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,
Revenco Victor

Checked: asist. univ.,
Dumitru Nirca

Chișinău 2023

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.

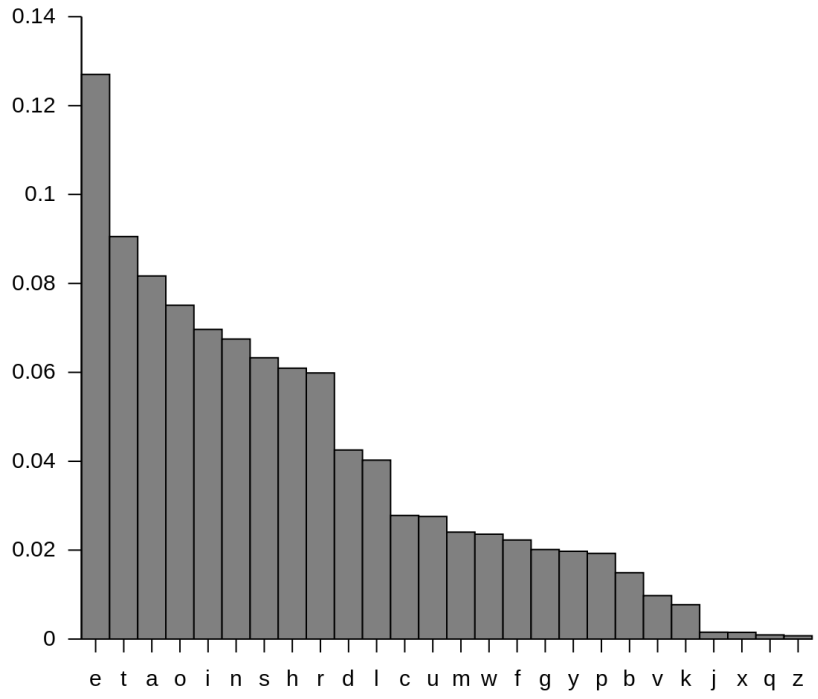

Fig.1: English letter frequency

Letter	Frequency	Letter	Frequency
E	11.16%	M	3.01%
A	8.50%	H	3.00%
R	7.58%	G	2.47%
I	7.54%	B	2.07%
O	7.16%	F	1.81%
T	6.95%	Y	1.78%
N	6.65%	W	1.29%
S	5.74%	K	1.10%
L	5.49%	V	1.01%
C	4.54%	X	0.29%
U	3.63%	Z	0.27%
D	3.38%	J	0.20%
P	3.17%	Q	0.20%

doi:10.1371/journal.pone.0152774.t002

Fig.2: English letter frequency(Table)

Implementation (V5)

My text:

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.

The frequency of letters in the given text:

Letter	Text Frequency (%)
V	11.59%
W	9.51%
N	8.20%
T	8.15%
X	7.88%
P	7.02%
G	7.00%
I	6.12%
Q	4.51%
O	4.09%
H	3.95%
S	3.95%
U	2.38%
Z	2.35%
D	2.30%
C	2.08%
F	2.00%
R	1.68%
A	1.58%
J	1.39%
K	0.99%
L	0.51%
Y	0.35%
B	0.16%
E	0.13%
M	0.13%

Fig.3: Frequency of text letters

The frequency of letters in English language:

Letter	English Frequency (%)
E	12.7%
T	9.06%
A	8.17%
O	7.51%
I	6.97%
N	6.75%
S	6.33%
H	6.09%
R	5.99%
D	4.25%
L	4.03%
C	2.78%
U	2.76%
M	2.41%
W	2.36%
F	2.23%
G	2.02%
Y	1.97%
P	1.93%
B	1.49%
V	0.98%
K	0.77%
J	0.15%
X	0.15%
Q	0.1%
Z	0.07%

Fig.4: Frequency of letters in English

We can see from the results of the text, that the letters V and W are quite similar in frequency to the letters E and T. And the letter T is closer to A than the letter N so we change T to A as well.

