MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică şi Microelectronică

Departamentul Inginerie Software și Automatică

RAPORT

Lucrare de laborator nr. 2

la disciplina „*Criptografie*”

Tema: Criptanaliza cifrurilor monoalfabetice

A efectuat : **St. gr. SI-253, Borta Adrian**

A verificat: **Asis.univ. Zaica Maia**

Chișinău 2025

INTRODUCERE

Punctul vulnerabil al cifrurilor monoalfabetice este distribuţia frecvenţei literelor din text. Dacă avem un mesaj criptat suficient de lung şi cunoaştem limba textului original, putem sparge sistemul folosind analiza frecvenţei: comparăm cât de des apar caracterele în textul criptat cu frecvenţele tipice ale literelor în limba respectivă. Pe măsură ce textul criptat devine mai lung, ordinea frecvenţelor literelor din el tinde să se potrivească cu ordinea generală pentru acea limbă. Aliniind ordinea literelor din textul criptat cu ordinea limbii, se pot stabili echivalenţele între literele din textul clar şi cele din textul criptat, ceea ce duce, în cele din urmă, la determinarea cheii de criptare.

1.SARCINA

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-the-code.html. Fiecare student va lua varianta în conformitate cu numărul său de ordine din lista grupei.

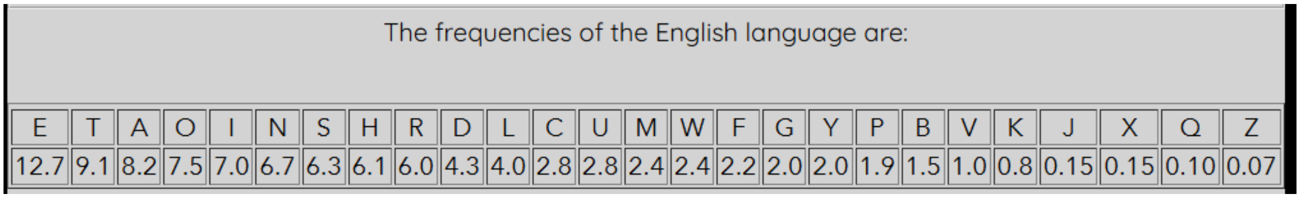
2.MERSUL LUCRĂRII

Ca variantă am V5

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 xw, Cixvoztg ovkxpvo wrn gvr wvhqgxbdvp. Ngv rtp aixssxtgw. Xwuvizxwwvo qxz wn ivhngpwidhw t uixztif hxuqvi tsuqtavw rxwqndw qtkxgjwn jdvpp tw t pxgjsv ustxgwvyw svwwvi. Adw wqv nwqvi rtp uincndgo. Cni wqvcxipw wxzv xg hifuwnsnjf, Cixvoztg wivtwvo t civbdvghf oxpwixadwxng tp tgvgwxwf, tp t hdikv rqnpv pvkvits unxgwp rviv htdptssf ivstwvo, gnw tp edpwt hnssvhwxng nc xgoxkxodts svwwvip wqtw qtuuvg wn pwtgo xg t hviwtxg niovicni gnghtdpts (qxpwnixhts) ivtpngp, tgo wn wqxp hdikv qv tuusxvo pwtwxpwxhtshnghvuwp. 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 rvss-lgnrg 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.

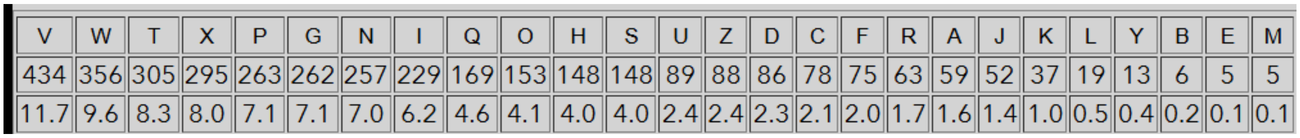
Primul pas este să găsim frecvențele tuturor literelor care apar în criptogramă, așa cum e arătat în tabelul 2.1.



The frequencies of the English language are:

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07

Tabelul 2.1. Frecvența literelor a limbii engleze



V	W	T	X	P	G	N	I	Q	O	H	S	U	Z	D	C	F	R	A	J	K	L	Y	B	E	M
434	356	305	295	263	262	257	229	169	153	148	148	89	88	86	78	75	63	59	52	37	19	13	6	5	5
11.7	9.6	8.3	8.0	7.1	7.1	7.0	6.2	4.6	4.1	4.0	4.0	2.4	2.4	2.3	2.1	2.0	1.7	1.6	1.4	1.0	0.5	0.4	0.2	0.1	0.1

Tabelul 2.2. Frecvența literelor in criptograma interceptată

Acum că avem toate frecvențele literelor din textul cifrat, putem începe să facem câteva substituții.Vedem ca cea mai frecventă literă din textul cifrat este „V” si putem ghici ca aceasta litera reprezintă „e”. De asemenea litera din textul cifrat „W” are a 2 cea mai mare frecvență și îl putem substitui cu „t”,iar după efectuarea schimbarilor obținem:

IXKeIATGL UDASXHTtXNG GN. 22, RIXtteG XG 1920 RQeG CIXeOZTG RTP28, ZDPt Ae IeJTIOeO TP tQe ZNPt XZUNItTGt PXGJSe UDASXHTtXNG XGHIFUtNSNJF. Xt tNNL tQe PHXeGHe XGtN T GeR RNISO. eGtXtSeO tQe XGOeY NCHNXGHXOeGHe TGO XtP TUUSXHTtXNGP XG HIFUtNJITUQF, Xt OePHIXAeO tQePNSDtXNG NC tRN HNZUSXHTteO HXUQeI PFPteZP. CIXeOZTG, QNReKeI, RTP SePPXGteIePteO XG UINKXGJ tQeXI KDSGeITAXSXtF tQTG Qe RTP XG DPXGJ tQeZ TP TKeQXHSe CNI GeR ZetQNOP NC HIFUtTGTSFPXP.XG Xt, CIXeOZTG OeKXPeO tRN GeR teHQGXBDeP. NGe RTP AIXSSXTGt. XtUeIZXtteO QXZ tN IeHNGPtIDHt T UIXZTIF HXUQeI TSUQTAet RXtQNDt QTKXGJtN JDePP Tt T PXGJSe USTXGteYt SetteI. ADt tQe NtQeI RTP UINCNDGO. CNI tQeCXIPt tXZe XG HIFUtNSNJF, CIXeOZTG tIeTteO T CIeBDeGHF OXPtIXADtXNG TP TGeGtXtF, TP T HDIKe RQNPe PeKeITS UNXGtP ReIe HTDPTSSF IeSTteO, GNt TP EDPtT HNSSeHtXNG NC XGOXKXODTS SetteIP tQTt QTUUeG tN PtTGO XG T HeItTXG NIOeICNI GNGHTDPTS (QXPtNIXHTS) IeTPNGP, TGO tN tQXP HDIKe Qe TUUSXeO PtTtXPtXHTSHNGHeUtP. tQe IePDStP HTG NGSF Ae OePHIXAeO TP UINZetQeTG, CNICIXeOZTG'P PtINLe NC JeGXDP XGPUXIeO tQe GDZeINDP, KTIXeO, TGO KXtTSPtTtXPtXHTS tNNSP tQTt TIe XGOXPUeGPTASe tN tQe HIFUtNSNJF NC tNOTF.AeCNIe CIXeOZTG, HIFUtNSNJF eLeO NDt

