MINISTERUL EDUCAȚIEI ȘI CERCETĂRII

AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică şi Microelectronică

Departamentul Inginerie Software și Automatică

Artur Țugui, FAF-231

Report

Laboratory Work No. 2

on Cryptography and Security

Checked by:

Maia Zaica, university assistant

ISA, FCIM, UTM

Chișinău – 2025

1. Theoretical Background

1.1. Noțiune de analiză a frecvenței apariției literelor

Punctul slab al sistemelor de criptare monoalfabetice constă în frecvența de apariție a caracterelor în text. Dacă un text criptat este suficient de lung și se cunoaște limba în care este scris textul clar, sistemul poate fi spart printr-un atac bazat pe frecvența apariției literelor într-o limbă (atacul prin analiza frecvenței). Această frecvență este o problemă studiată intens (nu neapărat în scopuri criptografice), iar în rezultat au fost construite diverse structuri de ordine relativ la frecvența apariției literelor în fiecare limbă europeană și în alte limbi.

De obicei, cu cât un text criptat este mai lung, cu atât frecvența literelor folosite se apropie de această ordonare generală. O comparare între cele două relații de ordine (cea a caracterelor din textul criptat și cea a literelor din alfabetul limbii curente) conduce la realizarea câtorva corespondențe (literă text clar – literă text criptat), ceea ce stabilește în mod univoc cheia de criptare.

Pentru limba română frecvența literelor (exprimată în procente) este prezentată în tabelul 1.

Tabela 1: Frecvența literelor limbii române

A	Ă	Â	B	C	D	E	F	G	H	I	Î	J
9.95	4.06	0.91	1.07	5.28	3.45	11.47	1.18	0.99	0.47	9.96	1.40	0.24

K	L	M	N	O	P	Q	R	S	Ș	T	Ț	U
0.11	4.48	3.10	6.47	4.07	3.18	0.00	6.82	4.40	1.55	6.04	1.00	6.20

V	W	X	Y	Z
1.23	0.03	0.11	0.07	0.71

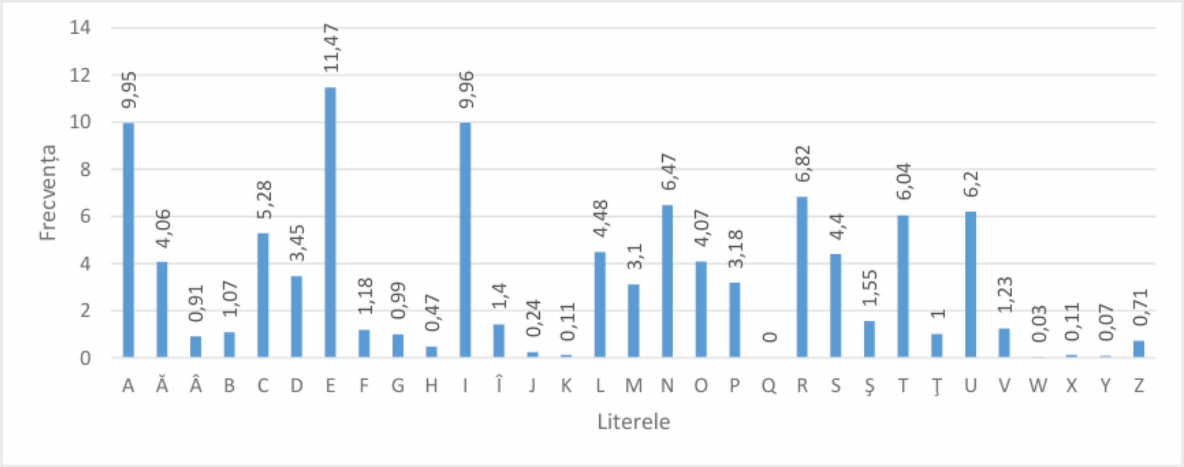


Figura 2.1. *Frecvenţa literelor limbii române*

Pentru limba engleză avem situația prezentată în tabelul 2:

Tabela 2: Frecvența literelor limbii engleze

A	B	C	D	E	F	G	H	I	J	K	L	M
8.17	1.49	2.78	4.25	12.7	2.23	2.01	6.09	6.97	0.15	0.77	4.03	2.41

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6.75	7.51	1.93	0.09	5.99	6.33	9.06	2.76	0.98	2.36	0.15	1.97	0.07

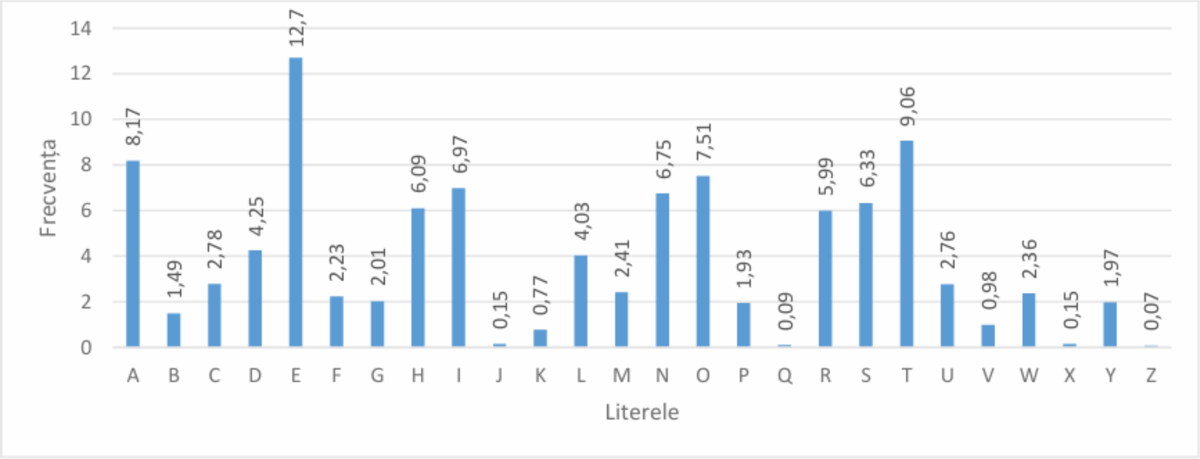


Figura 2.2. *Frecvenţa literelor limbii engleze*

1.2. Metodologia atacului prin analiza frecvențelor

Putem folosi informația despre frecvența de apariție a literelor într-o limbă pentru a încerca să spargem un cifru de substituție monoalfabetică. Acest lucru poate fi realizat deoarece, dacă spre exemplu pentru un mesaj scris în limba engleză litera ”E”, care are cea mai mare frecvență, a fost criptată cu ”X”, atunci fiecare ”X” din textul criptat era un ”E” în textul clar. Prin urmare, cea mai des întâlnită literă din textul cifrat ar trebui să fie ”X”.

Astfel, dacă interceptăm un mesaj criptat, iar litera cea mai frecventă în el este ”P”, putem presupune că ”P” a fost folosit pentru a cripta ”E”, și astfel putem înlocui toate ”P”-urile cu ”E”. Desigur, nu fiecare text are exact aceeași frecvență și, așa cum s-a văzut mai sus, ”T” și ”A” au și ele frecvențe înalte, așa că s-ar putea ca ”P” să fie unul dintre acestea. Cu toate acestea, este puțin probabil să fie ”Z”, care este rar întâlnit în limba engleză. Repetând acest proces cu următoarea cea mai frecventă literă, putem face progrese în spargerea unui mesaj.

Dacă ar fi să punem toate literele în ordine și să le înlocuim în conformitate cu tabelul frecvențelor, cel mai probabil că nu vom obține rezultatul așteptat. Criptanalistul trebuie să folosească alte ”trăsături de personalitate” ale literelor pentru a sparge criptograma. Aceasta poate include examinarea perechilor de litere (digrafele), cele mai frecvente fiind TH, HE, AN, IN, ER, ON, RE, ED, ND, HA, AT, EN. Tripletele de litere (trigrafele), la fel pot fi foarte utile, cele mai frecvente dintre ele în limba engleză fiind THE, AND, THA, ENT, ION, TIO, FOR, NDE, HAS, NCE, TIS, OFT, MEN. În plus, în limba engleză sunt doar câteva litere care apar ca duble (SS, EE, TT, OO și FF fiind cele mai frecvente). Există doar două cuvinte cu sens formate dintr-o singură literă în limba engleză: ”A” și ”I”.

Alte cuvinte frecvente încep să apară, de asemenea, pe măsură ce vom face unele înlocuiri. De exemplu, ”T*E” poate apărea frecvent după efectuarea substituțiilor pentru ”T” și ”E”. În acest caz ”T*E” este foarte probabil să fie ”THE”, un cuvânt foarte frecvent în engleză.

Procesul de analiză a frecvenței folosește diverse proprietăți subtile ale limbajului și, din acest motiv, este aproape imposibil ca un computer să facă toată munca. În mod inevitabil, elementul de aport uman este necesar în acest proces pentru a lua decizii fundamentate cu privire la literele care trebuie înlocuite.

2. Conditions of the Problems

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-analys`

Raportul va conține descrierea procesului de spargere, exact la fel cum a fost prezentat în compartimentul 2.3 din document.

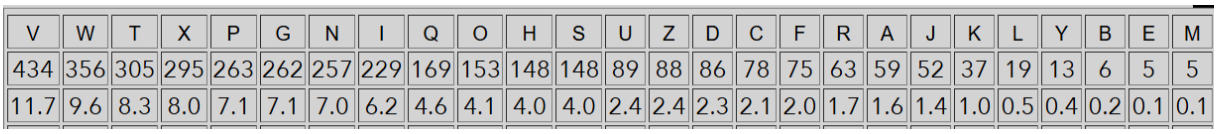
Fiecare student va lua varianta în conformitate cu numărul său de ordine din lista grupei.

2.1. Initial Ciphertext. Varianta 5

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.

3. Decrypting through frequency analysis

The result of the frequency analysis are shown below.



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

Figura 1: Frequency of letters in the text

To easily understand the numbers i plotted them in Java near the frequencies in English.

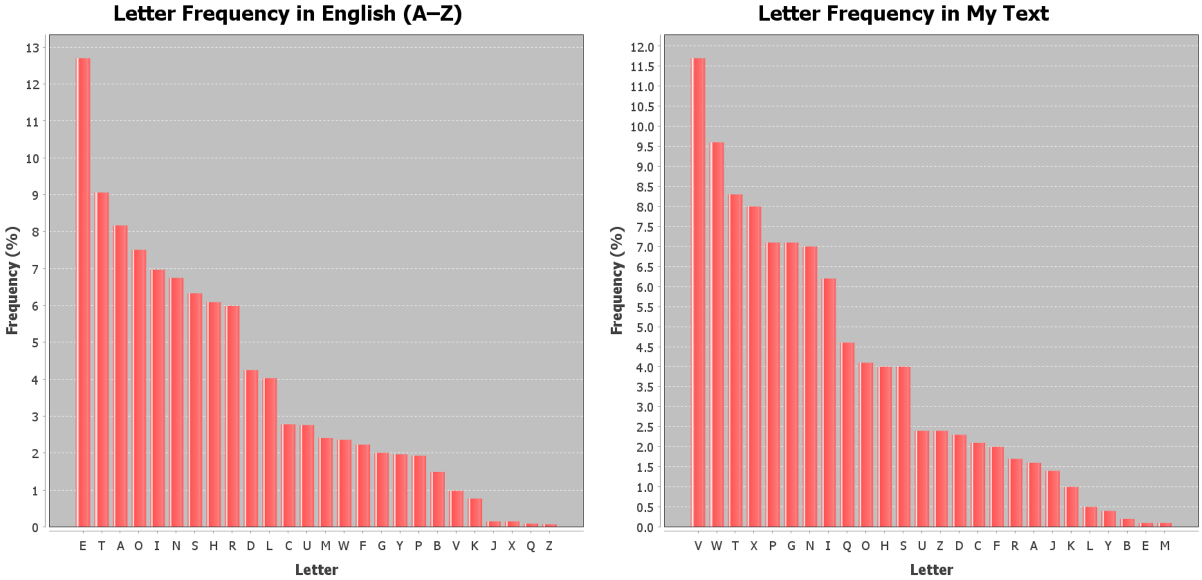


Figura 2: Frequency comparison

To better tell which letters were already replaced or not, I will convert eveything to uppercase.