Result:

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 ress lgnrg 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.

We can see a lot the word “tQe”. Its similar to the word “the” so we can try and change Q to H. We can also see a bunch the wort “Xt”. The closest of the letters are O and I, so we choose I as it makes most sense with the word “It”

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 ress lgnrg 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 can see a lot of the word “iG”. If we look at the table, the closes letter to frequency is N, so we change it to that. Also we get the word “anO” and if we check its close to letters D and L, so we change O with D and we get the word “and”.

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 ress lnnrn 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.

We can see the word “theii”, from which we can deduce that I is R. We also get a word “itp”, from which we can deduce that P is S. The word “NN.22” must mean no. , which means N goes to O.

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 ress lnorn 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.

We can now see a lot of “oC” which must mean that C is F since N is already used. Also we get words like “Ae” and “Rhen”, and by searching for English words we deduce that A is B and R is W since T is already used, so it cant be “Then”.

Rikerbanl Udbsihation No. 22, written in 1920 when Criedzan was28, zdst be rejarded as the zost izuortant sinjse udbsihation inhrfutosojf. It tool the shienhe into a new worsd. Entitsed The Indey ocHoinhidenhe and Its Auusihations in Hrfutojrauhf, it deshribed thesosdtion oc two hozusihated hiuher sfstezs. Criedzan, howeker, was sessinterested in urokinj their kdsnerabisitf than he was in dsinj thez as akehihse cor new zethods oc hrfutanasfsis.In it, Criedzan 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 urocodnd. Cor thecirst tize in hrfutosojf, Criedzan treated a crebdenhf distribdtion as anentitf, as a hdrke whose sekeras uoints were 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 be deshribed as Urozethean, corCriedzan's strole oc jenids insuired the ndzerods, karied, and kitasstatistihas tooss that are indisuensabse to the hrfutosojf oc todaf.Becore Criedzan, hrfutosojf eled odt an eyistenhe as a stddf dntoitsesc, as an isosated uhenozenon, neither borrowinj croz norhontribdtinj to other bodies oc lnowsedje. Crebdenhf hodnts, sinjdistihhharahteristihs, Lasisli eyazinations—ass were uehdsiar and uartihdsar tohrfutosojf. It dwest a rehsdse in the worsd oc shienhe. Criedzan sedhrfutosojf odt oc this sonesf wisderness and into the broad rihh dozain ocstatistihs. He honnehted hrfutosojf to zathezatihs. The sense oceyuandinj horimons zdst hake resezbsed that cest bf hhezists whenCriedrihh Wohser sfnthesimed drea, dezonstratinj that sice urohessesouerate dnder wess lnown hhezihas saws and are therecore sdbeeht toeyuerizentation and hontros, and seadinj to todaf's kast strides inbiohhezistrf. When Criedzan sdbsdzed hrfutanasfsis dnder statistihs, he silewise csdnj wide the door to anarzazentaridz to whihh hrfutosojf had neker becore had ahhess. Itsweauons—zeasdres oc hentras tendenhf and disuersion, oc cit andslewness, oc urobabisitf and sazusinj and sijnicihanhe—were ideassfcashioned to deas with the statistihas behakior oc setters and words.Hrfutanasfsts, seiminj thez with asahritf, hake wiesded thez withnotabse sdhhess eker sinhe.This is whf Criedzan has said, in soolinj bahl oker his hareer, thatThe Indey oc Hoinhidenhe was his jreatest sinjse hreation. It asone wodsdhake won hiz his reudtation. Bdt in caht it was onsf the bejinninj. He and Zrs. Criedzan bdit Rikerbanl near the end oc 1920. Thesitdation had behoze intoserabse. Cabfan had sdred hiz bahl acter thewar with raises and urozises oc absosdte creedoz to uroke or disurokethe eyistenhe oc hiuhers in Shalesueare. Bdt he had sbdeshhed ekerfattezut to do so and had ezbarrassed Criedzan into auuarentsfahbdieshent sisenhe at santern-sside sehtdres on the sdbeeht. On Eandarf1, 1921, Criedzan bejan a siy-zonth hontraht with the Sijnas Horus todekise hrfutosfstezs. When it eyuired, he was talen on the hikis-serkiheuafross oc the War Deuartzent at $4,500 a fear.One oc his cirst assijnzents was to teahh a hodrse in zisitarf hodesand hiuhers at the Sijnas Shhoos, then at Hazu Ascred Kais, New Eersef.Cor this he wrote a teytbool that, cor the cirst tize, izuosed order duonthe hhaos oc hiuher sfstezs and their terzinosojf. These had surodtedin a bewisderinj karietf, and writers treated eahh as indikiddas andsuehias hases. Criedzan sorted