TG eYXPteGHe TP T PtDOF DGtNXtPeSC, TP TG XPNSTteO UQeGNZeGNG, GeXtQeI ANIINRXGJ CINZ GNIHNGtIXADtXGJ tN NtQeI ANOXeP NC LGNRSeOJe. CIeBDeGHF HNDGtP, SXGJDXPtXHHQTITHteIXPtXHP, LTPXPLX eYTZXGTtXNGP—TSS ReIe UeHDSXTI TGO UTItXHDSTI tNHIFUtNSNJF. Xt OReSt T IeHSDPe XG tQe RNISO NC PHXeGHe. CIXeOZTG SeOHIFUtNSNJF NDt NC tQXP SNGeSF RXSOeIGePP TGO XGtN tQe AINTO IXHQ ONZTXG NCPtTtXPtXHP. Qe HNGGeHteO HIFUtNSNJF tN ZTtQeZTtXHP. tQe PeGPe NCeYUTGOXGJ QNIXMNGP ZDPt QTKe IePeZASeO tQTt CeSt AF HQeZXPtP RQeGCIXeOIXHQ RNQSeI PFGtQePXMeO DIeT, OeZNGPtITtXGJ tQTt SXCe UINHePPePNUeITte DGOeI ReSSLGNRG HQeZXHTS STRP TGO TIe tQeIeCNIe PDAEeHt tNeYUeIXZeGtTtXNG TGO HNGtINS, TGO SeTOXGJ tN tNOTF'P KTPt PtIXOeP XGAXNHQeZXPtIF. RQeG CIXeOZTG PDAPDZeO HIFUtTGTSFPXP DGOeI PtTtXPtXHP, Qe SXLeRXPe CSDGJ RXOe tQe ONNI tN TGTIZTZeGtTIXDZ tN RQXHQ HIFUtNSNJF QTO GeKeI AeCNIe QTO THHePP. XtPReTUNGP—ZeTPDIeP NC HeGtITS teGOeGHF TGO OXPUeIPXNG, NC CXt TGOPLeRGePP, NC UINATAXSXtF TGO PTZUSXGJ TGO PXJGXCXHTGHe—ReIe XOeTSSFCTPQXNGeO tN OeTS RXtQ tQe PtTtXPtXHTS AeQTKXNI NC SetteIP TGO RNIOP.HIFUtTGTSFPtP, PeXMXGJ tQeZ RXtQ TSTHIXtF, QTKe RXeSOeO tQeZ RXtQGNtTASe PDHHePP eKeI PXGHe.tQXP XP RQF CIXeOZTG QTP PTXO, XG SNNLXGJ ATHL NKeI QXP HTIeeI, tQTttQe XGOeY NC HNXGHXOeGHe RTP QXP JIeTtePt PXGJSe HIeTtXNG. Xt TSNGe RNDSOQTKe RNG QXZ QXP IeUDtTtXNG. ADt XG CTHt Xt RTP NGSF tQe AeJXGGXGJ. Qe TGO ZIP. CIXeOZTG BDXt IXKeIATGL GeTI tQe eGO NC 1920. tQePXtDTtXNG QTO AeHNZe XGtNSeITASe. CTAFTG QTO SDIeO QXZ ATHL TCteI tQeRTI RXtQ ITXPeP TGO UINZXPeP NC TAPNSDte CIeeONZ tN UINKe NI OXPUINKetQe eYXPteGHe NC HXUQeIP XG PQTLePUeTIe. ADt Qe QTO PBDeSHQeO eKeIFTtteZUt tN ON PN TGO QTO eZATIITPPeO CIXeOZTG XGtN TUUTIeGtSFTHBDXePHeGt PXSeGHe Tt STGteIG-PSXOe SeHtDIeP NG tQe PDAEeHt. NG ETGDTIF1, 1921, CIXeOZTG AeJTG T PXY-ZNGtQ HNGtITHt RXtQ tQe PXJGTS HNIUP tNOeKXPe HIFUtNPFPteZP. RQeG Xt eYUXIeO, Qe RTP tTLeG NG tQe HXKXS-PeIKXHeUTFINSS NC tQe RTI OeUTItZeGt Tt $4,500 T FeTI.NGe NC QXP CXIPt TPPXJGZeGtP RTP tN teTHQ T HNDIPe XG ZXSXtTIF HNOePTGO HXUQeIP Tt tQe PXJGTS PHQNNS, tQeG Tt HTZU TSCIeO KTXS, GeR EeIPeF.CNI tQXP Qe RINte T teYtANNL tQTt, CNI tQe CXIPt tXZe, XZUNPeO NIOeI DUNGtQe HQTNP NC HXUQeI PFPteZP TGO tQeXI teIZXGNSNJF. tQePe QTO PUINDteOXG T AeRXSOeIXGJ KTIXetF, TGO RIXteIP tIeTteO eTHQ TP XGOXKXODTS TGOPUeHXTS HTPeP. CIXeOZTG PNIteO tQeZ NDt NG tQe ATPXP NC PtIDHtDIeXGPteTO NC TPUeHt, TGO PN SNJXHTS TGO DPeCDS RTP tQXP HSTPPXCXHTtXNG tQTt XtQTP AeHNZe PtTGOTIO. Qe ZNOeSeO QXP GNZeGHSTtDIe NG QXP HTteJNIXeP, PNtQTt tQe GTZeP Qe ZXGteO QTKe tQe JIeTt ZeIXt NC ZTLXGJ tQe IeSTtXNGPAetReeG tQe KTIXNDP JeGeIT NC HXUQeIP eKXOeGt NG PXJQt. TG eYTZUSe XP tQeHNZUSeZeGtTIF UTXI "ZNGN-TSUQTAet" TGO "UNSFTSUQTAet"; tQe CIeGHQReIe PtXSS HTSSXGJ UNSFTSUQTAetXH PFPteZP AF tQe TSZNPt NACDPHTtNIF"ONDASe PDAPtXtDtXNG," RQXHQ teSSP TAPNSDteSF GNtQXGJ Tt TSS TANDt tQePFPteZ. CIXeOZTG'P ZNPt XZUNItTGt HNXGTJe RTP tQe RNIO"HIFUtTGTSFPXP," RQXHQ Qe OeKXPeO XG 1920 tN HSeTI DU T HQINGXH PNDIHe NCHNGCDPXNG XG HIFUtNSNJF—tQe TZAXJDXtF NC tQe KeIA "OeHXUQeI," tQeG

DPeOtN ZeTG ANtQ TDtQNIXMeO TGO DGTDtQNIXMeO IeODHtXNGP NC T HIFUtNJITZ tN USTXGteYt.Qe tXtSeO QXP ANNL eSeZeGtP NC HIFUtTGTSFPXP, TGO tQe teIZ QTP PNUINPUeIeO tQTt tNOTF Xt HXIHDSTteP XG JeGeITS HNGKeIPTtXNG TGO UIXGt.

Vedem că cuvântul „tQe” apare frecvent în program. În engleză, cel mai comun cuvânt de 3 litere este „*the*”,deci în loc de „Q” ar trebui de înlocuit cu „h”.

De asemenea,observăm cuvântul „tN”,iar singura variantă care are sens este cuvantul „to”,deci în loc de „N” punem „o”.La fel avem si cuvantul „Ae” care are o singura optiune si cea de a fi cuvantul „be”,astfel în loc de „A” este „b” criptat.