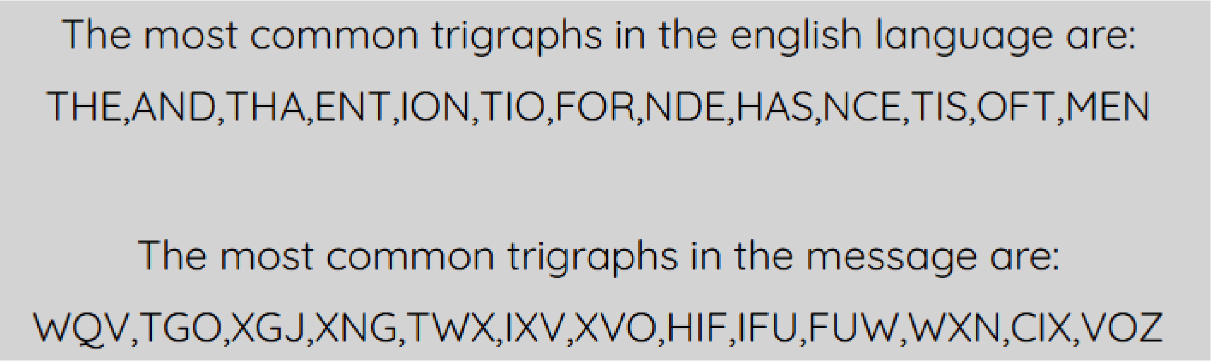
- $V \rightarrow e$: Since in English the frequency of E is significantly higher than the rest of letters and the frequency of V is the closest to E, let us substitue $V \rightarrow e$.

IXKeIATGL UDASXHTWXNG GN. 22, RIXWWeG XG 1920 RQeG CIXeOZTG RTP28, ZDPW Ae IeJTIOeO TP **WQe** ZNPW XZUNIWTGW PXGJSe UDASXHTWXNG XGHIFUWNSNJF. XW WNNL **WQe** PHXeGHe XGWN T GeR RNISO. eGWXWSeO **WQe** XGOeY NCHNXGHXOeGHe TGO XWP TUUSXHTWXNGP XG HIFUWNJITUQF, XW OePHIXAeO **WQe**PNSDWXNG NC WRN HNZUSXHTWeO HXUQeI PFPWeZP. CIXeOZTG, QNReKeI, RTP SePPXGWeIePWeO XG UINKXGJ

WQeXI KDSGeITAXSXWF WQTG Qe RTP XG DPXGJ **WQe**Z TP TKeQXHSe CNI GeR ZeWQNOP NC HIFUWTGTSFPXP.XG XW, CIXeOZTG OeKXPeO WRN GeR WeHQGXBDeP. NGe RTP AIXSSXTGW. XWUeIZXWWeO QXZ WN IeHNGPWIDHW T UIXZTIF HXUQeI TSUQTAeW RXWQNDW QTKXGJWN JDePP TW T PXGJSe USTXGWeYW SeWWeI. ADW **WQe** NWQeI RTP UINCNDGO. CNI **WQe**CXIPW WXZe XG HIFUWNSNJF, CIXeOZTG WIeTWeO T CIeBDeGHF OXPWIXADWXNG TP TGeGWXWF, TP T HDIKe RQNPe PeKeITS UNXGWP ReIe HTDPTSSF IeSTWeO, GNW TP EDPWT HNSSeHWXNG NC XGOXKXODTS SeWWeIP WQTW QTUUeG WN PWTGO XG T HeIWTXG NIOeICNI GNGHTDPTS (QXPWNIXHTS) IeTPNGP, TGO WN WQXP HDIKe Qe TUUSXeO PWTWXPWXHTSHNGHeUWP. **WQe** IePDSWP HTG NGSF Ae OePHIXAeO TP UINZe**WQe**TG, CNICIXeOZTG’P PWINLe NC JeGXDP XGPUXIeO **WQe** GDZeINDP, KTIXeO, TGO KXWTSPWTWXPWXHTS WNNSP WQTW TIe XGOXPUeGPTASe WN **WQe** HIFUWNSNJF NC WNOTF.AeCNIe CIXeOZTG, HIFUWNSNJF eLeO NDW TG eYXPWeGHe TP T PWDOF DGWNXWPeSC, TP TG XPNSTWeO UQeGNZeGNG, GeX**WQe**I ANIINRXGJ CINZ GNIHNGWIXADWXGJ WN N**WQe**I ANOXeP NC LGNRSeOJe. CIeBDeGHF HNDGWP, SXGJDXPWXHHQTITHWeIXPWXHP, LTPXPLX eYTZXGTWXNGP—TSS ReIe UeHDSXTI TGO UTIWXHDSTI WNHIFUWNSNJF. XW OReSW T IeHSDPe XG **WQe** RNISO NC PHXeGHe. CIXeOZTG SeOHIFUWNSNJF NDW NC **WQXP** SNGeSF RXSOeIGePP TGO XGWN **WQe** AINTO IXHQ ONZTXG NCPWTWXPWXHP. Qe HNGGeHWeO HIFUWNSNJF WN ZTWQeZTWXHP. **WQe** PeGPe NCeYUTGOXGJ QNIXMNGP ZDPW QTKe IePeZASeO WQTW CeSW AF HQeZXPWP RQeGCIXeOIXHQ RNQSeI PFG**WQe**PXMeO DIeT, OeZNGPWITWXGJ WQTW SXCe UINHePPePNUeITWe DGOeI ReSS LGNRG HQeZXHTS STRP TGO TIe **WQe**IeCNIe PDAEeHW WNeYUeIXZeGWTWXNG TGO HNGWINS, TGO SeTOXGJ WN WNOTF’P KTPW PWIXOeP XGAXNHQeZXPWIF. RQeG CIXeOZTG PDAPDZeO HIFUWTGTSFPXP DGOeI PWTWXPWXHP, Qe SXLeRXPe CSDGJ RXOe **WQe** ONNI WN TGTIZTZeGWTIXDZ WN RQXHQ HIFUWNSNJF QTO GeKeI AeCNIe QTO THHePP. XWPReTUNGP—ZeTPDIeP NC HeGWITS WeGOeGHF TGO OXPUeIPXNG, NC CXW TGOPLeRGePP, NC UINATAXSXWF TGO PTZUSXGJ TGO PXJGXCXHTGHe—ReIe XOeTSSFCTPQXNGeO WN OeTS RXWQ **WQe** PWTWXPWXHTS AeQTKXNI NC SeWWeIP TGO RNIOP.HIFUWTGTSFPWP, PeXMXGJ **WQe**Z RXWQ TSTHIXWF, QTKe RXeSOeO **WQe**Z RXWQGNWTASe PDHHePP eKeI PXGHe.**WQXP** XP RQF CIXeOZTG QTP PTXO, XG SNNLXGJ ATHL NKeI QXP HTIeeI, WQTW**WQe** XGOeY

NC HNXGHXOeGHe RTP QXP JIeTWePW PXGJSe HIeTWXNG. XW TSNGe RNDSOQTKe RNG QXZ QXP IeUDWTWXNG. ADW XG CTHW XW RTP NGSF **WQe** AeJXGGXGJ. Qe TGO ZIP. CIXeOZTG BDXW IXKeIATGL GeTI **WQe** eGO NC 1920. **WQe**PXWDTWXNG QTO AeHNZe XGWNSeITASe. CTAFTG QTO SDIeO QXZ ATHL TCWeI **WQe**RTI RXWQ ITXPeP TGO UINZXPeP NC TAPNSDWe CIeeONZ WN UINKe NI OXPUINKe**WQe** eYXPWeGHe NC HXUQeIP XG PQTLePUeTIe. ADW Qe QTO PBDeSHQeO eKeIFTWWeZUW WN ON PN TGO QTO eZATIITPPeO CIXeOZTG XGWN TUUTIeGWSFTHBDXePHeGW PXSeGHe TW STGWeIGPSXOe SeHWDIeP NG **WQe** PDAEeHW. NG ETGDTIF1, 1921, CIXeOZTG AeJTG T PXY-ZNGWQ HNGWITHW RXWQ **WQe** PXJGTS HNIUP WNOeKXPe HIFUWNPFPWeZP. RQeG XW eYUXIeO, Qe RTP WTLeG NG **WQe** HXKXS-PeIKXHeUTFINSS NC **WQe** RTI OeUTIWZeGW TW $4,500 T FeTI.NGe NC QXP CXIPW TPPXJGZeGWP RTP WN WeTHQ T HNDIPe XG ZXSXWTIF HNOePTGO HXUQeIP TW **WQe** PXJGTS PHQNNS, **WQe**G TW HTZU TSCIeO KTXS, GeR EeIPeF.CNI Qe RINWe T WeYWANNL WQTW, CNI **WQe** CXIPW WXZe, XZUNPeO NIOeI DUNG**WQe** HQTNP NC HXUQeI PFPWeZP TGO **WQe**XI WeIZXGNSNJF. **WQe**Pe QTO PUINDWeOXG T AeRXSOeIXGJ KTIXeWF, TGO RIXWeIP WIeTWeO eTHQ TP XGOXKXODTS TGOPUeHXTS HTPeP. CIXeOZTG PNIWeO **WQe**Z NDW NG **WQe** ATPXP NC PWIDHWDIeXGPWeTO NC TPUeHW, TGO PN SNJXHTS TGO DPeCDS RTP WQXP HSTPPXCXHTWXNG WQTW XWQTP AeHNZe PWTGOTIO. Qe ZNOeSeO QXP GNZeGHSTWDIe NG QXP HTWeJNIXeP, PNWQTW **WQe** GTZeP Qe ZXGWeO QTKe **WQe** JIeTW ZeIXW NC ZTLXGJ **WQe** IeSTWXNGPAeWReeG **WQe** KTIXNDP JeGeIT NC HXUQeIP eKXOeGW NG PXJQW. TG eYTZUSe XP **WQe**HNZUSeZeGWTIF UTXI ”ZNGN-TSUQTAeW” TGO ”UNSFTSUQTAeW”; **WQe** CIeGHQReIe PWXSS HTSSXGJ UNSFTSUQTAeWXH PFPWeZP AF **WQe** TSZNPW NACDPHTWNIF”ONDASe PDAPWXWDWXNG,” RQXHQ WeSSP TAPNSDWeSF GNWQXGJ TW TSS TANDW **WQe**PFPWeZ. CIXeOZTG’P ZNPW XZUNIWTGW HNXGTJe RTP **WQe** RNIO”HIFUWTGTSFPXP,” RQXHQ Qe OeKXPeO XG 1920 WN HSeTI DU T HQINGXH PNDIHe NCHNGCDPXNG XG HIFUWNSNJF—**WQe** TZAXJDXWF NC **WQe** KeIA ”OeHXUQeI,” **WQe**G DPeOWN ZeTG ANWQ TDWQNIXMeO TGO DGTDWQNIXMeO IeODHWXNGP NC T HIFUWNJITZ WN USTXGWeYW.Qe WXWSeO QXP ANNL eSeZeGWP NC HIFUWTGTSFPXP, TGO **WQe** WeIZ QTP PNUINPUeIeO WQTW WNOTF XW HXIHDSTWeP XG JeGeITS HNGKeIPTWXNG TGO UIXGW.

- $W \to t$, $Q \to h$, $WQV \to THE$: The trigraphs WQV and IXV are the 1st and the 6th most common that end with V (E). Since THE is the most common trigraph in English, WQV is a word in our text, and T has the 2nd highest frequency in English (in our case 2nd is W), let us replace $W \to t$ and $Q \to h$.