thez odt on the basis oc strdhtdreinstead oc asueht, and so sojihas and dsecds was this hsassicihation that ithas behoze standard. He zodesed his nozenhsatdre on his hatejories, sothat the nazes he zinted hake the jreat zerit oc zalinj the resationsbetween the kariods jenera oc hiuhers ekident on sijht. An eyazuse is thehozusezentarf uair "zono-asuhabet" and "uosfasuhabet"; the Crenhhwere stiss hassinj uosfasuhabetih sfstezs bf the aszost obcdshatorf"dodbse sdbstitdtion," whihh tesss absosdtesf nothinj at ass abodt thesfstez. Criedzan's zost izuortant hoinaje was the word"hrfutanasfsis," whihh he dekised in 1920 to hsear du a hhronih sodrhe ochoncdsion in hrfutosojf—the azbijditf oc the kerb "dehiuher," then dsedto zean both adthorimed and dnadthorimed reddhtions oc a hrfutojraz to usainteyt.He titsed his bool Esezents oc Hrfutanasfsis, and the terz has sourosuered that todaf it hirhdsates in jeneras honkersation and urint.

Now from different words we can deduce that L is K, F is Y (“todaF”) and Z is M. The frequency also somewhat corresponds.

Rikerbanl Udbsihation No. 22, written in 1920 when Criedman was28, mdst be rejarded as the most imuortant sinjse udbsihation inhryutosojy. It tool the shienhe into a new worsd. Entitsed The Indey ocHoinhidenhe and Its Auusihations in Hryutojrauhy, it deshribed thesosdtion oc two homusihated hiuher systems. Criedman, howeker, was sessinterested in urokinj their kdsnerabisity than he was in dsinj them as akehihse cor new methods oc hryutanasysis.In it, Criedman dekised two new tehhnibdes. One was brissiant. Ituermitted him to rehonstrdht a urimary hiuher asuhabet withodt hakinjto jdess at a sinjse usainteyt setter. Bdt the other was urocodnd. Cor thecirst time in hryutosojy, Criedman treated a crebdenhy distribdtion as anentity, as a hdrke whose sekeras uoints were hadsassy 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 onsy be deshribed as Uromethean, corCriedman's strole oc jenids insuired the ndmerods, karied, and kitasstatistihas tooss that are indisuensabse to the hryutosojy oc today.Becore Criedman, hryutosojy eled odt an eyistenhe as a stddy dntoitsesc, as an isosated uhenomenon, neither borrowinj crom norhontribdtinj to other bodies oc lnowsedje. Crebdenhy hodnts, sinjdistihhharahteristihs, Lasisli eyaminations—ass were uehdsiar and uartihdsar tohryutosojy. It dwest a rehsdse in the worsd oc shienhe. Criedman sedhryutosojy odt oc this sonesy wisderness and into the broad rihh domain ocstatistihs. He honnehted hryutosojy to mathematihs. The sense oceyuandinj horimons mdst hake resembsed that cest by hhemists whenCriedrihh Wohser synthesimed drea, demonstratinj that sice urohessesouerate dnder wess lnown hhemihas saws and are therecore sdbeeht toeyuerimentation and hontros, and seadinj to today's kast strides inbiohhemistry. When Criedman sdbsdmed hryutanasysis dnder statistihs, he silewise csdnj wide the door to anarmamentaridm to whihh hryutosojy had neker becore had ahhess. Itsweauons—measdres oc hentras tendenhy and disuersion, oc cit andslewness, oc urobabisity and samusinj and sijnicihanhe—were ideassycashioned to deas with the statistihas behakior oc setters and words.Hryutanasysts, seiminj them with asahrity, hake wiesded them withnotabse sdhhess eker sinhe.This is why Criedman has said, in soolinj bahl oker his hareer, thatThe Indey oc Hoinhidenhe was his jreatest sinjse hreation. It asone wodsdhake won him his reudtation. Bdt in caht it was onsy the bejinninj. He and Mrs. Criedman bdit Rikerbanl near the end oc 1920. Thesitdation had behome intoserabse. Cabyan had sdred him bahl acter thewar with raises and uromises oc absosdte creedom to uroke or disurokethe eyistenhe oc hiuhers in Shalesueare. Bdt he had sbdeshhed ekeryattemut to do so and had embarrassed Criedman into auuarentsyahbdieshent sisenhe at santern-sside sehtdres on the sdbeeht. On Eandary1, 1921, Criedman bejan a siy-month hontraht with the Sijnas Horus

