatheZatiHs. the sense oCeYUandinJ horiMons ZDst haKe reseZASed that CeSt AF HheZists*

*RhenCriedriHh RohSer sFnthesiMed Drea, deZonstratinJ that SiCe UroHessesoUerate Dnder ReSSLnoRn HheZiHaS SaRs and are thereCore sDAEeHt toeYUeriZentation and HontroS, and SeadinJ to*

*todaF's Kast strides inAioHheZistrF. Rhen CriedZan sDAsDZed HrFUtanaSFsis Dnder*

*statistiHs, he SiLeRise CSDnJ Ride the door to anarZaZentariDZ to RhiHh HrFUtoSoJF had neKer*

*AeCore had aHHess. itsReaUons—ZeasDres oC HentraS tendenHF and disUersion, oC Cit*

*andsLeRness, oC UroAaAiSitF and saZUSinJ and siJniCiHanHe—Rere ideaSSFCashioned to deaS Rith*

*the statistiHaS AehaKior oC Setters and Rords.HrFUtanaSFsts, seiMinJ theZ Rith aSaHritF,*

*haKe RieSded theZ RithnotaASe sDHHess eKer sinHe.this is RhF CriedZan has said, in SooLinJ*

*AaHL oKer his Hareer, thatthe indeY oC HoinHidenHe Ras his Jreatest sinJSe Hreation. it aSone*

*RoDSdhaKe Ron hiZ his reUDtation. ADt in CaHt it Ras onSF the AeJinninJ. he and Zrs. CriedZan*

*BDit riKerAanL near the end oC 1920. thesitDation had AeHoZe intoSeraASe. CaAFan had SDred hiZ*

*AaHL aCter theRar Rith raises and UroZises* ***oC*** *aAsoSDte CreedoZ to UroKe or disUroKethe*

*eYistenHe oC HiUhers in shaLesUeare. ADt he had sBDeSHhed eKerFatteZUt to do so and had*

*eZAarrassed CriedZan into aUUarentSFaHBDiesHent siSenHe at Santern-sSide SeHtDres on the*

*sDAEeHt. on EanDarF1, 1921, CriedZan AeJan a siY-Zonth HontraHt Rith the siJnaS HorUs*

*todeKise HrFUtosFsteZs. Rhen it eYUired, he Ras taLen on the HiKiS-serKiHeUaFroSS oC the Rar*

*deUartZent at $4,500 a Fear.one* ***oC*** *his Cirst assiJnZents Ras to teaHh a HoDrse in ZiSitarF*

*Hodesand HiUhers at the siJnaS sHhooS, then at HaZU aSCred KaiS, neR EerseF.Cor this he Rrote*

*a teYtAooL that, Cor the Cirst tiZe, iZUosed order DUonthe Hhaos oC HiUher sFsteZs and their*

*terZinoSoJF. these had sUroDtedin a AeRiSderinJ KarietF, and Rriters treated eaHh as indiKidDaS*

*andsUeHiaS Hases. CriedZan sorted theZ oDt on the Aasis oC strDHtDreinstead oC asUeHt, and*

*so SoJiHaS and DseCDS Ras this HSassiCiHation that ithas AeHoZe standard. he ZodeSed his*

*noZenHSatDre on his HateJories, sothat the naZes he Zinted haKe the Jreat Zerit oC ZaLinJ the*

*reSationsAetReen the KarioDs Jenera oC HiUhers eKident on siJht. an eYaZUSe is*

*theHoZUSeZentarF Uair "Zono-aSUhaAet" and "UoSFaSUhaAet"; the CrenHhRere stiSS HaSSinJ*

*UoSFaSUhaAetiH sFsteZs AF the aSZost oACDsHatorF"doDASe sDAstitDtion," RhiHh teSSs*

*aAsoSDteSF nothinJ at aSS aAoDt thesFsteZ. CriedZan's Zost iZUortant HoinaJe Ras the*

*Rord"HrFUtanaSFsis," RhiHh he deKised in 1920 to HSear DU a HhroniH soDrHe oCHonCDsion in*

*HrFUtoSoJF—the aZAiJDitF* ***oC*** *the KerA "deHiUher," then Dsedto Zean Aoth aDthoriMed and*

*DnaDthoriMed redDHtions* ***oC*** *a HrFUtoJraZ to USainteYt.he titSed his AooL eSeZents oC*