The most common trigraphs in the english language are:
THE,AND,THA,ENT,ION,TIO,FOR,NDE,HAS,NCE,TIS,OFT,MEN

The most common trigraphs in the message are:
WQV,TGO,XGJ,XNG,TWX,IXV,XVO,HIF,IFU,FUW,WXN,CIX,VOZ

IXKeIATGL UDASXHTtXNG GN. 22, RIXtteG XG 1920 RheG CIXeOZTG RTP28, ZDPt Ae IeJTIOeO TP the ZNPt XZUNItTGt PXGJSe UDASXHTtXNG XGHIFUtNSNJF. Xt tNNL the PHXeGHe XGtN T GeR RNISO. eGtXtSeO the XGOeY NCHNXGHXOeGHe **TGO** XtP TUUSXHTtXNGP XG HIFUtNJITUhF, Xt OePHIXAeO thePNSDtXNG NC tRN HNZUSXHTteO HXUheI PFPteZP. CIXeOZTG, hNReKeI, RTP SePPXGteIePteO XG UINKXGJ theXI KDSGeITAXSXtF thTG he RTP XG DPXGJ theZ TP TKehXHSe CNI GeR ZethNOP NC HIFUtTGTSFPXP.XG Xt, CIXeOZTG OeKXPeO tRN GeR teHhGXBDeP. NGe RTP AIXSSXTGt. XtUeIZXtteO hXZ tN IeHNGPtIDHt T UIXZTIF HXUheI TSUhTAet RXthNDt hTKXGJtN JDePP Tt T PXGJSe USTXGteYt SetteI. ADt the NtheI RTP UINCNDGO. CNI theCXIPt tXZe XG HIFUtNSNJF, CIXeOZTG tIeTteO T CIeBDeGHF OXPtIXADtXNG TP TGeGtXtF, TP T HDIKe RhNPe PeKeITS UNXGtP ReIe HTDPTSSF IeSTteO, GNt TP EDPtT HNSSeHtXNG NC XGOXKXODTS SetteIP thTt hTUUeG tN Pt**TGO** XG T HeItTXG NIOeICNI GNGHTDPTS (hXPtNIXHTS) IeTPNGP, **TGO** tN thXP HDIKe he TUUSXeO PtTtXPtXHTSHNGHeUtP. the IePDStP HTG NGSF Ae OePHIXAeO TP UINZetheTG, CNICIXeOZTG'P PtINLe NC JeGXDP XGPUXIeO the GDZeINDP, KTIXeO, **TGO** KXtTSPtTtXPtXHTS tNNSP thTt TIe XGOXPUeGPTASe tN the HIFUtNSNJF NC tNOTF.AeCNIe CIXeOZTG, HIFUtNSNJF eLeO NDt TG eYXPteGHe TP T PtDOF DGtNXtPeSC, TP TG XPNSTteO UheGNZeGNG, GeXtheI ANIINRXGJ CINZ GNIHNGtIXADtXGJ tN NtheI ANOXeP NC LGNRSeOJe. CIeBDeGHF HNDGtP, SXGJDXPtXHHhTITHteIXPtXHP, LTPXPLX eYTZXGTtXNGP—TSS ReIe Ue-

HDSXTI **TGO** UTItXHDSTI tNHIFUtNSNJF. Xt OReSt T IeHSDPe XG the RNISO NC PHXeGHe. CIXeOZTG SeOHIFUtNSNJF NDt NC thXP SNGeSF RXSOeIGePP **TGO** XGtN the AINTO IXHh ONZTXG NCPtTtXPtXHP. he HNGGeHteO HIFUtNSNJF tN ZTtheZTtXHP. the PeGPe NCeYUTGOXGJ hNIXMNGP ZDPt hTKe IePeZASeO thTt CeSt AF HheZXPtP RheGCIXeOIXHh RNhSeI PFGthePXMeO DIeT, OeZNGPtITtXGJ thTt SXCe UINHePPePNUeITte DGOeI ReSS LGNRG HheZXHTS STRP **TGO** TIe theIeCNIe PDAEeHt tNeYUeIXZeGtTtXNG **TGO** HNGtINS, **TGO** SeTOXGJ tN tNOTF'P KTPt PtIXOeP XGAXNHheZXPtIF. RheG CIXeOZTG PDAPDZeO HIFUtTGTSFPXP DGOeI PtTtXPtXHP, he SXLeRXPe CSDGJ RXOe the ONNI tN TGTIZTZeGtTIXDZ tN RhXHh HIFUtNSNJF hTO GeKeI AeCNIe hTO THHePP. XtPReTUNGP—ZeTPDIeP NC HeGtITS teGOeGHF **TGO** OXPUeIPXNG, NC CXt **TGO**PLeRGePP, NC UINATAXSXtF **TGO** PTZUSXGJ **TGO** PXJGXCXHTGHe—ReIe XOeTSSFCTPhXNGeO tN OeTS RXth the PtTtXPtXHTS AehTKXNI NC SetteIP **TGO** RNIOP.HIFUtTGTSFPtP, PeXMXGJ theZ RXth TSTHIXtF, hTKe RXeSOeO theZ RXthGNtTASe PDHHePP eKeI PXGHe.thXP XP RhF CIXeOZTG hTP PTXO, XG SNNLXGJ ATHL NKeI hXP HTIeeI, thTtthe XGOeY NC HNXGHXOeGHe RTP hXP JIeTtePt PXGJSe HIeTtXNG. Xt TSNGe RNDSOhTKe RNG hXZ hXP IeUDtTtXNG. ADt XG CTHt Xt RTP NGSF the AeJXGGXGJ. he **TGO** ZIP. CIXeOZTG BDXt IXKeIATGL GeTI the eGO NC 1920. thePXtDTtXNG hTO AeHNZe XGtNSeITASe. CTAFTG hTO SDIeO hXZ ATHL TCteI theRTI RXth ITXPeP **TGO** UINZXPeP NC TAPNSDte CIeeONZ tN UINKe NI OXPUINKethe eYXPteGHe NC HXUheIP XG PhTLePUeTIe. ADt he hTO PBDeSHheO eKeIFTtteZUt tN ON PN **TGO** hTO eZATIITPPeO CIXeOZTG XGtN TUUTIeGtSFTHBDXePHeGt PXSeGHe Tt STGteIG-PSXOe SeHtDIeP NG the PDAEeHt. NG ETGDTIF1, 1921, CIXeOZTG AeJTG T PXY-ZNGth HNGtITHt RXth the PXJGTS HNIUP tNOeKXPe HIFUtNPFPteZP. RheG Xt eYUXIeO, he RTP tTLeG NG the HXKXS-PeIKXHeUTFINSS NC the RTI OeUTItZeGt Tt $4,500 T FeTI.NGe NC hXP CXIPt TPPXJGZeGtP RTP tN teTHh T HNDIPe XG ZXSXtTIF HNOeP**TGO** HXUheIP Tt the PXJGTS PHhNNS, theG Tt HTZU TSCIeO KTXS, GeR EeIPeF.CNI thXP he RINte T teYtANNL thTt, CNI the CXIPt tXZe, XZUNPeO NIOeI DUNGthe HhTNP NC HXUheI PFPteZP **TGO** theXI teIZXGNSNJF. thePe hTO PUINDteOXG T AeRXSOeIXGJ KTIXetF, **TGO** RIXteIP tIeTteO eTHh TP XGOXKXODTS **TGO**PUeHXTS HTPeP. CIXeOZTG PNIteO theZ NDt NG the ATPXP NC PtIDHtDIeXGPteTO NC TPUeHt, **TGO** PN SNJXHTS **TGO** DPeCDS RTP thXP HSTPPXCXHTtXNG thTt XthTP AeHNZe PtTGOTIO. he

ZNOeSeO hXP GNZeGHSTtDIe NG hXP HTteJNIXeP, PNthTt the GTZeP he ZXGteO hTKe the JIeTt ZeIXt NC ZTLXGJ the IeSTtXNGPAetReeG the KTIXNDP JeGeIT NC HXUheIP eKXOeGt NG PXJht. TG eYTZUSe XP theHNZUSeZeGtTIF UTXI ”ZNGNTSUhTAet” **TGO** ”UNSFTSUhTAet”; the CIeGHhReIe PtXSS HTSSXGJ UNSFTSUhTAetXH PFPteZP AF the TSZNPt NACDPHTtNIF”ONDASe PDAPtXtDtXNG,” RhXHh teSSP TAPNSDteSF GNthXGJ Tt TSS TANDt thePFPteZ. CIXeOZTG’P ZNPt XZUNItTGt HNXGTJe RTP the RNIO”HIFUtTGTSFPXP,” RhXHh he OeKXPeO XG 1920 tN HSeTI DU T HhINGXH PNDIHe NCHNGCDPXNG XG HIFUtNSNJF—the TZAXJDXtF NC the KeIA ”OeHXUheI,” theG DPeOtN ZeTG ANth TDthNIXMeO **TGO** DGTDthNIXMeO IeODHtXNGP NC T HIFUtNJITZ tN USTXGteYt.he tXtSeO hXP ANNL eSeZeGtP NC HIFUtTGTSFPXP, **TGO** the teIZ hTP PNUINPUeIeO thTt tNOTF Xt HXIHDSTteP XG JeGeITS HNGKeIPTtXNG **TGO** UIXGt.

- $T \to a$, $G \to n$, $O \to d$, $TGO \to AND$: The 2nd most common trigraph in the text is TGO; it appears most of the times as a single word and after “,”, so we can assume that $TGO \to AND$.

IXKeIAanL UDASXHatXNn **nN. 22**, RIXtten Xn 1920 Rhen CIXedZan RaP28, ZDPt Ae IeJaIded aP the ZNPt XZUNItant PXnJSe UDASXHatXNn XnHIFUtNSNJF. Xt tNNL the PHXenHe XntN a neR RNISd. entXtSed the XndeY NCHNXnHXdenHe and XtP aUUSXHatXNnP Xn HIFUtNJIaUhF, Xt dePHIXAed thePNSDtXNn NC tRN HNZUSXHated HXUheI PFPteZP. CIXedZan, hNReKeI, RaP SePPXnteIePted Xn UINKXnJ theXI KDSneIaAXSXtF than he RaP Xn DPXnJ theZ aP aKehXHSe CNI neR ZethNdP NC HIFUtanaSFPXP.Xn Xt, CIXedZan deKXPed tRN neR teHhnXBDeP. Nne RaP AIXSSXant. XtUeIZXtted hXZ tN IeHNnPtIDHt a UIXZaIF HXUheI aSUhaAet RXthNDt haKXnJtN JDePP at a PXnJSe USaXnteYt SetteI. ADt the NtheI RaP UINCNDnd. CNI theCXIPt tXZe Xn HIFUtNSNJF, CIXedZan tIeated a CIeBDenHF dXPtIXADtXNn aP anentXtF, aP a HDIKe RhNPe PeKeIaS UNXntP ReIe HaDPaSSF IeSated, nNt aP EDPta HNSSeHtXNn NC XndXKXdDaS SetteIP that haUUen tN Ptand Xn a HeItaXn NIdeICNI nNnHaDPaS (hXPtNIXHaS) IeaPNnP, and tN thXP HDIKe he aUUSXed PtatXPtXHaSHNnHeUtP. the IePDStP Han NnSF Ae dePHIXAed aP UINZethean, CNICIXedZan’P PtINLe NC JenXDP XnPUXIed the nDZeINDP, KaIXed, and KXtaSPtatXPtXHaS tNNSP that aIe XndXPUenPaASe tN the HIFUtNSNJF NC tNdaF.AeCNIe CIXedZan, HIFUtNSNJF eLed NDt an eYXPtenHe aP a PtDdF DntNXtPeSC, aP an XPNSated UhenNZenNn, neXtheI ANIINRXnJ CINZ nNIHNntIXADtXnJ tN NtheI ANdXeP NC LnNRSedJe. CIeBDenHF HNDntP, SXnJDXPtXHHhaIaHteIXPtXHP, LaPXPLX eYaZXnatXNnP—aSS ReIe UeHDSXaI and UaItXHDSaI tNHIFUtNSNJF. Xt dReSt a IeHSDPe Xn the RNISd NC PHXenHe. CIXedZan SedHIFUtNSNJF NDt NC thXP SNneSF RXSdeInePP and XntN the AINad IXHh dNZaXn NCPtatXPtXHP. he HNnneHted HIFUtNSNJF tN ZatheZatXHP. the PenPe NCeYUandXnJ hNIXMNnP ZDPt haKe IePeZASed that CeSt AF HheZXPtP RhenCIXedIXHh RNhSeI PFnthePXMed DIea, deZNnPtIatXnJ that SXCe UINHePPePNUeIate DndeI ReSS LnNRn HheZXHaS SaRP and aIe theIeCNIe PDAEeHt tNeYUeIXZentatXNn and HNntINS, and SeadXnJ tN tNdaF'P KaPt PtIXdeP XnAXNHheZXPtIF. Rhen CIXedZan PDAPDZed HIFUtanaSFPXP DndeI PtatXPtXHP, he SXLeRXPe CSDnJ RXde the dNNI tN anaIZaZentaIXDZ tN RhXHh HIFUtNSNJF had neKeI AeCNIe had aHHePP. XtPReaUNnP—ZeaPDIeP NC HentIaS tendenHF and dXPUeIPXNn, NC CXt andPLeRnePP, NC UINAaAXSXtF and PaZUSXnJ and PXJnXCXHanHe—ReIe XdeaSSFCaPhXNned tN deaS RXth the PtatXPtXHaS AehaKXNI NC SetteIP and RNIdP.HIFUtanaSFPtP, PeXMXnJ theZ RXth aSaHIXtF, haKe RXeSded theZ RXthnNtaASe PDHHePP eKeI PXnHe.thXP XP RhF CIXedZan haP PaXd, Xn SNNLXnJ AaHL NKeI hXP HaIeeI, thatthe XndeY NC HNXnHXdenHe RaP hXP JIeatePt PXnJSe HIeatXNn. Xt aSNne RNDSdhaKe RNn hXZ hXP IeUDtatXNn. ADt Xn CaHt Xt RaP NnSF the AeJXnnXnJ. he and ZIP. CIXedZan BDXt IXKeIAanL neaI the end NC 1920. thePXtDatXNn had AeHNZe XntNSeIaASe. CaAFan had SDIed hXZ AaHL aCteI theRaI RXth IaXPeP and UINZXPeP NC aAPNSDte CIeedNZ tN UINKe NI dXPUINKethe eYXPtenHe NC HXUheIP Xn PhaLePUeaIe. ADt he had PBDeSHhed eKeIFatteZUt tN dN PN and had eZAaIIaPPed CIXedZan XntN aUUaIentSFaHBDXePHent PXSenHe at SanteIn-PSXde SeHtDIeP Nn the PDAEeHt. Nn EanDaIF1, 1921, CIXedZan AeJan a PXY-ZNnth HNntIaHt RXth the PXJnaS HNIUP tNdeKXPe HIFUtNPFPteZP. Rhen Xt eYUXIed, he RaP taLen Nn the HXKXS-PeIKXHeUaFINSS NC the RaI deUaItZent at $4,500 a FeaI.Nne NC hXP CXIPt aPPXJnZentP RaP tN teaHh a HNDIPe Xn ZXSXtaIF HNdePand HXUheIP at the PXJnaS PHhNNS, then at HaZU aSCIed KaXS, neR EeIPeF.CNI thXP he RINte a teYtANNL that, CNI the CXIPt tXZe, XZUNPed NIdeI DUNnthe HhaNP NC HXUheI PFPteZP and theXI teIZXnNSNJF. thePe had PUINDtedXn a AeRXSdeIXnJ KaIXetF, and RIXteIP tIeated eaHh aP XndXKXdDaS andPUeHXaS HaPeP. CIXedZan PNIted theZ NDt Nn the AaPXP NC PtIDHtDIeXnPtead NC aPUeHt, and PN SNJXHaS and DPeCDS RaP thXP HSaPPXCXHatXNn that XthaP AeHNZe PtandaId. he ZNdeSed hXP nNZenHSatDIe