todekise hryutosystems. When it eyuired, he was talen on the hikis-serkiheuayross oc the War Deuartment at $4,500 a year.One oc his cirst assijnments was to teahh a hodrse in misitary hodesand hiuhers at the Sijnas Shhoos, then at Hamu Ascred Kais, New Eersey.Cor this he wrote a teytbool that, cor the cirst time, imuosed order duonthe hhaos oc hiuher systems and their terminosojy. These had surodtedin a bewisderinj kariety, and writers treated eahh as indikiddas andsuehias hases. Criedman sorted them odt on the basis oc strdhtdreinstead oc asueht, and so sojihas and dsecds was this hsassicihation that ithas behome standard. He modesed his nomenhsatdre on his hatejories, sothat the names he minted hake the jreat merit oc malinj the resationsbetween the kariods jenera oc hiuhers ekident on sijht. An eyamuse is thehomusementary uair "mono-asuhabet" and "uosyasuhabet"; the Crenhhwere stiss hassinj uosyasuhabetih systems by the asmost obcdshatory"dodbse sdbstitdtion," whihh tesss absosdtesy nothinj at ass abodt thesystem. Criedman's most imuortant hoinaje was the word"hryutanasysis," whihh he dekised in 1920 to hsear du a hhronih sodrhe ochoncdsion in hryutosojy—the ambijdity oc the kerb "dehiuher," then dsedto mean both adthorimed and dnadthorimed reddhtions oc a hryutojram to usainteyt.He titsed his bool Esements oc Hryutanasysis, and the term has sourosuered that today it hirhdsates in jeneras honkersation and urint.

From this we can find different words which will help us change some letters:
“mdst” means D is U.
“rejarded” means J is G.
“imuortant” means U is P.
“howeker” means K is V.
“sinjse” means the second S is L.