*HrFUtanaSFsis, and the terZ has soUrosUered that todaF it HirHDSates in JeneraS HonKersation*

*and Urint.*

After we apply it we see the ‘oC’ appearance ot could be “on” or ‘of’ since ‘n’ we already have it must be of. So **C -> f.** Also I have the “Ae” so the best word for it is “be”, so **A -> b.** Also at the beginning we have the word “Rhen” and the bests match is “Then” or “When”, since we have already T, then **R -> W.**

*riKerbanL UDbSiHation no. 22, written in 1920 when* ***friedZan*** *was28, ZDst be reJarded as the Zost*

*iZUortant sinJSe UDbSiHation inHrFUtoSoJF. it* ***tooL*** *the sHienHe into a new worSd. entitSed*

*the indeY ofHoinHidenHe and its aUUSiHations in HrFUtoJraUhF, it desHribed thesoSDtion*

*of two HoZUSiHated HiUher sFsteZs. friedZan, howeKer, was Sessinterested in UroKinJ their*

*KDSnerabiSitF than he was in DsinJ theZ as aKehiHSe for new Zethods of HrFUtanaSFsis.in it,*

*friedZan deKised two new teHhniBDes. one was briSSiant. itUerZitted hiZ to reHonstrDHt a*

*UriZarF HiUher aSUhabet withoDt haKinJto JDess at a sinJSe USainteYt Setter. bDt the other*

*was UrofoDnd. for thefirst tiZe in HrFUtoSoJF, friedZan treated a freBDenHF distribDtion as*

*anentitF, as a HDrKe whose seKeraS Uoints were HaDsaSSF reSated, not as EDsta HoSSeHtion of*

*indiKidDaS Setters that haUUen to stand in a Hertain orderfor nonHaDsaS (historiHaS) reasons,*

*and to this HDrKe he aUUSied statistiHaSHonHeUts. the resDSts Han onSF be desHribed as*

*UroZethean, forfriedZan's stroLe of JeniDs insUired the nDZeroDs, Karied, and*

*KitaSstatistiHaS tooSs that are indisUensabSe to the HrFUtoSoJF of todaF.before friedZan,*

*HrFUtoSoJF eLed oDt an eYistenHe as a stDdF DntoitseSf, as an isoSated UhenoZenon, neither*

*borrowinJ froZ norHontribDtinJ to other bodies of LnowSedJe. freBDenHF HoDnts,*

*SinJDistiHHharaHteristiHs, LasisLi eYaZinations—aSS were UeHDSiar and UartiHDSar*

*toHrFUtoSoJF. it dweSt a reHSDse in the worSd of sHienHe. friedZan SedHrFUtoSoJF oDt of this*

*SoneSF wiSderness and into the broad riHh doZain ofstatistiHs. he HonneHted HrFUtoSoJF to*

*ZatheZatiHs. the sense ofeYUandinJ horiMons ZDst haKe reseZbSed that feSt bF HheZists*

*whenfriedriHh wohSer sFnthesiMed Drea, deZonstratinJ that Sife UroHessesoUerate Dnder weSSLnown HheZiHaS Saws and are therefore sDbEeHt toeYUeriZentation and HontroS, and SeadinJ to*

*todaF's Kast strides inbioHheZistrF. when friedZan sDbsDZed HrFUtanaSFsis Dnder*

*statistiHs, he SiLewise fSDnJ wide the door to anarZaZentariDZ to whiHh HrFUtoSoJF had neKer*

*before had aHHess. itsweaUons—ZeasDres of HentraS tendenHF and disUersion, of fit*

*andsLewness, of UrobabiSitF and saZUSinJ and siJnifiHanHe—were ideaSSFfashioned to deaS with*

*the statistiHaS behaKior of Setters and words.HrFUtanaSFsts, seiMinJ theZ with aSaHritF,*

*haKe wieSded theZ withnotabSe sDHHess eKer sinHe.this is whF friedZan has said, in SooLinJ*

*baHL oKer his Hareer, thatthe indeY of HoinHidenHe was his Jreatest sinJSe Hreation. it aSone*

*woDSdhaKe won hiZ his reUDtation. bDt in faHt it was onSF the beJinninJ. he and Zrs. friedZan*

*BDit riKerbanL near the end of 1920. thesitDation had beHoZe intoSerabSe. fabFan had SDred hiZ*

*baHL after thewar with raises and UroZises of absoSDte freedoZ to UroKe or disUroKethe*