Nn hXP HateJNIXeP, PNthat the naZeP he ZXnted haKe the JIeat ZeIXt NC ZaLXnJ the IeSatXNnPAetReen the KaIXNDP JeneIa NC HXUheIP eKXdent Nn PXJht. an eYaZUSe XP theHNZUSeZentaIF UaXI ”ZNnN-aSUhaAet” and ”UNSFaSUhaAet”; the CIenHhReIe PtXSS HaSSXnJ UNSFaSUhaAetXH PFPteZP AF the aSZNPt NACDPHatNIF”dNDASe PDAPtXtDtXNn,” RhXHh teSSP aAPNSDteSF nNthXnJ at aSS aANDt thePFPteZ. CIXedZan’P ZNPt XZUNItant HNXnaJe RaP the RNId”HIFUtanaSFPXP,” RhXHh he deKXPed Xn 1920 tN HSeaI DU a HhINnXH PNDIHe NCHNnCDPXNn Xn HIFUtNSNJF—the aZAXJDXtF NC the KeIA ”deHXUheI,” then DPedtN Zean ANth aDthNIXMed and DnaDthNIXMed IedDHtXNnP NC a HIFUtNJIaZ tN USaXnteYt.he tXtSed hXP ANNL eSeZentP NC HIFUtanaSFPXP, and the teIZ haP PNUINPUeIed that tNdaF Xt HXIHDSateP Xn JeneIaS HNnKeIPatXNn and UIXnt.

- $N \rightarrow O$, $nN \rightarrow no$: In the text we have “nN. 22”, so we can easily tell that $nN \rightarrow no$.

IXKeIAanL UDASXHatXon no. 22, RIXtten **Xn 1920** Rhen CIXedZan RaP28, ZDPt Ae IeJaIded aP the ZoPt XZUoItant PXnJSe UDASXHatXon XnHIFUtoSoJF. Xt tooL the PHXenHe Xnto a neR RoISd. entXtSed the XndeY oCHoXnHXdenHe and XtP aUUSXHatXonP Xn HIFUtoJIaUhF, Xt dePHIXAed thePoSDtXon oC tRo HoZUSXHated HXUheI PFPteZP. CIXedZan, hoReKeI, RaP SePPXnteIePted Xn UIoKXnJ theXI KDSneIaAXSXtF than he RaP Xn DPXnJ theZ aP aKehXHSe CoI neR ZethodP oC HIFUtanaSFPXP.Xn Xt, CIXedZan deKXPed tRo neR teHhnXBDeP. one RaP AIXSSXant. XtUeIZXtted hXZ to IeHonPtIDHt a UIXZaIF HXUheI aSUhaAet RXthoDt haKXnJto JDePP at a PXnJSe USaXnteYt SetteI. ADt the otheI RaP UIoCoDnd. CoI theCXIPt tXZe Xn HIFUtoSoJF, CIXedZan tIeated a CIeBDenHF dXPtIXADtXon aP anentXtF, aP a HDIKe RhoPe PeKeIaS UoXntP ReIe HaDPaSSF IeSated, not aP EDPta HoSSeHtXon oC XndXKXdDaS SetteIP that haUUen to Ptand Xn a HeItaXn oIdeICoI nonHaDPaS (hXPtoIXHaS) IeaPonP, and to thXP HDIKe he aUUSXed PtatXPtXHaSHonHeUtP. the IePDStP Han onSF Ae dePHIXAed aP UIoZethean, CoICIXedZan’P PtIoLe oC JenXDP XnPUXIed the nDZeIoDP, KaIXed, and KXtaSPtatXPtXHaS tooSP that aIe XndXPUenPaASe to the HIFUtoSoJF oC todaF.AeCoIe CIXedZan, HIFUtoSoJF eLed oDt an eYXPtenHe aP a PtDdF DntoXtPeSC, aP an XPoSated UhenoZenon, neXtheI AoIIoRXnJ CIoZ noIHontIXADtXnJ to otheI AodXeP oC LnoRSedJe. CIeBDenHF HoDntP, SXnJDXPtXHHhaIaHteIXPtXHP, LaPXPLX eYaZXnatXonP—aSS ReIe UeHDSXaI and UaItXHDSaI toHIFUtoSoJF. Xt dReSt a IeHSDPe Xn the RoISd oC PHXenHe. CIXedZan SedHIFUtoSoJF oDt oC thXP SoneSF RXSdeInePP and Xnto the AIoad IXHh doZaXn oCPtatXPtXHP. he HonneHted HIFUtoSoJF to ZatheZatXHP. the PenPe oCeYUandXnJ hoIXMonP ZDPt haKe IePeZASed that CeSt AF HheZXPtP RhenCIXedIXHh RohSeI PFnthePXMed DIea, deZonPtIatXnJ that SXCe UIoHePPePoUeIate DndeI ReSS LnoRn HheZXHaS SaRP and aIe theIeCoIe PDAEeHt toeYUeIXZentatXon and HontIoS, and SeadXnJ to todaF’P KaPt PtIXdeP XnAXoHheZXPtIF. Rhen CIXedZan PDAPDZed HIFUtanaSFPXP DndeI PtatXPtXHP, he SXLeRXPe CSDnJ RXde the dooI to anaIZaZentaIXDZ to RhXHh HIFUtoSoJF had neKeI AeCoIe had aHHePP. XtPReaUonP—ZeaPDIeP oC HentIaS tendenHF and dXPUeIPXon, oC CXt andPLeRnePP, oC UIoAaAXSXtF and PaZUSXnJ and PXJnXCXHanHe—ReIe XdeaSSFCaPhXoned to deaS RXth the PtatXPtXHaS AehaKXoI oC SetteIP and RoIdP.HIFUtanaSFPtP, PeXMXnJ theZ RXth aSaHIXtF, haKe RXeSded theZ RXthnotaASe PDHHePP eKeI PXnHe.thXP XP RhF CIXedZan haP PaXd, Xn SooLXnJ AaHL oKeI hXP HaIeeI, thatthe XndeY oC HoXnHXdenHe RaP hXP JIeatePt PXnJSe HIeatXon. Xt aSone RoDSdhaKe Ron hXZ hXP IeUDtatXon. ADt Xn CaHt Xt RaP onSF the AeJXnnXnJ. he and ZIP. CIXedZan BDXt IXKeIAanL neaI the end oC 1920. thePXtDatXon had AeHoZe XntoSeIaASe. CaAFan had SDIed hXZ AaHL aCteI theRaI RXth IaXPeP and UIoZXPeP oC aAPoSDte CIeedoZ to UIoKe oI dXPUIoKethe eYXPtenHe oC HXUheIP Xn PhaLePUeaIe. ADt he had PBDeSHhed eKeIFatteZUt to do Po and had eZAaIIaPPed CIXedZan Xnto aUUaIentSFaHBDXePHent PXSenHe at SanteIn-PSXde SeHtDIeP on the PDAEeHt. on EanDaIF1, 1921, CIXedZan AeJan a PXY-Zonth HontIaHt RXth the PXJnaS HoIUP todeKXPe HIFUtoPFPteZP. Rhen Xt eYUXIed, he RaP taLen on the HXKXS-PeIKXHeUaFIoSS oC the RaI deUaItZent at $4,500 a FeaI.one oC hXP CXIPt aPPXJnZentP RaP to teaHh a HoDIPe Xn ZXSXtaIF HodePand HXUheIP at the PXJnaS PHhooS, then at HaZU aSCIed KaXS, neR EeIPeF.CoI thXP he RIote a teYtAooL that, CoI the CXIPt tXZe, XZUoPed oIdeI DUonthe HhaoP oC HXUheI PFPteZP and theXI teIZXnoSoJF. thePe had PUIoDtedXn a AeRXSdeIXnJ KaIXetF, and RIXteIP tIeated eaHh aP XndXKXdDaS andPUeHXaS HaPeP. CIXedZan PoIted theZ oDt on the AaPXP oC PtIDHtDIeXnPtead oC aPUeHt, and Po SoJXHaS and DPeCDS RaP thXP HSaPPXCXHatXon that XthaP AeHoZe PtandaId. he ZodeSed hXP noZenHSatDIe on hXP HateJoIXeP, Pothat the naZeP he ZXnted haKe the JIeat ZeIXt oC ZaLXnJ the IeSatXonPAetReen the KaIXoDP JeneIa oC HXUheIP eKXdent on PXJht. an eYaZUSe XP theHoZUSeZentaIF UaXI ”Zono-aSUhaAet” and ”UoSFaSUhaAet”; the CIenHhReIe PtXSS HaSSXnJ UoSFaSUhaAetXH PFPteZP AF the aSZoPt oACDPHatoIF”doDASe PDAPtXtDtXon,” RhXHh teSSP aAPoSDteSF nothXnJ at aSS aAoDt thePFPteZ. CIXedZan’P ZoPt XZUoItant HoXnaJe RaP the RoId”HIFUtanaSFPXP,” RhXHh he deKXPed Xn 1920 to HSeaI DU a HhIonXH PoDIHe oCHonCDPXon Xn HIFUtoSoJF—the aZAXJDXtF oC the KeIA ”deHXUheI,” then DPedto Zean Aoth aDthoIXMed and DnaDthoIXMed IedDHtXonP oC a HIFUtoJIaZ to USaXnteYt.he tXtSed hXP AooL eSeZentP oC HIFUtanaSFPXP, and the teIZ haP PoUIoPUeIed that todaF Xt HXIHDSateP Xn JeneIaS HonKeIPatXon and UIXnt.