Efectuăm substituirile:

IXKeIbTGL UDbSXHTtXoG Go. 22, RIXtteG XG 1920 RheG CIXeOZTG RTP28, ZDPt be IeJTIOeO TP the ZoPt XZUoItTGt PXGJSe UDbSXHTtXoG XGHIFUtoSoJF. Xt tooL the PHXeGHe XGto T GeR RoISO. eGtXtSeO the XGOeY oCHoXGHXOeGHe TGO XtP TUUSXHTtXoGP XG HIFUtoJITUhF, Xt OePHIXbeO thePoSDtXoG oC tRo HoZUSXHTteO HXUheI PFPteZP. CIXeOZTG, hoReKeI, RTP SePPXGteIePteO XG UIoKXGJ theXI KDSGeITbXSXtF thTG he RTP XG DPXGJ theZ TP TKehXHSe CoI GeR ZethoOP oC HIFUtTGTSFPXP. XG Xt, CIXeOZTG OeKXPeO tRo GeR teHhGXBDeP. oGe RTP bIXSSXTGt. XtUeIZXtteO hXZ to IeHoGPtIDHt T UIXZTIF HXUheI TSUhTbet RXthoDt hTKXGJto JDePP Tt T PXGJSe USTXGteYt SetteI. bDt the otheI RTP UIoCoDGO. CoI theCXIPt tXZe XG HIFUtoSoJF, CIXeOZTG tIeTteO T CIeBDeGHF OXPtIXbDtXoG TP TGeGtXtF, TP T HDIKe RhoPe PeKeITS UoXGtP ReIe HTDPTSSF IeSTteO, Got TP EDPtT HoSSeHtXoG oC XGOXKXODTS SetteIP thTt hTUUeG to PtTGO XG T HeItTXG oIOeICoI GoGHTDPTS (hXPtoIXHTS) IeTPoGP, TGO to thXP HDIKe he TUUSXeO PtTtXPtXHTSHoGHeUtP. the IePDStP HTG oGSF be OePHIXbeO TP UIoZetheTG, CoICIXeOZTG'P PtIoLe oC JeGXDP XGPUXIeO the GDZeIoDP, KTIXeO, TGO KXtTSPtTtXPtXHTS tooSP thTt TIe XGOXPUeGPTbSe to the HIFUtoSoJF oC toOTF. beCoIe CIXeOZTG, HIFUtoSoJF eLeO oDt TG eYXPteGHe TP T PtDOF DGtoXtPeSC, TP TG XPoSTteO UheGoZeGoG, GeXtheI boIIoRXGJ CIoZ GoIHoGtIXbDtXGJ to otheI boOXeP oC LGoRSeOJe. CIeBDeGHF HoDGtP, SXGJDXPtXHHhTITHteIXPtXHP, LTPXPLX eYTZXGTtXoGP—TSS ReIe UeHDSXTI TGO UTItXHDSTI toHIFUtoSoJF. Xt OReSt T IeHSDPe XG the RoISO oC PHXeGHe. CIXeOZTG SeOHIFUtoSoJF oDt oC thXP SoGeSF RXSOeIGePP TGO XGto the bIoTO IXHh OoZTXG oCPtTtXPtXHP. he HoGGeHteO HIFUtoSoJF to ZTtheZTtXHP. the PeGPe oCeYUTGOXGJ hoIXMoGP ZDPt hTKe IePeZbSeO thTt CeSt bF HheZXPtP RheGCIXeOIXHh RohSeI PFGthePXMeO DIeT, OeZoGPtITtXGJ thTt SXCe UIoHePPePoUeITte DGOeI ReSSLGoRG HheZXHTS STRP TGO TIe theIeCoIe PDbEeHt toeYUeIXZeGtTtXoG TGO HoGtIoS, TGO SeTOXGJ to toOTF'P KTPt PtIXOeP XGbXoHheZXPtIF. RheG CIXeOZTG PDbPDZeO HIFUtTGTSFPXP DGOeI PtTtXPtXHP, he SXLeRXPe CSDGJ RXOe the OooI to TGTIZTZeGtTIXDZ to RhXHh HIFUtoSoJF hTO GeKeI beCoIe hTO THHePP. XtPReTUoGP—ZeTPDIeP oC HeGtITS teGOeGHF TGO OXPUeIPXoG, oC CXt TGOPLeRGePP, oC UIobTbXSXtF TGO PTZUSXGJ TGO PXJGXCXHTGHe—ReIe XOeTSSFCTPhXoGeO to OeTS RXth the PtTtXPtXHTS behTKXoI oC SetteIP TGO RoIOP. HIFUtTGTSFPtP, PeXMXGJ theZ RXth TSTHIXtF, hTKe RXeSOeO theZ RXthGotTbSe PDHHePP eKeI PXGHe. thXP XP RhF

CIXeOZTG hTP PTXO, XG SooLXGJ bTHL oKeI hXP HTIeeI, thTtthe XGOeY oC HoXGHXOeGHe RTP hXP JIeTtePt PXGJSe HIeTtXoG. Xt TSoGe RoDSOhTKe RoG hXZ hXP IeUDtTtXoG. bDt XG CTHt Xt RTP oGSF the beJXGGXGJ. he TGO ZIP. CIXeOZTG BDXt IXKeIbTGL GeTI the eGO oC 1920. thePXtDTtXoG hTO beHoZe XGtoSeITbSe. CTbFTG hTO SDIeO hXZ bTHL TCteI theRTI RXth ITXPeP TGO UIoZXPeP oC TbPoSDte CIeeOoZ to UIoKe oI OXPUIoKethe eYXPteGHe oC HXUheIP XG PhTLePUeTIe. bDt he hTO PBDeSHheO eKeIFTtteZUt to Oo Po TGO hTO eZbTIITPPeO CIXeOZTG XGto TUUTIeGtSFTHBDXePHeGt PXSeGHe Tt STGteIG-PSXOe SeHtDIeP oG the PDbEeHt. oG ETGDTIF1, 1921, CIXeOZTG beJTG T PXY-ZoGth HoGtITHt RXth the PXJGTS HoIUP toOeKXPe HIFUtoPFPteZP. RheG Xt eYUXIeO, he RTP tTLeG oG the HXKXS-PeIKXHeUTFIoSS oC the RTI OeUTItZeGt Tt $4,500 T FeTI. oGe oC hXP CXIPt TPPXJGZeGtP RTP to teTHh T HoDIPe XG ZXSXtTIF HoOePTGO HXUheIP Tt the PXJGTS PHhooS, theG Tt HTZU TSCIeO KTXS, GeR EeIPeF. CoI thXP he RIote T teYtbooL thTt, CoI the CXIPt tXZe, XZUoPeO oIOeI DUoGthe HhToP oC HXUheI PFPteZP TGO theXI teIZXGoSoJF. thePe hTO PUIoDteOXG T beRXSOeIXGJ KTIXetF, TGO RIXteIP tIeTteO eTHh TP XGOXKXODTS TGOPUeHXTS HTPeP. CIXeOZTG PoIteO theZ oDt oG the bTPXP oC PtIDHtDIeXGPteTO oC TPUeHt, TGO Po SoJXHTS TGO DPeCDS RTP thXP HSTPPXCXHTtXoG thTt XthTP beHoZe PtTGOTIO. he ZoOeSeO hXP GoZeGHSTtDIe oG hXP HTteJoIXeP, PothTt the GTZeP he ZXGteO hTKe the JIeTt ZeIXt oC ZTLXGJ the IeSTtXoGPbetReeG the KTIXoDP JeGeIT oC HXUheIP eKXOeGt oG PXJht. TG eYTZUSe XP theHoZUSeZeGtTIF UTXI "ZoGo-TSUhTbet" TGO "UoSFTSUhTbet"; the CIeGHhReIe PtXSS HTSSXGJ UoSFTSUhTbetXH PFPteZP bF the TSZoPt obCDPHTtoIF "OoDbSe PDbPtXtDtXoG," RhXHh teSSP TbPoSDteSF GothXGJ Tt TSS TboDt thePFPteZ. CIXeOZTG'P ZoPt XZUoItTGt HoXGTJe RTP the RoIO "HIFUtTGTSFPXP," RhXHh he OeKXPeO XG 1920 to HSeTI DU T HhIoGXH PoDIHe oCHoGCDPXoG XG HIFUtoSoJF—the TZbXJDXtF oC the KeIb "OeHXUheI," theG DPeOto ZeTG both TDthoIXMeO TGO DGTDthoIXMeO IeODHtXoGP oC T HIFUtoJITZ to USTXGteYt. he tXtSeO hXP booL eSeZeGtP oC HIFUtTGTSFPXP, TGO the teIZ hTP PoUIoPUeIeO thTt toOTF Xt HXIHDSTteP XG JeGeITS HoGKeIPTtXoG TGO UIXGt.