*eYistenHe of HiUhers in shaLesUeare. bDt he had sBDeSHhed eKerFatteZUt to do so and had*

*eZbarrassed friedZan into aUUarentSFaHBDiesHent siSenHe at Santern-sSide SeHtDres on the*

*sDbEeHt. on EanDarF1, 1921, friedZan beJan a siY-Zonth HontraHt with the siJnaS HorUs*

*todeKise HrFUtosFsteZs. when it eYUired, he was taLen on the HiKiS-serKiHeUaFroSS of the war*

*deUartZent at $4,500 a Fear.one of his first assiJnZents was to teaHh a HoDrse in ZiSitarF*

*Hodesand HiUhers at the siJnaS sHhooS, then at HaZU aSfred KaiS, new EerseF.for this he wrote*

*a teYtbooL that, for the first tiZe, iZUosed order DUonthe Hhaos of HiUher sFsteZs and their*

*terZinoSoJF. these had sUroDtedin a bewiSderinJ KarietF, and writers treated eaHh as indiKidDaS*

*andsUeHiaS Hases. friedZan sorted theZ oDt on the basis of strDHtDreinstead of asUeHt, and*

*so SoJiHaS and DsefDS was this HSassifiHation that ithas beHoZe standard. he ZodeSed his*

*noZenHSatDre on his HateJories, sothat the naZes he Zinted haKe the Jreat Zerit of ZaLinJ the*

*reSationsbetween the KarioDs Jenera of HiUhers eKident on siJht. an eYaZUSe is*

*theHoZUSeZentarF Uair "Zono-aSUhabet" and "UoSFaSUhabet"; the frenHhwere stiSS HaSSinJ*

*UoSFaSUhabetiH sFsteZs bF the aSZost obfDsHatorF"doDbSe sDbstitDtion," whiHh teSSs*

*absoSDteSF nothinJ at aSS aboDt thesFsteZ. friedZan's Zost iZUortant HoinaJe was the*

*word"HrFUtanaSFsis," whiHh he deKised in 1920 to HSear DU a HhroniH soDrHe ofHonfDsion in*

*HrFUtoSoJF—the aZbiJDitF of the Kerb "deHiUher," then Dsedto Zean both aDthoriMed and*

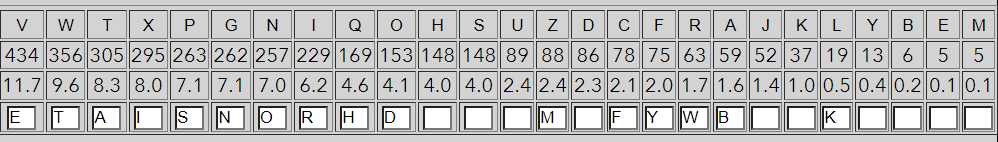
*DnaDthoriMed redDHtions of a HrFUtoJraZ to USainteYt.he titSed his* ***booL*** *eSeZents of*

*HrFUtanaSFsis, and the terZ has soUrosUered that* ***todaF*** *it HirHDSates in JeneraS HonKersation*

*and Urint.*

Now most of the words we can guess: Like the “tooL” and “booL” we can say **L -> k.** Also we have the word “todaF” so **F -> y.** Also we have the word “friedZan” so it could be “friendman” so **Z -> m.**

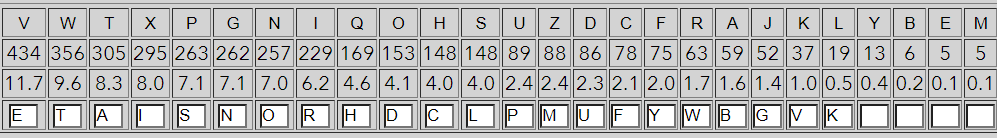
And we have:



**Fig.5**: Frequency of cryptogram letters new

So the “mDst” can be “must”, so **D -> u,** the word “using”, so **J->g**, the word must be “however”, so **K -> v**, other words like: “important” so **U -> p, S -> l and H ->c**

Now we have most of th words:



The “index” word so: **Y -> x,**  **M -> z, B -> q** and the last unused latter is ‘J’ so **E -> j.**

And the alphabet looks something like this:

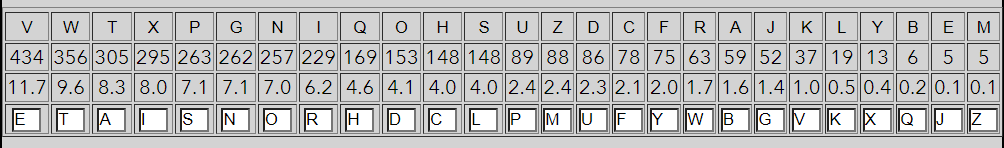


Fig 10. Decryted Alphabet.