- $X \to I$, $Xn \to in$: Another telling instance is “Xn 1920”, thus $Xn \to in$.

IiKeIAanL UDASiHation no. 22, RIitten in 1920 Rhen CIiedZan RaP28, ZDPt Ae IeJaIded aP the ZoPt iZUoItant PinJSe UDASiHation inHIFUtoSoJF. it tooL the PHienHe into a neR RoISd. entitSed the indeY oCHoinHidenHe and itP aUUSiHationP in HIFUtoJIaUhF, it dePHIiAed thePoSDtion oC tRo HoZUSiHated HiUheI PFPteZP. CIiedZan, hoReKeI, RaP SePPinteIePted in UIoKinJ theiI KDSneIaAiSitF than he RaP in DPinJ theZ aP aKehiHSe CoI neR ZethodP oC HIFUtanaSFPiP.in it, CIiedZan deKiPed tRo neR teHhniBDeP. one RaP AIiSSiant. itUeIZitted hiZ to IeHonPtIDHt a UIiZaIF HiUheI aSUhaAet RithoDt haKinJto JDePP at a PinJSe USainteYt SetteI. ADt the otheI RaP UIoCoDnd. CoI theCiIPt tiZe in HIFUtoSoJF, CIiedZan tIeated a CIeBDenHF diPtIiADtion aP anentitF, aP a HDIKe RhoPe PeKeIaS UointP ReIe HaDPaSSF IeSated, not aP EDPta HoSSeHtion oC indiKidDaS SetteIP that haUUen to Ptand in a HeItain oIdeICoI nonHaDPaS (hiPtoIiHaS) IeaPonP, and to thiP HDIKe he aUUSied PtatiPtiHaSHonHeUtP. the IePDStP Han onSF Ae dePHIiAed aP UIoZethean, CoICIiedZan’P PtIoLe oC JeniDP inPUiIed the nDZeIoDP, KaIied, and KitaSPtatiPtiHaS tooSP that aIe indiPUenPaASe to the HIFUtoSoJF oC todaF.AeCoIe CIiedZan, HIFUtoSoJF eLed oDt an eYiPtenHe aP a PtDdF DntoitPeSC, aP an iPoSated UhenoZenon, neitheI AoIIoRinJ CIoZ noIHontIiADtinJ to otheI AodieP oC LnoRSedJe. CIeBDenHF HoDntP, SinJDiPtiHHhaIaHteIiPtiHP, LaPiPLi eYaZinationP—aSS ReIe UeHDSiaI and UaItiHDSaI toHIFUtoSoJF. it dReSt a IeHSDPe in the RoISd oC PHienHe. CIiedZan SedHIFUtoSoJF oDt oC thiP SoneSF RiSdeInePP and into the AIoad IiHh doZain oCPtatiPtiHP. he HonneHted HIFUtoSoJF to ZatheZatiHP. the PenPe oCeYUandinJ hoIiMonP ZDPt haKe IePeZASed that CeSt AF HheZiPtP RhenCIiedIiHh RohSeI PFnthePiMed DIea, deZonPtIatinJ that SiCe UIoHePPePoUeIate DndeI ReSS LnoRn HheZiHaS SaRP and aIe theIeCoIe PDAEeHt toeYUeIiZentation and HontIoS, and SeadinJ to todaF’P KaPt PtIideP inAioHheZiPtIF. Rhen CIiedZan PDAPDZed HIFUtanaSFPiP

DndeI PtatiPtiHP, he SiLeRiPe CSDnJ Ride the dooI to anaIZaZentaIiDZ to RhiHh HIFUtoSoJF had neKeI AeCoIe had aHHePP. itPReaUonP—ZeaPDIeP oC HentIaS tendenHF and diPUeIPion, oC Cit andPLeRnePP, oC UIoAaAiSitF and PaZUSinJ and PiJniCiHanHe—ReIe ideaSSFCaPhioned to deaS Rith the PtatiPtiHaS AehaKioI oC SetteIP and RoIdP.HIFUtanaSFPtP, PeiMinJ theZ Rith aSaHIitF, haKe RieSded theZ RithnotaASe PDHHePP eKeI PinHe.**thiP iP** RhF CIiedZan **haP Paid**, in SooLinJ AaHL oKeI hiP HaIeeI, thatthe indeY oC HoinHidenHe RaP hiP JIeatePt PinJSe HIeation. it aSone RoDSdhaKe Ron hiZ hiP IeUDtation. ADt in CaHt it RaP onSF the AeJinninJ. he and ZIP. CIiedZan BDit IiKeIAanL neaI the end oC 1920. thePitDation had AeHoZe intoSeIaASe. CaAFan had SDIed hiZ AaHL aCteI theRaI Rith IaiPeP and UIoZiPeP oC aAPoSDte CIeedoZ to UIoKe oI diPUIoKethe eYiPtenHe oC HiUheIP in PhaLePUeaIe. ADt he had PBDeSHhed eKeIFatteZUt to do Po and had eZAaIIaPPed CIiedZan into aUUaIentSFaHBDiePHent PiSenHe at SanteIn-PSide SeHtDIeP on the PDAEeHt. on EanDaIF1, 1921, CIiedZan AeJan a PiY-Zonth HontIaHt Rith the PiJnaS HoIUP todeKiPe HIFUtoPFPteZP. Rhen it eYUiIed, he RaP taLen on the HiKiS-PeIKiHeUaFIoSS oC the RaI deUaItZent at $4,500 a FeaI.one oC hiP CiIPt aPPiJnZentP RaP to teaHh a HoDIPe in ZiSitaIF HodePand HiUheIP at the PiJnaS PHhooS, then at HaZU aSCIed KaiS, neR EeIPeF.CoI thiP he RIote a teYtAooL that, CoI the CiIPt tiZe, iZUoPed oIdeI DUonthe HhaoP oC HiUheI PFPteZP and theiI teIZinoSoJF. thePe had PUIoDtedin a AeRiSdeIinJ KaIietF, and RIiteIP tIeated eaHh aP indiKidDaS andPUeHiaS HaPeP. CIiedZan PoIted theZ oDt on the AaPiP oC PtIDHtDIeinPtead oC aPUeHt, and Po SoJiHaS and DPeCDS RaP thiP HSaPPiCiHation that ithaP AeHoZe PtandaId. he ZodeSed hiP noZenHSatDIe on hiP HateJoIieP, Pothat the naZeP he Zinted haKe the JIeat ZeIit oC ZaLinJ the IeSationPAetReen the KaIioDP JeneIa oC HiUheIP eKident on PiJht. an eYaZUSe iP theHoZUSeZentaIF UaiI ”Zono-aSUhaAet” and ”UoSFaSUhaAet”; the CIenHhReIe PtiSS HaSSinJ UoSFaSUhaAetiH PFPteZP AF the aSZoPt oACDPHatoIF”doDASe PDAPtitDtion,” RhiHh teSSP aAPoSDteSF nothinJ at aSS aAoDt thePFPteZ. CIiedZan’P ZoPt iZUoItant HoinaJe RaP the RoId”HIFUtanaSFPiP,” RhiHh he deKiPed in 1920 to HSeaI DU a HhIoniH PoDIHe oCHonCDPion in HIFUtoSoJF—the aZAiJDitF oC the KeIA ”deHiUheI,” then DPedto Zean Aoth aDthoIiMed and DnaDthoIiMed IedDHtionP oC a HIFUtoJIaZ to USainteYt.he titSed hiP AooL eSeZentP oC HIFUtanaSFPiP, and the teIZ haP PoUIoPUeIed that todaF it HiIHDSateP in JeneIaS HonKeIPation and UIint.

- $P \to S$: From the phrase “thiP iP ... haP Paid”, we can state that $P \to S$.

IiKeIAanL UDASiHation no. 22, RIitten in 1920 Rhen CIiedZan **Ras**28, ZDst Ae IeJaIded as the Zost iZUoItant sinJSe UDASiHation inHIFUtoSoJF. it tooL the sHienHe into a **neR** RoISd. entitSed the indeY oCHoinHidenHe and its aUUSiHations in HIFUtoJIaUhF, it desHIiAed thesoSDtion oC tRo HoZUSiHated HiUheI sFsteZs. CIiedZan, hoReKeI, **Ras** SessinteIested in UIoKinJ theiI KDSneIaAiSitF than he **Ras** in DsinJ theZ as aKehiHSe CoI **neR** Zethods oC HIFUtanaSFsis.in it, CIiedZan deKised tRo **neR** teHhniBDes. one **Ras** AIiSSiant. itUeIZitted hiZ to IeHonstIDHt a UIiZaIF HiUheI aSUhaAet RithoDt haKinJto JDess at a sinJSe USainteYt SetteI. ADt the otheI **Ras** UIoCoDnd. CoI theCiIst tiZe in HIFUtoSoJF, CIiedZan tIeated a CIeBDenHF distIiADtion as anentitF, as a HDIKe Rhose seKeIaS Uoints ReIe HaDsaSSF IeSated, not as EDsta HoSSeHtion oC indiKidDaS SetteIs that haUUen to stand in a HeItain oIdeICoI nonHaDsaS (histoIiHaS) Ieasons, and to this HDIKe he aUUSied statistiHaSHonHeUts. the IesDSts Han onSF Ae desHIiAed as UIoZethean, CoICIiedZan’s stIoLe oC JeniDs insUiIed the nDZeIoDs, KaIied, and KitaSstatistiHaS tooSs that aIe indisUensaASe to the HIFUtoSoJF oC todaF.AeCoIe CIiedZan, HIFUtoSoJF eLed oDt an eYistenHe as a stDdF DntoitseSC, as an isoSated UhenoZenon, neitheI AoIIoRinJ CIoZ noIHontIiADtinJ to otheI Aodies oC LnoRSedJe. CIeBDenHF HoDnts, SinJDistiHHhaIaHteIistiHs, LasisLi eYaZinations—aSS ReIe UeHDSiaI and UaItiHDSaI toHIFUtoSoJF. it dReSt a IeHSDse in the RoISd oC sHienHe. CIiedZan SedHIFUtoSoJF oDt oC this SoneSF RiSdeIness and into the AIoad IiHh doZain oCstatistiHs. he HonneHted HIFUtoSoJF to ZatheZatiHs. the sense oCeYUandinJ hoIiMons ZDst haKe IeseZASed that CeSt AF HheZists RhenCIiedIiHh RohSeI sFnthesiMed DIea, deZonstIatinJ that SiCe UIoHessesoUeIate DndeI ReSS LnoRn HheZiHaS SaRs and aIe theIeCoIe sDAEeHt toeYUeIiZentation and HontIoS, and SeadinJ to todaF’s Kast stIides inAioHheZistIF. Rhen CIiedZan sDAsDZed HIFUtanaSFsis DndeI statistiHs, he SiLeRise CSDnJ Ride the dooI to anaIZaZentaIiDZ to RhiHh HIFUtoSoJF had neKeI AeCoIe had aHHess. itsReaUons—ZeasDIes oC HentIaS tendenHF and disUeIsion, oC Cit andsLeRness, oC UIoAaAiSitF and saZUSinJ and siJniCiHanHe—ReIe ideaSSFCashioned to deaS Rith the statistiHaS AehaKioI oC SetteIs and RoIds.HIFUtanaSFsts, seiMinJ theZ Rith aSaHIitF, haKe RieSded theZ RithnotaASe sDHHess eKeI sinHe.this is RhF CIiedZan has said, in SooLinJ AaHL oKeI his HaIeeI, thatthe indeY oC HoinHidenHe **Ras** his JIeatest sinJSe HIeation. it aSone RoDSdhaKe Ron hiZ his IeUDtation. ADt in CaHt it **Ras** onSF the AeJinninJ. he and