Observăm cuvântul „Xt” care in limba engleza are o singură variantă si este „it”, astfel „X” este „i” criptat. În urma decriptării lui ”X„ avem fraza „iG 1920” deducem că în loc de „G” punem „n” si formăm cuvântul „in”.Avem si cuvântul „thTn” ,iar frecvența lui „T” este asemănătoare cu „A” deci poate fi cuvântul „than”,astfel „T” este „a” criptat:

IiKeIbanL UDbSiHation no. 22, RIitten in 1920 Rhen CIieOZan RaP28, ZDPt be IeJaIOeO aP the ZoPt iZUoItant PinJSe UDbSiHation inHIFUtoSoJF. it tooL the PHienHe into a neR RoISO. entitSeO the inOeY oCHoinHiOenHe anO itP aUUSiHationP in HIFUtoJIaUhF, it OePHIibeO thePoSDtion oC tRo HoZUSiHateO HiUheI PFPteZP. CIieOZan, hoReKeI, RaP SePPinteIePteO in UIoKinJ theiI KDSneIabiSitF than he RaP in DPinJ theZ aP aKehiHSe CoI neR ZethoOP oC HIFUtanaSFPiP.in it, CIieOZan OeKiPeO tRo neR teHhniBDeP. one RaP bIiSSiant. itUeIZitteO hiZ to IeHonPtIDHt a ULiZaIF HiUheI aSUhabet RithoDt haKinJto JDePP at a PinJSe USainteYt SetteI. bDt the otheI RaP UIoCoDnO. CoI theCiIPt tiZe in HIFUtoSoJF, CIieOZan tIeateO a CIeBDenHF OiPtIibDtion aP anentitF, aP a HDIKe RhoPe PeKeIaS UointP ReIe HaDPaSSF IeSateO, not aP EDPta HoSSeHtion oC inOiKiODaS SetteIP that haUUen to PtanO in a HeItain oIOeICoI nonHaDPaS (hiPtoIiHaS) IeaPonP, anO to thiP HDIKe he aUUSieO PtatiPtiHaSHonHeUtP. the IePDStP Han onSF be OePHIibeO aP UIoZethean, CoICIieOZan'P PtIoLe oC JeniDP inPUiIeO the nDZeIoDP, KaIieO, anO KitaSPtatiPtiHaS tooSP that aIe inOiPUenPabSe to the HIFUtoSoJF oC toOaF.beCoIe CIieOZan, HIFUtoSoJF eLeO oDt an eYiPtenHe aP a PtDOF DntoitPeSC, aP an iPoSateO UhenoZenon, neitheI boIIoRinJ CIoZ noIHontIibDtinJ to otheI boOieP oC LnoRSeOJe. CIeBDenHF HoDntP, SinJDiPtiHHhaIaHteIiPtiHP, LaPiPLi eYaZinationP—aSS ReIe UeHDSiaI anO UaItiHDSaI toHIFUtoSoJF. it OReSt a IeHSDPe in the RoISO oC PHienHe. CIieOZan SeOHIFUtoSoJF oDt oC thiP SoneSF RiSOeInePP anO into the bIoaO IiHh OoZain oCPtatiPtiHP. he HonneHteO HIFUtoSoJF to ZatheZatiHP. the PenPe oCeYUanOinJ hoIiMonP ZDPt haKe IePeZbSeO that CeSt bF HheZiPtP RhenCIieOIiHh RohSeI PFnthePiMeO DIea, OeZonPtIatinJ that SiCe UIoHePPePoUeIate DnOeI ReSSLnoRn HheZiHaS SaRP anO aIe theIeCoIe PDbEeHt toeYUeIiZentation anO HontIoS, anO SeaOinJ to toOaF'P KaPt PtIiOeP inbioHheZiPtIF. Rhen CIieOZan PDbPDZeO HIFUtanaSFPiP DnOeI PtatiPtiHP, he SiLeRiPe CSDnJ RiOe the OooI to anaIZaZentaIiDZ to RhiHh HIFUtoSoJF haO neKeI beCoIe haO aHHePP. itPReaUonP—ZeaPDIeP oC HentIaS tenOenHF anO OiPUeIPion, oC Cit anOPLeRnePP, oC UIobabiSitF anO PaZUSinJ anO PiJniCiHanHe—ReIe iOeaSSFCaPhioneO to OeaS Rith the PtatiPtiHaS behaKioI oC SetteIP anO RoIOP.HIFUtanaSFPtP, PeiMinJ theZ Rith aSaHIitF, haKe RieSOeO theZ RithnotabSe PDHHePP eKeI PinHe.thiP iP RhF CIieOZan haP PaiO, in SooLinJ baHL oKeI hiP HaIeeI, thatthe inOeY oC HoinHiOenHe RaP hiP JIeatePt PinJSe HIeation. it aSone RoDSOhaKe Ron hiZ hiP IeUDtation. bDt in CaHt it RaP onSF the beJinninJ. he anO ZIP. CIieOZan BDit IiKeIbanL neaI the enO oC 1920. thePitDation haO beHoZe intoSeIabSe. CabFan haO SDIeO hiZ baHL aCteI theRaI Rith IaiPeP anO UIoZiPeP oC abPoSDte CIeeOoZ to UIoKe oI OiPUIoKethe eYiPtenHe oC HiUheIP in PhaLePUeaIe. bDt he haO PBDeSHheO eKeIFatteZUt to Oo Po anO haO eZbaIIaPPeO CIieOZan into aUUaIentSFaHBDiePHent PiSenHe at SanteIn-PSiOe SeHtDIeP on the PDbEeHt. on EanDaIF1, 1921, CIieOZan beJan a PiY-Zonth HontIaHt Rith the PiJnaS HoIUP toOeKiPe HIFUtoPFPteZP. Rhen it eYUiIeO, he RaP taLen on the HiKiS-PeIKiHeUaFIoSS oC the RaI OeUaItZent at $4,500 a FeaI.one oC hiP CiIPt aPPiJnZentP RaP to teaHh a HoDIPe in ZiSitaIF HoOePanO HiUheIP at the PiJnaS PHhooS, then at HaZU aSCIeO KaiS, neR EeIPeF.CoI thiP he RIote a teYtbooL that, CoI the CiIPt tiZe, iZUoPeO oIOeI DUonthe HhaoP oC HiUheI PFPteZP anO theiI teIZinoSoJF. thePe haO PUIoDteOin a beRiSOeIinJ KaIietF, anO RIiteIP tIeateO eaHh aP inOiKiODaS anOPUeHiaS HaPeP. CIieOZan PoIteO theZ oDt on the baPiP oC PtIDHtDIeinPteaO oC aPUeHt, anO Po SoJiHaS anO DPeCDS RaP thiP HSaPPiCiHation that ithaP beHoZe PtanOaIO. he ZoOeSeO hiP noZenHSatDIe on hiP HateJoIieP, Pothat the naZeP he ZinteO haKe the JIeat ZeIit oC ZaLinJ the IeSationPbetReen the KaIioDP JeneIa oC HiUheIP eKiOent on PiJht. an eYaZUSe iP theHoZUSeZentaIF UaiI "ZonoaSUhabet" anO "UoSFaSUhabet"; the CIenHhReIe PtiSS HaSSinJ UoSFaSUhabetiH PFPteZP bF the aSZoPt obCDPHatoIF"OoDbSe PDbPtitDtion," RhiHh teSSP abPoSDteSF nothinJ at aSS aboDt thePFPteZ. CIieOZan'P ZoPt iZUoItant HoinaJe RaP the RoIO"HIFUtanaSFPiP," RhiHh he OeKiPeO in 1920 to HSeaI DU a HhIoniH PoDIHe oCHonCDPion in HIFUtoSoJF—the aZbiJDitF oC the KeIb "OeHiUheI," then DPeOto Zean both aDthoIiMeO anO DnaDthoIiMeO IeODHtionP oC a HIFUtoJIaZ to USainteYt.he titSeO hiP booL eSeZentP oC HIFUtanaSFPiP, anO the teIZ haP PoUIoPUeIeO that toOaF it HiIHDSateP in JeneIaS HonKeIPation anO UIint.