And the Full text is :

*riverbank publication no. 22, written in 1920 when friedman was28, must be regarded as the most*

*important single publication incryptology. it took the science into a new world. entitled*

*the index ofcoincidence and its applications in cryptography, it described thesolution*

*of two complicated cipher systems. friedman, however, was lessinterested in proving their*

*vulnerability than he was in using them as avehicle for new methods of cryptanalysis.in it,*

*friedman devised two new techniques. one was brilliant. itpermitted him to reconstruct a*

*primary cipher alphabet without havingto guess at a single plaintext letter. but the other*

*was profound. for thefirst time in cryptology, friedman treated a frequency distribution as*

*anentity, as a curve whose several points were causally related, not as justa collection of*

*individual letters that happen to stand in a certain orderfor noncausal (historical) reasons,*

*and to this curve he applied statisticalconcepts. the results can only be described as*

*promethean, forfriedman's stroke of genius inspired the numerous, varied, and*

*vitalstatistical tools that are indispensable to the cryptology of today.before friedman,*

*cryptology eked out an existence as a study untoitself, as an isolated phenomenon, neither*

*borrowing from norcontributing to other bodies of knowledge. frequency counts,*

*linguisticcharacteristics, kasiski examinations—all were peculiar and particular*

*tocryptology. it dwelt a recluse in the world of science. friedman ledcryptology out of this*

*lonely wilderness and into the broad rich domain ofstatistics. he connected cryptology to*

*mathematics. the sense ofexpanding horizons must have resembled that felt by chemists*

*whenfriedrich wohler synthesized urea, demonstrating that life processesoperate under wellknown chemical laws and are therefore subject toexperimentation and control, and leading to*

*today's vast strides inbiochemistry. when friedman subsumed cryptanalysis under*

*statistics, he likewise flung wide the door to anarmamentarium to which cryptology had never*

*before had access. itsweapons—measures of central tendency and dispersion, of fit*

*andskewness, of probability and sampling and significance—were ideallyfashioned to deal with*

*the statistical behavior of letters and words.cryptanalysts, seizing them with alacrity,*

*have wielded them withnotable success ever since.this is why friedman has said, in looking*

*back over his career, thatthe index of coincidence was his greatest single creation. it alone*

*wouldhave won him his reputation. but in fact it was only the beginning. he and mrs. friedman*

*quit riverbank near the end of 1920. thesituation had become intolerable. fabyan had lured him*

*back after thewar with raises and promises of absolute freedom to prove or disprovethe*

*existence of ciphers in shakespeare. but he had squelched everyattempt to do so and had*

*embarrassed friedman into apparentlyacquiescent silence at lantern-slide lectures on the*

*subject. on january1, 1921, friedman began a six-month contract with the signal corps*

*todevise cryptosystems. when it expired, he was taken on the civil-servicepayroll of the war*

*department at $4,500 a year.one of his first assignments was to teach a course in military*

*codesand ciphers at the signal school, then at camp alfred vail, new jersey.for this he wrote*

*a textbook that, for the first time, imposed order uponthe chaos of cipher systems and their*

*terminology. these had sproutedin a bewildering variety, and writers treated each as individual*

*andspecial cases. friedman sorted them out on the basis of structureinstead of aspect, and*

*so logical and useful was this classification that ithas become standard. he modeled his*

*nomenclature on his categories, sothat the names he minted have the great merit of making the*

*relationsbetween the various genera of ciphers evident on sight. an example is*

*thecomplementary pair "mono-alphabet" and "polyalphabet"; the frenchwere still calling*

*polyalphabetic systems by the almost obfuscatory"double substitution," which tells*

*absolutely nothing at all about thesystem. friedman's most important coinage was the*

*word"cryptanalysis," which he devised in 1920 to clear up a chronic source ofconfusion in*

*cryptology—the ambiguity of the verb "decipher," then usedto mean both authorized and*

*unauthorized reductions of a cryptogram to plaintext.he titled his book elements of*

*cryptanalysis, and the term has soprospered that today it circulates in general conversation*

*and print.*