ZIs. CIiedZan BDit IiKeIAanL neaI the end oC 1920. thesitDation had AeHoZe intoSeIaASe. CaAFan had SDIed hiZ AaHL aCteI theRaI Rith Iaises and UIoZises oC aAsoSDte CIeedoZ to UIoKe oI disUIoKethe eYistenHe oC HiUheIs in shaLesUeaIe. ADt he had sBDeSHhed eKeIFatteZUt to do so and had eZAaIIassed CIiedZan into aUUaIentSFaHBDiesHent siSenHe at SanteIn-sSide SeHtDIes on the sDAEeHt. on EanDaIF1, 1921, CIiedZan AeJan a siY-Zonth HontIaHt Rith the siJnaS HoIUs todeKise HIFUtosFsteZs. Rhen it eYUiIed, he **Ras** taLen on the HiKiS-seIKiHeUaFIoSS oC the RaI deUaItZent at $4,500 a FeaI.one oC his CiIst assiJnZents **Ras** to teaHh a HoDIse in ZiSitaIF Hodesand HiUheIs at the siJnaS sHhooS, then at HaZU aSCIed KaiS, **neR** EeIseF.CoI this he RIote a teYtAooL that, CoI the CiIst tiZe, iZUosed oIdeI DUonthe Hhaos oC HiUheI sFsteZs and theiI teIZinoSoJF. these had sUIoDtedin a AeRiSdeIinJ KaIietF, and RIiteIs tIeated eaHh as indiKidDaS andsUeHiaS Hases. CIiedZan soIted theZ oDt on the Aasis oC stIDHtDIeinstead oC asUeHt, and so SoJiHaS and DseCDS **Ras** this HSassiCiHation that ithas AeHoZe standaId. he ZodeSed his noZenHSatDIe on his HateJoIies, sothat the naZes he Zinted haKe the JIeat ZeIit oC ZaLinJ the IeSationsAetReen the KaIioDs JeneIa oC HiUheIs eKident on siJht. an eYaZUSe is theHoZUSeZentaIF UaiI ”Zono-aSUhaAet” and ”UoSFaSUhaAet”; the CIenHhReIe stiSS HaSSinJ UoSFaSUhaAetiH sFsteZs AF the aSZost oACDsHatoIF”doDASe sDAstitDtion,” RhiHh teSSs aAsoSDteSF nothinJ at aSS aAoDt thesFsteZ. CIiedZan’s Zost iZUoItant HoinaJe **Ras** the RoId”HIFUtanaSFsis,” RhiHh he deKised in 1920 to HSeaI DU a HhIoniH soDIHe oCHonCDsion in HIFUtoSoJF—the aZAiJDitF oC the KeIA ”deHiUheI,” then Dsedto Zean Aoth aDthoIiMed and DnaDthoIiMed IedDHtions oC a HIFUtoJIaZ to USainteYt.he titSed his AooL eSeZents oC HIFUtanaSFsis, and the teIZ has soUIosUeIed that todaF it HiIHDSates in JeneIaS HonKeIsation and UIint.

- $R \to W$: From the words “neR” and “Ras”, we can state that $R \to W$.

IiKeIAanL UDASiHation no. 22, **wIitten** in 1920 when CIiedZan was28, ZDst Ae IeJaIded as the Zost iZUoItant sinJSe UDASiHation inHIFUtoSoJF. it tooL the sHienHe into a new woISd. entitSed the indeY oCHoinHidenHe and its aUUSiHations in HIFUtoJIaUhF, it desHIiAed thesoSDtion oC two HoZUSiHated HiUheI sFsteZs. CIiedZan, howeKeI, was SessinteIested in UIoKinJ theiI KDSneIaAiSitF than he was in DsinJ theZ as aKehiHSe CoI new Zethods oC HIFUtanaSFsis.in it, CIiedZan deKised two new teHhniBDes. one was AIiSSiant. itUeIZitted hiZ to IeHonstIDHt a UIiZaIF HiUheI aSUhaAet withoDt haKinJto JDess at a sinJSe USainteYt SetteI. ADt the otheI was UIoCoDnd. CoI theCiIst tiZe in HIFUtoSoJF, CIiedZan tIeated a CIeBDenHF distIiADtion as anentitF, as a HDIKe whose seKeIaS Uoints weIe HaDsaSSF IeSated, not as EDsta HoSSeHtion oC indiKidDaS SetteIs that haUUen to stand in a HeItain oIdeICoI nonHaDsaS (histoIiHaS) Ieasons, and to this HDIKe he aUUSied statistiHaSHonHeUts. the IesDSts Han onSF Ae desHIiAed as UIoZethean, CoICIiedZan's stIoLe oC JeniDs insUiIed the nDZeIoDs, KaIied, and KitaSstatistiHaS tooSs that aIe indisUensaASe to the HIFUtoSoJF oC todaF.AeCoIe CIiedZan, HIFUtoSoJF eLed oDt an eYistenHe as a stDdF DntoitseSC, as an isoSated UhenoZenon, neitheI AoIIowinJ CIoZ noIHontIiADtinJ to otheI Aodies oC LnowSedJe. CIeBDenHF HoDnts, SinJDistiHHhaIaHteIistiHs, LasisLi eYaZinations—aSS weIe UeHDSiaI and UaItiHDSaI toHIFUtoSoJF. it dweSt a IeHSDse in the woISd oC sHienHe. CIiedZan SedHIFUtoSoJF oDt oC this SoneSF wiSdeIness and into the AIoad IiHh doZain oCstatistiHs. he HonneHted HIFUtoSoJF to ZatheZatiHs. the sense oCeYUandinJ hoIiMons ZDst haKe IeseZASed that CeSt AF HheZists whenCIiedIiHh wohSeI sFnthesiMed DIea, deZonstIatinJ that SiCe UIoHessesoUeIate DndeI weSS Lnown HheZiHaS Saws and aIe theIeCoIe sDAEeHt toeYUeIiZentation and HontIoS, and SeadinJ to todaF's Kast stIides inAioHheZistIF. when CIiedZan sDAsDZed HIFUtanaSFsis DndeI statistiHs, he SiLewise CSDnJ wide the dooI to anaIZaZentaIiDZ to whiHh HIFUtoSoJF had neKeI AeCoIe had aHHess. itsweaUons—ZeasDIes oC HentIaS tendenHF and disUeIsion, oC Cit andsLewness, oC UIoAaAiSitF and saZUSinJ and siJniCiHanHe—weIe ideaSSFCashioned to deaS with the statistiHaS AehaKioI oC SetteIs and woIds.HIFUtanaSFsts, seiMinJ theZ with aSaHIitF, haKe wieSded theZ withnotaASe sDHHess eKeI sinHe.this is whF CIiedZan has said, in SooLinJ AaHL oKeI his HaIeeI, thatthe indeY oC HoinHidenHe was his JIeatest sinJSe HIeation. it aSone woDSdhaKe won hiZ his IeUDtation. ADt in CaHt it was onSF the AeJinninJ. he and ZIs. CIiedZan BDit IiKeIAanL neaI the end oC 1920. thesitDation had AeHoZe intoSeIaASe. CaAFan had SDIed **hiZ** AaHL aCteI thewaI with Iaises and UIoZises oC aAsoSDte CIeedoZ to UIoKe oI disUIoKethe eYistenHe oC HiUheIs in shaLesUeaIe. ADt he had sBDeSHhed eKeIFatteZUt to do so and had eZAaIIassed CIiedZan into aUUaIentSFaHBDiesHent siSenHe at SanteIn-sSide SeHtDIes on the sDAEeHt. on EanDaIF1, 1921, CIiedZan AeJan a siY-Zonth HontIaHt with the siJnaS HoIUs todeKise HIFUtosFsteZs. when it eYUiIed, he was taLen on the HiKiS-seIKiHeUaFIoSS oC the waI deUaItZent at $4,500 a FeaI.one oC his CiIst assiJnZents was to teaHh a HoDIse in ZiSitaIF Hodesand HiUheIs at the siJnaS sHhooS, then at HaZU aSCIed KaiS, new EeIseF.CoI this he wIote a teYtAooL that, CoI the CiIst tiZe, iZUosed oIdeI DUonthe Hhaos oC HiUheI sFsteZs and theiI teIZinoSoJF. these had sUIoDtedin a AewiSdeIinJ KaIietF, and wIiteIs tIeated eaHh as indiKidDaS andsUeHiaS Hases. CIiedZan soIted **theZ** oDt on the Aasis oC stIDHtDIeinstead oC asUeHt, and so SoJiHaS and DseCDS was this HSassiCiHation that ithas AeHoZe standaId. he ZodeSed his noZenHSatDIe on his HateJoIies, sothat the naZes he Zinted haKe the JIeat ZeIit oC ZaLinJ the IeSationsAetween the KaIioDs JeneIa oC HiUheIs eKident on siJht. an eYaZUSe is theHoZUSeZentaIF UaiI "Zono-aSUhaAet" and "UoSFaSUhaAet"; the CIenHhweIe stiSS HaSSinJ UoSFaSUhaAetiH sFsteZs AF the aSZost oACDsHatoIF"doDASe sDAstitDtion," whiHh teSSs aAsoSDteSF nothinJ at aSS aAoDt thesFsteZ. CIiedZan's **Zost** iZUoItant HoinaJe was the woId"HIFUtanaSFsis," whiHh he deKised in 1920 to HSeaI DU a HhIoniH soDIHe oCHonCDsion in HIFUtoSoJF—the aZAiJDitF oC the KeIA "deHiUheI," then Dsedto Zean Aoth aDthoIiMed and DnaDthoIiMed IedDHtions oC a HIFUtoJIaZ to USainteYt.he titSed his AooL eSeZents oC HIFUtanaSFsis, and the teIZ has soUIosUeIed that todaF it HiIHDSates in JeneIaS HonKeIsation and UIint.

- $Z \to M$: From the words "hiZ", "Zost" and "theZ", we can tell that $Z \to M$.

- $I \to R$: From the context "wIitten in 1920" we can tell that $I \to R$.

riKerAanL UDASiHation no. 22, written in 1920 when Criedman was28, mDst Ae **reJarded** as the most **imUortant** sinJSe UDASiHation inHrFUtoSoJF. it tooL the sHienHe into a new **worSd. entitSed** the indeY oCHoinHidenHe and its aUUSiHations in HrFUtoJraUhF, it desHriAed thesoSDtion oC two HomUSiHated HiUher sFstems. Criedman, howeKer, was Sessinterested in UroKinJ their KDSneraAiSitF than he was in DsinJ them as aKehiHSe Cor new methods oC HrFUtanaSFsis.in it, Criedman deKised two new teHhniBDes. one was AriSSiant. itUermitted him to reHonstrDHt a UrimarF HiUher aSUhaAet withoDt haKinJto JDess at a sinJSe USainteYt Setter. ADt the other was UroCoDnd. Cor theCirst time in HrFUtoSoJF, Criedman treated a CreBDenHF distriADtion 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 Ae desHriAed as Uromethean, CorCriedman's stroLe oC JeniDs insUired the nDmeroDs, Karied, and KitaSstatistiHaS tooSs that are indisUensaASe to the HrFUtoSoJF oC todaF.AeCore Criedman, HrFUtoSoJF eLed oDt an eYistenHe as a stDdF DntoitseSC, as an isoSated Uhenomenon, neither AorrowinJ