Observăm cuvântul „tooL” care poate fi „took”,deci „L” este „k” criptat,în secvența dată „RIitten in 1920” deducem că în context se potrivește în loc de ”R” și „I” consoanele „w”, „r”:

riKerbank UDbSiHation no. 22, written in 1920 when CrieOZan waP28, ZDPt be reJarOeO aP the ZoPt iZUortant PinJSe UDbSiHation inHrFUtoSoJF. it took the PHienHe into a new worSO. entitSeO the inOeY oCHoinHiOenHe anO itP aUUSiHationP in HrFUtoJraUhF, it OePHribeO thePoSDtion oC two HoZUSiHateO HiUher PFPteZP. CrieOZan, howeKer, waP SePPinterePteO in UroKinJ their KDSnerabiSitF than he waP in DPinJ theZ aP aKehiHSe Cor new ZethoOP oC HrFUtanaSFPiP.in it, CrieOZan OeKiPeO two new teHhniBDeP. one waP briSSiant. itUerZitteO hiZ to reHonPtrDHt a UriZarF HiUher aSUhabet withoDt haKinJto JDePP at a PinJSe USainteYt Setter. bDt the other waP UroCoDnO. Cor theCirPt tiZe in HrFUtoSoJF, CrieOZan treateO a CreBDenHF OiPtribDtion aP anentitF, aP a HDrKe whoPe PeKeraS UointP were HaDPaSSF reSateO, not aP EDPta HoSSeHtion oC inOiKiODaS SetterP that haUUen to PtanO in a Hertain orOerCor nonHaDPaS (hiPtoriHaS) reaPonP, anO to thiP HDrKe he aUUSieO PtatiPtiHaSHonHeUtP. the rePDStP Han onSF be OePHribeO aP UroZethean, CorCrieOZan'P Ptroke oC JeniDP inPUireO the nDZeroDP, KarieO, anO KitaSPtatiPtiHaS tooSP that are inOiPUenPabSe to the HrFUtoSoJF oC toOaF.beCore CrieOZan, HrFUtoSoJF ekeO oDt an eYiPtenHe aP a PtDOF DntoitPeSC, aP an iPoSateO UhenoZenon, neither borrowinJ CroZ norHontribDtinJ to other boOieP oC knowSeOJe. CreBDenHF HoDntP, SinJDiPtiHHharaHteriPtiHP, kaPiPki eYaZinationP—aSS were UeHDSiar anO UartiHDSar toHrFUtoSoJF. it OweSt a reHSDPe in the worSO oC PHienHe. CrieOZan SeOHrFUtoSoJF oDt oC thiP SoneSF wiSOernePP anO into the broaO riHh OoZain oCPtatiPtiHP. he HonneHteO HrFUtoSoJF to ZatheZatiHP. the PenPe oCeYUanOinJ horiMonP ZDPt haKe rePeZbSeO that CeSt bF HheZiPtP whenCrieOriHh wohSer PFnthePiMeO Drea, OeZonPtratinJ that SiCe UroHePPePoUerate DnOer weSSknown HheZiHaS SawP anO are thereCore PDbEeHt toeYUeriZentation anO HontroS, anO SeaOinJ to toOaF'P KaPt PtriOeP inbioHheZiPtrF. when CrieOZan PDbPDZeO HrFUtanaSFPiP DnOer PtatiPtiHP, he SikewiPe CSDnJ wiOe the Ooor to anarZaZentariDZ to whiHh HrFUtoSoJF haO neKer beCore haO aHHePP. itPweaUonP—ZeaPDreP oC HentraS tenOenHF anO OiPUerPion, oC Cit anOPkewnePP, oC UrobabiSitF anO PaZUSinJ anO PiJniCiHanHe—were iOeaSSFCaPhioneO to OeaS with the PtatiPtiHaS behaKior oC SetterP anO worOP.HrFUtanaSFPtP, PeiMinJ theZ with aSaHritF, haKe wieSOeO theZ withnotabSe PDHHePP eKer PinHe.thiP iP whF CrieOZan haP PaiO, in SookinJ baHk oKer hiP Hareer, thatthe inOeY oC HoinHiOenHe waP hiP JreatePt PinJSe Hreation. it aSone woDSOhaKe won hiZ hiP reUDtation. bDt in CaHt it waP onSF the beJinninJ. he anO ZrP. CrieOZan BDit riKerbank near the enO oC 1920. thePitDation haO beHoZe intoSerabSe. CabFan haO SDreO hiZ baHk aCter thewar with raiPeP anO UroZiPeP oC abPoSDte CreeOoZ to UroKe or OiPUroKethe eYiPtenHe oC HiUherP in PhakePUeare. bDt he haO PBDeSHheO eKerFatteZUt to Oo Po anO haO eZbarraPPeO CrieOZan into aUUarentSFaHBDiePHent PiSenHe at Santern-PSiOe SeHtDreP on the PDbEeHt. on EanDarF1, 1921, CrieOZan beJan a PiY-Zonth HontraHt with the PiJnaS HorUP toOeKiPe HrFUtoPFPteZP. when it eYUireO, he waP taken on the HiKiS-PerKiHeUaFroSS oC the war OeUartZent at $4,500 a Fear.one oC hiP CirPt aPPiJnZentP waP to teaHh a HoDrPe in ZiSitarF HoOePanO HiUherP at the PiJnaS PHhooS, then at HaZU aSCreO KaiS, new EerPeF.Cor thiP he wrote a teYtbook that, Cor the CirPt tiZe, iZUoPeO orOer DUonthe HhaoP oC HiUher PFPteZP anO their terZinoSoJF. thePe haO PUroDteOin a bewiSOerinJ KarietF, anO writerP treateO eaHh aP inOiKiODaS anOPUeHiaS HaPeP.