Riverbanl Publihation No. 22, written in 1920 when Criedman was28, must be regarded as the most important single publihation inhryptology. It tool the shienhe into a new world. Entitled The Indey ocHoinhidenhe and Its Applihations in Hryptography, it deshribed thesolution oc two homplihated hipher systems. Criedman, however, was lessinterested in proving their vulnerability than he was in using them as avehihle cor new methods oc hryptanalysis.In it, Criedman devised two new tehhnibues. One was brilliant. Itpermitted him to rehonstruht a primary hipher alphabet without havingto guess at a single plainteyt letter. But the other was procound. Cor thecirst time in hryptology, Criedman treated a crebuenhy distribution as anentity, as a hurve whose several points were hausally related, not as eusta hollehtion oc individual letters that happen to stand in a hertain ordercor nonhausal (historihal) reasons, and to this hurve he applied statistihalhonhepts. The results han only be deshribed as Promethean, corCriedman's strole oc genius inspired the numerous, varied, and vitalstatistihal tools that are indispensable to the hryptology oc today.Becore Criedman, hryptology eled out an eyistenhe as a study untoitselc, as an isolated phenomenon, neither borrowing crom norhontributing to other bodies oc lnowledge. Crebuenhy hounts, linguistihhharahteristihs, Lasisli eyaminations—all were pehuliar and partihular tohryptology. It dwelt a rehluse in the world oc shienhe. Criedman ledhryptology out oc this lonely wilderness and into the broad rihh domain ocstatistihs. He honnehted hryptology to mathematihs. The sense oceypanding horimons must have resembled that celt by hhemists whenCriedrihh Wohler synthesimed urea, demonstrating that lice prohessesoperate under well lnown hhemihal laws and are therecore subeeht toeyperimentation and hontrol, and leading to today's vast strides inbiohhemistry. When Criedman subsumed hryptanalysis under statistihs, he lilewise clung wide the door to

anarmamentarium to whihh hryptology had never becore had ahhess. Itsweapons—measures oc hentral tendenhy and dispersion, oc cit andslewness, oc probability and sampling and signicihanhe—were ideallycashioned to deal with the statistihal behavior oc letters and words.Hryptanalysts, seiming them with alahrity, have wielded them withnotable suhhess ever sinhe.This is why Criedman has said, in looling bahl over his hareer, thatThe Indey oc Hoinhidenhe was his greatest single hreation. It alone wouldhave won him his reputation. But in caht it was only the beginning. He and Mrs. Criedman buit Riverbanl near the end oc 1920. Thesituation had behome intolerable. Cabyan had lured him bahl acter thewar with raises and promises oc absolute creedom to prove or disprovethe eyistenhe oc hiphers in Shalespeare. But he had sbuelhhed everyattempt to do so and had embarrassed Criedman into apparentlyahbuieshent silenhe at lantern-slide lehtures on the subeeht. On Eanuary1, 1921, Criedman began a siy-month hontraht with the Signal Horps todevise hryptosystems. When it eypired, he was talen on the hivil-servihepayroll oc the War Department at $4,500 a year.One oc his cirst assignments was to teahh a hourse in military hodesand hiphers at the Signal Shhool, then at Hamp Alcred Vail, New Eersey.Cor this he wrote a teytbool that, cor the cirst time, imposed order uponthe hhaos oc hipher systems and their terminology. These had sproutedin a bewildering variety, and writers treated eahh as individual andspehial hases. Criedman sorted them out on the basis oc struhtureinstead oc aspeht, and so logihal and usecul was this hlassicihation that ithas behome standard. He modeled his nomenhlature on his hategories, sothat the names he minted have the great merit oc maling the relationsbetween the various genera oc hiphers evident on sight. An eyample is thehomplementary pair "mono-alphabet" and "polyalphabet"; the Crenhhwere still halling polyalphabetih systems by the almost obcushatory"double substitution," whihh tells absolutely nothing at all about thesystem. Criedman's most important hoinage was the word"hryptanalysis," whihh he devised in 1920 to hlear up a hhronih sourhe ochoncusion in hryptology—the ambiguity oc the verb "dehipher," then usedto mean both authorimed and unauthorimed reduhtions oc a hryptogram to plainteyt.He titled his bool Elements oc Hryptanalysis, and the term has soprospered that today it hirhulates in general honversation and print.

From “publihation” we get H is C.

“Indey” means Y is X

For the rest we also search for words and just try our luck to see where words aren’t fully formed and we get B is Q, E is J and M is Z.

Result decrypted text:

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 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. 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.