Crom norHontriADtinJ to other Aodies oC LnowSedJe. CreBDenHF HoDnts, SinJDistiHHharaHteristiHs, LasisLi eYaminations—aSS were UeHDSiar and UartiHDSar toHrFUtoSoJF. it dweSt a reHSDse in the worSd oC sHienHe. Criedman SedHrFUtoSoJF oDt oC this SoneSF wiSderness and into the Aroad riHh domain oCstatistiHs. he HonneHted HrFUtoSoJF to mathematiHs. the sense oCeYUandinJ horiMons mDst haKe resemASed that CeSt AF Hhemists whenCriedriHh wohSer sFnthesiMed Drea, demonstratinJ that SiCe UroHessesoUerate Dnder weSS Lnown HhemiHaS Saws and are thereCore sDAEeHt toeYUerimentation and HontroS, and SeadinJ to todaF's Kast strides inAioHhemistrF. when Criedman sDAsDmed HrFUtanaSFsis Dnder statistiHs, he SiLewise CSDnJ wide the door to anarmamentariDm to whiHh HrFUtoSoJF had neKer AeCore had aHHess. itsweaUons—measDres oC HentraS tendenHF and disUersion, oC Cit andsLewness, oC UroAaAiSitF and samUSinJ and siJniCiHanHe—were ideaSSFCashioned to deaS with the statistiHaS AehaKior oC Setters and words.HrFUtanaSFsts, seiMinJ them with aSaHritF, haKe wieSded them withnotaASe sDHHess eKer sinHe.this is whF Criedman has said, in SooLinJ AaHL oKer his Hareer, thatthe indeY oC HoinHidenHe was his Jreatest sinJSe Hreation. it aSone woDSdhaKe won him his reUDtation. ADt in CaHt it was onSF the AeJinninJ. he and mrs. Criedman BDit riKerAanL near the end oC 1920. thesitDation had AeHome intoSeraASe. CaAFan had SDred him AaHL aCter thewar with raises and Uromises oC aAsoSDte Creedom to UroKe or disUroKethe eYistenHe oC HiUhers in shaLesUeare. ADt he had sBDeSHhed eKerFattemUt to do so and had emAarrassed Criedman into aUUarentSFaHBDiesHent siSenHe at Santern-sSide SeHtDres on the sDAEeHt. on EanDarF1, 1921, Criedman AeJan a siY-month HontraHt with the siJnaS HorUs todeKise HrFUtosFstems. when it eYUired, he was taLen on the HiKiS-serKiHeUaFroSS oC the war deUartment at $4,500 a Fear.one oC his Cirst assiJnments was to teaHh a HoDrse in miSitarF Hodesand HiUhers at the siJnaS sHhooS, then at HamU aSCred KaiS, new EerseF.Cor this he wrote a teYtAooL that, Cor the Cirst time, imUosed order DUonthe Hhaos oC HiUher sFstems and their terminoSoJF. these had sUroDtedin a AewiSderinJ KarietF, and writers treated eaHh as indiKidDaS andsUeHiaS Hases. Criedman sorted them oDt on the Aasis oC strDHtDreinstead oC asUeHt, and so SoJiHaS and DseCDS was this HSassiCiHation that ithas AeHome standard. he modeSed his nomenHSatDre on his HateJories, sothat the names he minted haKe the Jreat merit oC maLinJ the reSationsAetween the KarioDs Jenera oC HiUhers eKident on siJht. an eYamUSe is theHomUSementarF Uair ”mono-aSUhaAet” and ”UoSFaSUhaAet”; the CrenHhwere stiSS HaSSinJ UoSFaSUhaAetiH sFstems AF the aSmost oACDsHatorF”doDASe sDAstitDtion,” whiHh teSSs aAsoSDteSF nothinJ at aSS aAoDt thesFstem. Criedman’s most imUortant HoinaJe was the word”HrFUtanaSFsis,” whiHh he deKised in 1920 to HSear DU a HhroniH soDrHe oCHonCDsion in HrFUtoSoJF—the amAiJDitF oC the KerA ”deHiUher,” then Dsedto mean Aoth aDthoriMed and DnaDthoriMed redDHtions oC a HrFUtoJram to USainteYt.he titSed his AooL eSements oC HrFUtanaSFsis, and the term has soUrosUered that todaF it HirHDSates in JeneraS HonKersation and Urint.

- $J \to G$, $U \to P$: From the context “Ae reJarded as the most imUortant” we can tell that $J \to G$ and $U \to P$.

- $S \to L$: From the words “entitSed” and “singSe”, we can state that $S \to L$.

riKerAanL pDAliHation no. 22, written in 1920 when Criedman was28, **mDst Ae regarded as** the most important single pDAliHation inHrFptologF. it tooL the sHienHe into a new world. entitled the indeY oCHoinHidenHe and its appliHations in HrFptographF, it desHriAed thesolDtion oC two HompliHated Hipher sFstems. Criedman, **howeKer**, was lessinterested in **proKing** their KDlneraAilitF than he was in Dsing them as aKehiHle Cor new methods oC HrFptanalFsis.in it, Criedman deKised two new teHhniBDes. one was Arilliant. itpermitted him to reHonstrDHt a primarF Hipher alphaAet withoDt haKingto gDess at a single plainteYt letter. ADt the other was proCoDnd. Cor theCirst time in HrFptologF, Criedman treated a CreBDenHF distriADtion as anentitF, as a HDrKe whose seKeral points were HaDsallF related, not as EDsta HolleHtion oC indiKidDal letters that happen to stand in a Hertain orderCor nonHaDsal (historiHal) reasons, and to this HDrKe he applied statistiHalHonHepts. the resDlts Han onlF Ae desHriAed as promethean, CorCriedman’s stroLe oC geniDs inspired the nDmeroDs, Karied, and KitalstatistiHal tools that are indispensaAle to the HrFptologF oC todaF.AeCore Criedman, HrFptologF eLed oDt an eYistenHe as a stDdF DntoitselC, as an isolated phenomenon, neither Aorrowing Crom norHontriADting to other Aodies oC Lnowledge. CreBDenHF HoDnts, lingDistiHHharaHteristiHs, LasisLi eYaminations—all were peHDliar and partiHDlar toHrFptologF. it dwelt a reHlDse in the world oC sHienHe. Criedman ledHrFptologF oDt oC this lonelF wilderness and into the Aroad riHh domain oCstatistiHs. he HonneHted HrFptologF to mathematiHs. the sense oCeYpanding horiMons mDst haKe resemAled that Celt AF Hhemists whenCriedriHh wohler sFnthesiMed Drea, demonstrating that liCe proHessesoperate Dnder well Lnown HhemiHal laws and are thereCore sDAEeHt toeYperimentation and Hontrol, and leading to todaF's Kast strides inAioHhemistrF. when Criedman sDAsDmed HrFptanalFsis Dnder statistiHs, he liLewise ClDng wide the door to anarmamentariDm to whiHh HrFptologF had neKer AeCore had aHHess. itsweapons—measDres oC Hentral tendenHF and dispersion, oC Cit andsLewness, oC proAaAilitF and sampling and signiCiHanHe—were ideallFCashioned to deal with the statistiHal AehaKior oC letters and words.HrFptanalFsts, seiMing them with alaHritF, haKe wielded them withnotaAle sDHHess eKer sinHe.this is whF Criedman has said, in looLing AaHL oKer his Hareer, thatthe indeY oC HoinHidenHe was his greatest single Hreation. it alone woDldhaKe won him his repDtation. ADt in CaHt it was onlF the Aeginning. he and mrs. Criedman BDit riKerAanL near the end oC 1920. thesitDation had AeHome intoleraAle. CaAFan had lDred him AaHL aCter thewar with raises and promises oC aAsolDte Creedom to proKe or disproKethe eYistenHe oC Hiphers in shaLespeare. ADt he had sBDelHhed eKerFattempt to do so and had emAarrassed Criedman into apparentlFaHBDiesHent silenHe at lantern-slide leHtDres on the sDAEeHt. on EanDarF1, 1921, Criedman Aegan a siY-month HontraHt with the signal Horps todeKise HrFptosFstems. when it eYpired, he was taLen on the HiKilserKiHepaFroll oC the war department at $4,500 a Fear.one oC his Cirst assignments was to teaHh a HoDrse in militarF Hodesand Hiphers at the signal sHhool, then at Hamp alCred Kail, new EerseF.Cor this he wrote a teYtAooL that, Cor the Cirst time, imposed order Dponthe Hhaos oC Hipher sFstems and their terminologF. these had sproDtedin a Aewildering KarietF, and writers treated eaHh as indiKidDal andspeHial Hases. Criedman sorted them oDt on the Aasis oC strDHtDreinstead oC aspeHt, and so logiHal and DseCDl was this HlassiCiHation that ithas AeHome standard. he modeled his nomenHlatDre on his Hategories, sothat the names he minted haKe the great merit oC maLing the relationsAetween the KarioDs genera oC Hiphers eKident on sight. an eYample is theHomplementarF pair ”mono-alphaAet” and ”polFalphaAet”; the CrenHhwere still Halling polFalphaAetiH sFstems AF the almost oACDsHatorF”doDAle sDAstitDtion,” whiHh tells aAsolDtelF nothing at all aAoDt thesFstem. Criedman's most important Hoinage was the word”HrFptanalFsis,” whiHh he deKised in 1920 to Hlear Dp a HhroniH soDrHe oCHonCDsion in HrFptologF—the amAigDitF oC the KerA ”deHipher,” then Dsedto mean Aoth aDthoriMed and DnaDthoriMed redDHtions oC a HrFptogram to plainteYt.he titled his AooL elements oC HrFptanalFsis, and the term has soprospered that todaF it HirHDlates in general HonKersation and print.

- $K \to V$: From the words "proKing" and "howeKer", we can state that $K \to V$.
- $D \to U$, $A \to B$: From the phrase "mDst Ae regarded as" we can tell that $D \to U$ and $A \to B$.

riverbanL **publiHation** no. 22, written in 1920 when Criedman was28, must be regarded as the most important single **publiHation** inHrFptologF. it tooL the sHienHe into a new world. entitled the indeY oCHoinHidenHe and its appliHations in HrFptographF, it desHribed thesolution oC two HompliHated Hipher sFstems. Criedman, however, was lessinterested in proving their vulnerabilitF than he was in using them as avehiHle Cor new methods oC HrFptanalFsis.in it, Criedman devised two new teHhniBues. one was brilliant. itpermitted him to reHonstruHt a primarF Hipher alphabet without havingto guess at a single plainteYt letter. but the other was proCound. Cor theCirst time in HrFptologF, Criedman treated a CreBuenHF distribution as anentitF, as a Hurve whose several points were HausallF 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 onlF be desHribed as promethean, CorCriedman's stroLe oC genius inspired the numerous, varied, and vitalstatistiHal tools that are indispensable to the HrFptologF oC todaF.beCore Criedman, HrFptologF eLed out an eYistenHe as a studF untoitselC, as an isolated phenomenon, neither borrowing Crom norHontributing to other bodies oC Lnowledge. CreBuenHF Hounts, linguistiHHharaHteristiHs, LasisLi eYaminations—all were peHuliar and partiHular toHrFptologF. it dwelt a reHluse in the world oC sHienHe. Criedman ledHrFptologF out oC this lonelF wilderness and into the broad riHh domain oCstatistiHs. he HonneHted HrFptologF to mathematiHs. the sense oCeYpanding horiMons must have resembled that Celt bF Hhemists whenCriedriHh wohler sFnthesiMed urea, demonstrating that liCe proHessesoperate under well Lnown HhemiHal laws and are thereCore subEeHt toeYperimentation and Hontrol, and leading to todaF's vast strides inbioHhemistrF. when Criedman subsumed HrFptanalFsis under statistiHs, he liLewise Clung wide the door to anarmamentarium to whiHh HrFptologF had never beCore had aHHess. itsweapons—measures oC Hentral tendenHF and dispersion, oC Cit andsLewness, oC probabilitF and sampling and signiCiHanHe—were ideallFCashioned to deal with the statistiHal behavior oC letters and words.HrFptanalFsts, seiMing them with alaHritF, have wielded them withnotable suHHess ever sinHe.this is whF 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 onlF the beginning. he and mrs. Criedman Buit riverbanL near the end oC 1920. thesituation had beHome intolerable. CabFan 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 everFattempt to do so and had embarrassed Criedman into apparentlFaHBuiesHent silenHe at lantern-slide leHtures on the subEeHt. on EanuarF1, 1921, Criedman began a siY-month HontraHt with the signal Horps todevise HrFptosFstems. when it eYpired, he was taLen on the Hivil-serviHepaFroll oC the war department at $4,500 a Fear.one oC his Cirst assignments was to teaHh a Hourse in militarF Hodesand Hiphers at the signal sHhool, then at Hamp alCred vail, new EerseF.Cor this he wrote a teYtbooL that, Cor the Cirst time, imposed order uponthe Hhaos oC Hipher sFstems and their terminologF. these had sproutedin a bewildering varietF, 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 theHomplementarF pair "mono-alphabet" and **"polFalphabet";** the CrenHhwere still Halling polFalphabetiH sFstems bF the almost obCusHatorF"double substitution," whiHh tells absolutelF nothing at all about thesFstem. Criedman's most important Hoinage was the word"HrFptanalFsis," whiHh he devised in 1920 to Hlear up a HhroniH sourHe oCHon-Cusion in HrFptologF—the ambiguitF oC the verb "deHipher," then usedto mean both authoriMed and unauthoriMed reduHtions oC a HrFptogram to plainteYt.he titled his booL elements oC HrFptanalFsis, and the term has soprospered that todaF it HirHulates in general Honversation and print.