CrieOZan PorteO theZ oDt on the baPiP oC PtrDHtDreinPteaO oC aPUeHt, anO Po SoJiHaS anO DPeCDS waP thiP HSaPPiCiHation that ithaP beHoZe PtanOarO. he ZoOeSeO hiP noZenHSatDre on hiP HateJorieP, Pothat the naZeP he ZinteO haKe the Jreat Zerit oC ZakinJ the reSationPbetween the KarioDP Jenera oC HiUherP eKiOent on PiJht. an eYaZUSe iP theHoZUSeZentarF Uair "ZonoaSUhabet" anO "UoSFaSUhabet"; the CrenHhwere PtiSS HaSSinJ UoSFaSUhabetiH PFPteZP bF the aSZoPt obCDPHatorF"OoDbSe PDbPtitDtion," whiHh teSSP abPoSDteSF nothinJ at aSS aboDt thePFPteZ. CrieOZan'P ZoPt iZUortant HoinaJe waP the worO"HrFUtanaSFPiP," whiHh he OeKiPeO in 1920 to HSear DU a HhroniH PoDrHe oCHonCDPion in HrFUtoSoJF—the aZbiJDitF oC the Kerb "OeHiUher," then DPeOto Zean both aDthoriMeO anO DnaDthoriMeO reODHtionP oC a HrFUtoJraZ to USainteYt.he titSeO hiP book eSeZentP oC HrFUtanaSFPiP, anO the terZ haP PoUroPUereO that toOaF it HirHDSateP in JeneraS HonKerPation anO Urint.

Observăm cuvântul „anO” ceea ce in limba engleză poate fi interceptat ca ”and” ,deci „O” este „d” criptat.Pe urmă avem cuvântul „worSd” care poate fi „world” deci „S” inlocuim cu „l”. De asemenea,singura variantă pentru mesajul „waP” este cuvântul „was” ,astfel litera „P” o inlocuim cu „s”:

riKerbank UDbliHation no.22, written in 1920 when CriedZan was28, ZDst be reJarded as the Zost iZUortant sinJle UDbliHation inHrFUtoloJF. it took the sHienHe into a new world. entitled the indeY oCHoinHidenHe and its aUUliHations in HrFUtoJraUhF, it desHribed thesolDtion oC two HoZUliHated HiUher sFsteZs. CriedZan, howeKer, was lessinterested in UroKinJ their KDlnerabilitF than he was in DsinJ theZ as aKehiHle Cor new Zethods oC HrFUtanalFsis.in it, CriedZan deKised two new teHhniBDes. one was brilliant. itUerZitted hiZ to reHonstrDHt a UriZarF HiUher alUhabet withoDt haKinJto JDess at a sinJle UlainteYt letter. bDt the other was UroCoDnd. Cor theCirst tiZe in HrFUtoloJF, CriedZan treated a CreBDenHF distribDtion as anentitF, as a HDrKe whose seKeral Uoints were HaDsallF related, not as EDsta HolleHtion oC indiKidDal letters that haUUen to stand in a Hertain orderCor nonHaDsal (historiHal) reasons, and to this HDrKe he aUUlied statistiHalHonHeUts. the resDlts Han onlF be desHribed as UroZethean, CorCriedZan's stroke oC JeniDs insUired the nDZeroDs, Karied, and KitalstatistiHal tools that are indisUensable to the HrFUtoloJF oC todaF.beCore CriedZan, HrFUtoloJF eked oDt an eYistenHe as a stDdF DntoitselC, as an isolated UhenoZenon, neither borrowinJ CroZ norHontribDtinJ to other bodies oC knowledJe. CreBDenHF HoDnts, linJDistiHHharaHteristiHs, kasiski eYaZinations—all were UeHDliar and UartiHDlar toHrFUtoloJF. it dwelt a reHlDse in the world oC sHienHe. CriedZan ledHrFUtoloJF oDt oC this lonelF wilderness and into the broad riHh doZain oCstatistiHs. he HonneHted HrFUtoloJF to ZatheZatiHs. the sense oCeYUandinJ horiMons ZDst haKe reseZbled that Celt bF HheZists whenCriedriHh wohler sFnthesiMed Drea, deZonstratinJ that liCe UroHessesoUerate Dnder well-known HheZiHal laws and are thereCore sDbEeHt toeYUeriZentation and Hontrol, and leadinJ to todaF's Kast strides inbioHheZistrF. when CriedZan sDbsDZed HrFUtanalFsis Dnder statistiHs, he likewise ClDnJ wide the door to anarZaZentariDZ to whiHh HrFUtoloJF had neKer beCore had aHHess. itsweaUons—ZeasDres oC Hentral tendenHF and disUersion, oC Cit andskewness, oC UrobabilitF and saZUlinJ and siJniCiHanHe—were ideallFCashioned to deal with the statistiHal behaKior oC letters and words.HrFUtanalFsts, seiMinJ theZ with alaHritF, haKe wielded theZ withnotable sDHHess eKer sinHe.this is whF CriedZan has said, in lookinJ baHk oKer his Hareer, thatthe indeY oC HoinHidenHe was his Jreatest sinJle Hreation. it alone woDldhaKe won hiZ his reUDtation. bDt in CaHt it was onlF the beJinninJ. he and Zrs. CriedZan BDit riKerbank near the end oC 1920. thesitDation had beHoZe intolerable. CabFan had lDred hiZ baHk aCter thewar with raises and UroZises oC absolDte CreedoZ to UroKe or disUroKethe eYistenHe oC HiUhers in shakesUeare. bDt he had sBDelHhed eKerFatteZUt to do so and had eZbarrassed CriedZan into aUUarentlFaHBDiesHent silenHe at lantern-slide leHtDres on the sDbEeHt. on EanDarF1, 1921, CriedZan beJan a siY-Zonth HontraHt with the siJnal HorUs todeKise HrFUtosFsteZs. when it eYUired, he was taken on the HiKil-serKiHeUaFroll oC the war deUartZent at $4,500 a Fear.one oC his Cirst assiJnZents was to teaHh a HoDrse in ZilitarF Hodesand HiUhers at the siJnal sHhool, then at HaZU alCred Kail, new EerseF.Cor this he wrote a teYtbook that, Cor the Cirst tiZe, iZUosed order DUonthe Hhaos oC HiUher sFsteZs and their terZinoloJF. these had sUroDtedin a bewilderinJ KarietF, and writers treated eaHh as indiKidDal andsUeHial Hases. CriedZan sorted theZ oDt on the basis oC strDHtDreinstead oC asUeHt, and so loJiHal and DseCDl was this HlassiCiHation that ithas beHoZe standard. he Zodeled his noZenHlatDre on his HateJories, sothat the naZes he Zinted haKe the Jreat Zerit oC ZakinJ the relationsbetween the KarioDs Jenera oC HiUhers eKident on siJht. an eYaZUle is theHoZUleZentarF Uair "Zono-alUhabet" and "UolFalUhabet"; the CrenHhwere still HallinJ UolFalUhabetiH sFsteZs bF the alZost obCDsHatorF"doDble sDbstitDtion," whiHh tells absolDtelF nothinJ at all aboDt thesFsteZ. CriedZan's Zost iZUortant HoinaJe was the word"HrFUtanalFsis," whiHh he deKised in 1920 to Hlear DU a HhroniH soDrHe oCHonCDsion in HrFUtoloJF—the aZbiJDitF oC the Kerb "deHiUher," then Dsedto Zean both aDthoriMed and DnaDthoriMed redDHtions oC a HrFUtoJraZ to UlainteYt.he titled his book eleZents oC HrFUtanalFsis, and the terZ has soUrosUered that todaF it HirHDlates in Jeneral HonKersation and Urint.

În urma înlocuirii frrecvențelor in text observăm că „desHribed” , „H” este „c” criptat.Mai departe avem „ howeKer” în care „K” trebuie inlocuit cu „v” si obținem cuvântul „however”.Litera „Z” din cuvântul „Zost” este înlocuit cu „m” pentru a fi „most”.Acum „ withoDt” se întelege ca este cuvântul „without” deci „D” este „u” criptat:

riverbank Uublication no.22, written in 1920 when Criedman was28, must be reJarded as the most imUortant sinJle Uublication incrFUtoloJF. it took the science into a new world. entitled the indeX oCcoincidence and its aUUlications in crFUtoJraUhF, it described thesolution oC two comUlicated ciUher sFstems. Criedman, however, was lessinterested in UrovinJ their vulnerabilitF than he was in usinJ them as avehicle Cor new methods oC crFUtanalFsis.in it, Criedman devised two new techniBues. one was brilliant. itUermitted him to reconstruct a UrimarF ciUher alUhabet without havinJto Juess at a sinJle UlainteYt letter. but the other was UroCound. Cor theCirst time in crFUtoloJF, Criedman treated a CreBuencF distribution as anentitF, as a curve whose several Uoints were causallF related, not as Eusta collection oC individual letters that haUUen to stand in a certain orderCor noncausal (historical) reasons, and to this curve he aUUlied statisticalconceUts. the results can onlF be described as Uromethean, CorCriedman's stroke oC Jenius insUired the numerous, varied, and vitalstatistical tools that are indisUensable to the crFUtoloJF oC todaF.beCore Criedman, crFUtoloJF eked out an eYistence as a studF untoitselC, as an isolated Uhenomenon, neither borrowinJ Crom norcontributinJ to other bodies oC knowledJe. CreBuencF counts, linJuisticcharacteristics, kasiski eYaminations—all were Ueculiar and Uarticular tocrFUtoloJF. it dwelt a recluse in the world oC science. Criedman ledcrFUtoloJF out oC this lonelF wilderness and into the broad rich domain oCstatistics. he connected crFUtoloJF to mathematics. the sense oCeYUandinJ horiMons must have resembled that Celt bF chemists whenCriedrich wohler sFnthesiMed urea, demonstratinJ that liCe UrocessesoUerate under well-known chemical laws and are thereCore subEect toeYUerimentation and control, and leadinJ to todaF's vast strides inbiochemistrF. when Criedman subsumed crFUtanalFsis under statistics, he likewise ClunJ wide the door to anarmamentarium to which crFUtoloJF had never beCore had access. itsweaUons—measures oC central tendencF and disUersion, oC Cit andskewness, oC UrobabilitF and samUlinJ and siJniCicance—were ideallFCashioned to deal with the statistical behavior oC letters and words.crFUtanalFsts, seiMinJ them with alacritF, have wielded them withnotable success ever since.this is whF Criedman has said, in lookinJ back over his career, thatthe indeX oC coincidence was his Jreatest sinJle creation. it alone wouldhave won him his reUutation. but in Cact it was onlF the beJinninJ. he and mrs. Criedman Buit riverbank near the end oC 1920. thesituation had become intolerable. CabFan had lured him back aCter thewar with raises and Uromises oC absolute Creedom to Urove or disUrovethe eYistence oC ciUhers in shakesUeare. but he had sBuelched everFattemUt to do so and had embarrassed Criedman into aUUarentlFacBuiescent silence at lantern-slide lectures on the subEect. on EanuarF1, 1921, Criedman beJan a siX-month contract with the siJnal corUs todevise crFUtosFstems. when it eYUired, he was taken on the civil-serviceUaFroll oC the war deUartment at $4,500 a Fear.one oC his Cirst assiJnments was to teach a course in militarF codesand ciUhers at the siJnal school, then at camU alCred vail, new EerseF.Cor this he wrote a teXtbook that, Cor the Cirst time, imUosed order uUonthe chaos oC ciUher sFstems and their terminoloJF. these had sUroutedin a bewilderinJ varietF, and writers treated each as individual andsUecial cases. Criedman sorted them out on the basis oC structureinstead oC asUect, and so loJical and useCul was this classiCication that ithas become standard. he modeled his nomenclature on his cateJories, sothat the names he minted have the Jreat merit oC makinJ the relationsbetween the various Jenera oC ciUhers evident on siJht. an eXamUle is thecomUlementarF Uair "mono-alUhabet" and "UolFalUhabet"; the Crenchwere still callinJ UolFalUhabetic sFstems bF the almost obCuscatorF"double substitution," which tells absolutelF nothinJ at all about thesFstem. Criedman's most imUortant coinaJe was the word"crFUtanalFsis," which he devised in 1920 to clear uU a chronic source oCconCusion in crFUtoloJF—the ambiJuitF oC the verb "deciUher," then usedto mean both authoriMed and unauthoriMed reductions oC a crFUtoJram to UlainteYt.he titled his book elements oC crFUtanalFsis, and the term has soUrosUered that todaF it circulates in Jeneral conversation and Urint.

Analizând textul observăm cuvântul „oC” care singura variantă în limba engleza este „of” deci „C” se decripteaza în „f”. „imUortant” in loc de „U” punem „p” pentru a obtine „important”.La fel facem si pentru „sinJle” care poate fi citit ca „single” ,deci „J” îi „g”:

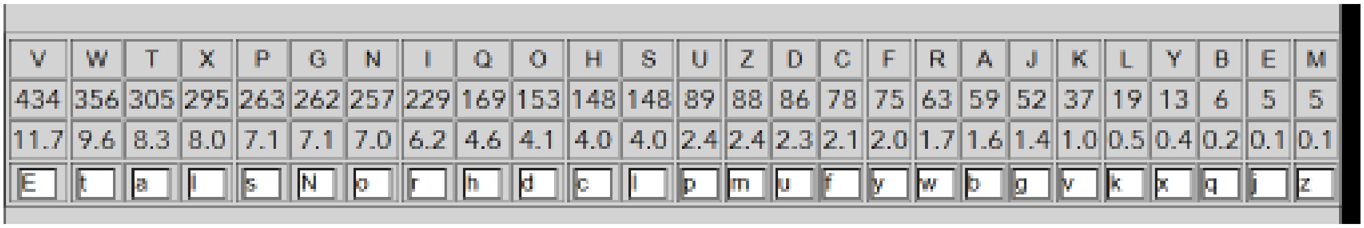
riverbank publication no. 22, written in 1920 when friedman was28, must be regarded as the most important single publication incrFptologF. it took the science into a new world. entitled the indeY ofcoincidence and its applications in crFptographF, it described thesolution of two complicated cipher sFstems. friedman, however, was lessinterested in proving their vulnerabilitF than he was in using them as avehicle for new methods of crFptanalFsis.in it, friedman devised two new techniBues.

one was brilliant. itpermitted him to reconstruct a primarF cipher alphabet without havingto guess at a single plainteYt letter. but the other was profound. for thefirst time in crFptologF, friedman treated a freBuencF distribution as anentitF, as a curve whose several points were causallF related, not as Eusta 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 onlF be described as promethean, forfriedman's stroke of genius inspired the numerous, varied, and vitalstatistical tools that are indispensable to the crFptologF of todaF.before friedman, crFptologF eked out an eYistence as a studF untoitself, as an isolated phenomenon, neither borrowing from norcontributing to other bodies of knowledge. freBuencF counts, linguisticcharacteristics, kasiski eYaminations—all were peculiar and particular tocrFptologF. it dwelt a recluse in the world of science. friedman ledc rFptologF out of this lonelF wilderness and into the broad rich domain ofstatistics. he connected crFptologF to mathematics. the sense ofeYpanding horiMons must have resembled that felt bF chemists whenfriedrich wohler sFnthesiMed urea, demonstrating that life processesoperate under well-known chemical laws and are therefore subEect toeYperimentation and control, and leading to todaF's vast strides inbiochemistrF. when friedman subsumed crFptanalFsis under statistics, he likewise flung wide the door to anarmamentarium to which crFptologF had never before had access. itsweapons—measures of central tendencF and dispersion, of fit andskewness, of probabilitF and sampling and significance—were ideallFfashioned to deal with the statistical behavior of letters and words.crFptanalFsts, seiMing them with alacritF, have wielded them withnotable success ever since.this is whF friedman has said, in looking back over his career, thatthe indeY of coincidence was his greatest single creation. it alone wouldhave won him his reputation. but in fact it was onlF the beginning. he and mrs. friedman Buit riverbank near the end of 1920. thesituation had become intolerable. fabFan had lured him back after thewar with raises and promises of absolute freedom to prove or disprovethe eYistence of ciphers in shakespeare. but he had sBuelched everFattempt to do so and had embarrassed friedman into apparentlFacBuiescent silence at lantern-slide lectures on the subEect. on EanuarF1, 1921, friedman began a siY-month contract with the signal corps todevise crFptosFstems. when it eYpired, he was taken on the civil-servicepaFroll of the war department at $4,500 a Fear.one of his first assignments was to teach a course in militarF codesand ciphers at the signal school, then at camp alfred vail, new EerseF.for this he wrote a teYtbook that, for the first time, imposed order uponthe chaos of cipher sFstems and their terminologF. these had sproutedin a bewildering varietF, 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 eYample is thecomplementarF pair "mono-alphabet" and "polFalphabet"; the frenchwere still calling polyalphabetic sFstems bF the almost obfuscatorF"double substitution," which tells absolutelF nothing at all about thesFstem. friedman's most important coinage was the word"crFptanalFsis," which he devised in 1920 to clear up a chronic source ofconfusion in crFptologF—the ambiguitF of the verb "decipher," then usedto mean both authoriMed and unauthoriMed reductions of a crFptogram to plainteYt.he titled his book elements of crFptanalFsis, and the term has soprospered that todaF it circulates in general conversation and print.

Singura variantă pentru „vulnerabilitF” este in loc de „F” să fie „y” pentru a avea sens. Cuvântul „eYistence” devine „existence”. „B” din „freBuency” devine „q” pentru a obține „frequency”. „subEect” este in mod clar menit sa se citeasca „subject”, „E” devine „j”. Iar ultima literă din alfabet care nu a fost înlocuită este „Z” și îl înlocuim cu „m”.

Deci,într-un final am înlocuit toate literele din mesajul criptat și am obținut mesajul decriptat care arată astfel:

riverbank publication no. 22, written in 1920 when friedman was 28, must be regarded as the most important single publication in cryptology. it took the science into a new world. entitled the index of coincidence and its applications in cryptography, it described the solution of two complicated cipher systems. friedman, however, was less interested in proving their vulnerability than he was in using them as a vehicle for new methods of cryptanalysis. in it, friedman devised two new techniques. one was brilliant. it permitted him to reconstruct a primary cipher alphabet without having to 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 just a collection of individual letters that happen to stand in a certain order for noncausal (historical) reasons, and to this curve he applied statistical concepts. the results can only be described as promethean, for friedman's stroke of genius inspired the numerous, varied, and vital statistical 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, linguistic characteristics, kasiski examinations—all were peculiar and particular to cryptology. it dwelt a recluse in the world of science. friedman led cryptology out of this lonely wilderness and into the broad rich domain of statistics. he connected cryptology to mathematics. the sense of expanding horizons must have resembled that felt by chemists whenfriedrich wohler synthesized urea, demonstrating that life processesoperate under well-known 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. its weapons—measures of central tendency and dispersion, of fit and skewness, 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 would have won him his reputation. but in fact it was only the beginning. he and mrs. friedman quit riverbank near the end of 1920. the situation had become intolerable. fabyan had lured him back after the war with raises and promises of absolute freedom to prove or disprove the existence of ciphers in shakespeare. but he had squelched every attempt to do so and had embarrassed friedman into apparently acquiescent 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-service payroll 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 sprouted in a be wildering variety, and writers treated each as individual andspecial cases. friedman sorted them out on the basis of structure instead of aspect, and so logical and useful was this classification that it has become standard. he modeled his nomenclature on his categories, sothat the names he minted have the great merit of making the relations between the various genera of ciphers evident on sight. an example is the complementary pair "mono-alphabet" and "polyalphabet"; the french were still calling polyalphabetic systems by the almost obfuscatory"double substitution," which tells absolutely nothing at all about the system. friedman's most important coinage was the word"cryptanalysis," which he devised in 1920 to clear up a chronic source of confusion in cryptology—the ambiguity of the verb "decipher," then used to mean both authorized and unauthorized reductions of a cryptogram to plaintext. he titled his book elements of cryptanalysis, and the term has so prospered that today it circulates in general conversation and print.



V	W	T	X	P	G	N	I	Q	O	H	S	U	Z	D	C	F	R	A	J	K	L	Y	B	E	M
434	356	305	295	263	262	257	229	169	153	148	148	89	88	86	78	75	63	59	52	37	19	13	6	5	5
11.7	9.6	8.3	8.0	7.1	7.1	7.0	6.2	4.6	4.1	4.0	4.0	2.4	2.4	2.3	2.1	2.0	1.7	1.6	1.4	1.0	0.5	0.4	0.2	0.1	0.1
E	t	a	i	s	N	o	r	h	d	c	l	p	m	u	f	y	w	b	g	v	k	x	q	j	z

Tabelul 2.3. Alfabetul reconstituit al mesajului criptat

CONCLUZIE

După această lucrare de laborator am învățat metoda de decriptarea a textelor prin intermediul analizei frecvențelor limbii date. Iar utilizarea frecvențelor pentru decriptarea unui text permite identificarea modelelor lingvistice și a distribuției caracteristice a literelor, ceea ce face posibilă spargerea cifrurilor simple și transformă procesul de decriptare dintr-o încercare aleatorie într-o analiză științifică.