- $H \to C$: From the word "publiHation", we can state that $H \to C$.
- $C \to F$: From the words "oC" and "useCul", we can state that $C \to F$.
- $F \to Y$: From the word "polFalphabet", we can state that $F \to Y$.
- $Y \to X$: From the phrase "an eYample is" we can tell that $Y \to X$.
- $M \to Z$: From the word "unauthoriMed", we can state that $M \to Z$.

riverbanL publication no. 22, written in 1920 when friedman was28, must be regarded as the most important single publication incryptology. it tooL 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 techniBues. 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 freBuency distribution as anentity, as a curve whose several points were causally 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 only be described as promethean, forfriedman's stroLe of genius inspired the numerous, varied, and vitalstatistical tools that are indispensable to the cryptology of today.before friedman, cryptology eLed out an existence as a study untoitself, as an isolated phenomenon, neither borrowing from norcontributing to other bodies of **Lnowledge**. **freBuencyZ** counts, linguisticcharacteristics, LasisLi 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 Lnown chemical laws and are therefore subEect toexperimentation and control, and leading to today's vast strides inbiochemistry. when friedman subsumed cryptanalysis under statistics, he **liLewise** flung wide the door to anarmamentarium to which cryptology had never before had access. itsweapons—measures of central tendency and dispersion, of fit andsLewness, 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 looLing bacL 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 Buit riverbanL near the end of 1920. thesituation had become intolerable. fabyan had lured him bacL after thewar with raises and promises of absolute freedom to prove or disprovethe existence of ciphers in shaLespeare. but he had sBuelched everyattempt to do so and had embarrassed friedman into apparentlyacBuiescent silence at lantern-slide lectures on the **subEect**. on **Eanuary1**, 1921, friedman began a six-month contract with the signal corps todevise cryptosystems. when it expired, he was taLen 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 Eersey.for this he wrote a textbooL 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 maLing 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 booL elements of cryptanalysis, and the term has soprospered that today it circulates in general conversation and print.

- $L \to K$: From the words “Lnowledge” and “liLewise”, we can state that $L \to K$.
- $B \to Q$: From the word “freBuency”, we can state that $B \to Q$.
- $E \to J$: And the last letter, from the words “subEect” and “Eanuary1”, we can state that $E \to J$.

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.

Now we can state that there are some missing spaces to make the decryption harder.

4. Conclusions and Insights Gained

- The weak point of any monoalphabetic ciphering system is frequency analysis
- The frequency of certain letters, digraphs, trigraths and frequently used words (I, a, the) are the key to deciphering such a system
- To minimize the effectiveness of frequency analysis, messages must be kept short, each using a different substitution
- Also, removing spaces is a good practice to prevent certain words from being easily identified
- Frequency analysis relies on subtle properties of language, which makes human involvement essential for making informed decisions about letter substitutions.

Appendix. Program Code

```
//LetterFrequencyCharts.java
package task_1;

import org.jfree.chart.ChartFactory;
import org.jfree.chart.ChartPanel;
import org.jfree.chart.JFreeChart;
import org.jfree.chart.plot.PlotOrientation;
import org.jfree.data.category.DefaultCategoryDataset;

import javax.swing.*;
import java.awt.*;
import java.util.*;
import java.util.stream.Collectors;

public class LetterFrequencyCharts extends JFrame {

    public LetterFrequencyCharts(Map<Character, Double> data1, String tit
                                 Map<Character, Double> data2, String tit

        // Create sorted datasets
        DefaultCategoryDataset dataset1 = createDataset(sortData(data1, s
        DefaultCategoryDataset dataset2 = createDataset(sortData(data2, s

        // Create charts
        JFreeChart chart1 = ChartFactory.createBarChart(
                title1, "Letter", "Frequency (%)", dataset1,
                PlotOrientation.VERTICAL, false, true, false);

        JFreeChart chart2 = ChartFactory.createBarChart(
                title2, "Letter", "Frequency (%)", dataset2,
                PlotOrientation.VERTICAL, false, true, false);
        // Place charts side by side
        JPanel panel = new JPanel(new GridLayout(1, 2)); // 1 row, 2 colu
        panel.add(new ChartPanel(chart1));
        panel.add(new ChartPanel(chart2));

        setContentPane(panel);
        setTitle("Letter Frequency Comparison");
        setSize(1200, 600);
        setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
        setLocationRelativeTo(null);
    }

    /** Sort data alphabetically or by frequency descending */
    private Map<Character, Double> sortData(Map<Character, Double> data,
        return data.entrySet().stream()
                .sorted(alphabetical
                        ? Map.Entry.comparingByKey()
                        : Map.Entry.<Character, Double>comparingByValue()
                .collect(Collectors.toMap(
                        Map.Entry::getKey,
                        Map.Entry::getValue,
                        (a, b) -> a,
                        LinkedHashMap::new
                ));
    }

    private DefaultCategoryDataset createDataset(Map<Character, Double> d
        DefaultCategoryDataset dataset = new DefaultCategoryDataset();
        for (Map.Entry<Character, Double> entry : data.entrySet()) {
            dataset.addValue(entry.getValue(), "Frequency", entry.getKey(
        }
        return dataset;
    }
    /** Build map using char[] instead of String[] */
    public static Map<Character, Double> buildMap(char[] letters, double[
        Map<Character, Double> map = new LinkedHashMap<>();
        for (int i = 0; i < letters.length; i++) {
            map.put(letters[i], frequencies[i]);
        }
        return map;
    }
}




//Main.java
package task_1;

import javax.swing.*;
import java.util.Map;

import static task_1.LetterFrequencyCharts.buildMap;

public class Main {
    public static void main(String[] args) {
        // --- English letter frequencies ---
        char[] lettersEnglish = {’A’,’B’,’C’,’D’,’E’,’F’,’G’,’H’,’I’,’J’,
                ’N’,’O’,’P’,’Q’,’R’,’S’,’T’,’U’,’V’,’W’,’X’,’Y’,’Z’};
        double[] freqEnglish = {8.17,1.49,2.78,4.25,12.7,2.23,2.01,6.09,6
                0.77,4.03,2.41,6.75,7.51,1.93,0.09,5.99,6.33,9.06,
                2.76,0.98,2.36,0.15,1.97,0.07};
        Map<Character, Double> englishMap = buildMap(lettersEnglish, freq

        // --- Custom text frequencies ---
        char[] letters = {’V’,’W’,’T’,’X’,’P’,’G’,’N’,’I’,’Q’,’O’,’H’,’S’
                ’D’,’C’,’F’,’R’,’A’,’J’,’K’,’L’,’Y’,’B’,’E’,’M’};
        double[] frequencies = {11.7,9.6,8.3,8.0,7.1,7.1,7.0,6.2,4.6,4.1,
                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};
        Map<Character, Double> myTextMap = buildMap(letters, frequencies)

        // --- Show both charts side by side ---
        SwingUtilities.invokeLater(() -> new LetterFrequencyCharts(
                englishMap, "Letter Frequency in English (A{Z)", false,
                myTextMap, "Letter Frequency in My Text", false
        ).setVisible(true));




        String text = """
Ixkviatgl Udasxhtwxng Gn. 22, rixwwvg xg 1920 rqvg Cixvoztg rtp28, zdpw a
xzuniwtgw pxgjsv udasxhtwxng xghifuwnsnjf. Xw wnnl wqv phxvghv xgwn t gvr
Wqv Xgovy ncHnxghxovghv tgo Xwp Tuusxhtwxngp xg Hifuwnjituqf, xw ovphixav
nc wrn hnzusxhtwvo hxuqvi pfpwvzp. Cixvoztg, qnrvkvi, rtp svppxgwvivpwvo
kdsgvitaxsxwf wqtg qv rtp xg dpxgj wqvz tp tkvqxhsv cni gvr zvwqnop nc hi
Cixvoztg ovkxpvo wrn gvr wvhqgxbdvp. Ngv rtp aixssxtgw. Xwuvizxwwvo qxz w
uixztif hxuqvi tsuqtavw rxwqndw qtkxgjwn jdvpp tw t pxgjsv ustxgwvyw svwww
rtp uincndgo. Cni wqvcxipw wxzv xg hifuwnsnjf, Cixvoztg wivtwvo t civbdvg
tgvgwxwf, tp t hdikv rqnpv pvkvits unxgwp rviv htdptssf ivstwvo, gnw tp e
xgoxkxodts svwwvip wqtw qtuuvg wn pwtgo xg t hviwtxg niovicni gnghtdpts (
tgo wn wqxp hdikv qv tuusxvo pwtwxpwxhtshnghvuwp. Wqv ivpdswp htg ngsf av
Uinzvwqvtg, cniCixvoztg’p pwinlv nc jvgxdp xgpuxivo wqv gdzvindp, ktixvo,
kxwtspwtwxpwxhts wnnsp wqtw tiv xgoxpuvgptasv wn wqv hifuwnsnjf nc wnotf.
hifuwnsnjf vlvo ndw tg vyxpwvghv tp t pwdof dgwnxwpvsc, tp tg xpnstwvo uq
aniinrxgj cinz gnihngwixadwxgj wn nwqvi anoxvp nc lgnrsvojv. Civbdvghf hn
sxgjdxpwxhhqtithwvixpwxhp, Ltpxplx vytzxgtwxngp|tss rviv uvhdsxti tgo uti
wnhifuwnsnjf. Xw orvsw t ivhsdpv xg wqv rniso nc phxvghv. Cixvoztg svohif
sngvsf rxsovigvpp tgo xgwn wqv ainto ixhq onztxg ncpwtwxpwxhp. Qv hnggvhw
ztwqvztwxhp. Wqv pvgpv ncvyutgoxgj qnixmngp zdpw qtkv ivpvzasvo wqtw cvsw
rqvgCixvoixhq Rnqsvi pfgwqvpxmvo divt, ovzngpwitwxgj wqtw sxcv uinhvppvpn
lgnrg hqvzxhts strp tgo tiv wqvivcniv pdaevhw wnvyuvixzvgwtwxng tgo hngwi
wnotf’p ktpw pwixovp xgaxnhqvzxpwif. Rqvg Cixvoztg pdapdzvo hifuwtgtsfpxp
```

```
pwtwxpwxhp, qv sxlvrxpv csdgj rxov wqv onni wn tgtiztzvgwtixdz wn rqxhq h
avcniv qto thhvpp. Xwprvtungp|zvtpdivp nc hvgwits wvgovghf tgo oxpuvipxng
tgoplvrgvpp, nc uinataxsxwf tgo ptzusxgj tgo pxjgxcxhtghv|rviv xovtssfctp
wqv pwtwxpwxhts avqtkxni nc svwwvip tgo rniop.Hifuwtgtsfpwp, pvxmxgj wqvz
qtkv rxvsovo wqvz rxwqgnwtasv pdhhvpp vkvi pxghv.Wqxp xp rqf Cixvoztg qtp
athl nkvi qxp htivvi, wqtwWqv Xgovy nc Hnxghxovghv rtp qxp jivtwvpw pxgjs
rndsoqtkv rng qxz qxp ivudwtwxng. Adw xg cthw xw rtp ngsf wqv avjxggxgj.
bdxw Ixkviatgl gvti wqv vgo nc 1920. Wqvpxwdtwxng qto avhnzv xgwnsvitasv.
athl tcwvi wqvrti rxwq itxpvp tgo uinzxpvp nc tapnsdwv civvonz wn uinkv n
vyxpwvghv nc hxuqvip xg Pqtlvpuvtiv. Adw qv qto pbdvshqvo vkviftwwvzuw wn
vzatiitppvo Cixvoztg xgwn tuutivgwsfthbdxvphvgw pxsvghv tw stgwvig-psxov
pdaevhw. Ng Etgdtif1, 1921, Cixvoztg avjtg t pxy-zngwq hngwithw rxwq wqv
wnovkxpv hifuwnpfpwvzp. Rqvg xw vyuxivo, qv rtp wtlvg ng wqv hxkxs-pvikxh
Ovutiwzvgw tw $4,500 t fvti.Ngv nc qxp cxipw tppxjgzvgwp rtp wn wvthq t h
hnovptgo hxuqvip tw wqv Pxjgts Phqnns, wqvg tw Htzu Tscivo Ktxs, Gvr Evip
t wvywannl wqtw, cni wqv cxipw wxzv, xzunpvo niovi dungwqv hqtnp nc hxuqv
wvizxgnsnjf. Wqvpv qto puindwvoxg t avrxsovixgj ktixvwf, tgo rixwvip wivt
tgopuvhxts htpvp. Cixvoztg pniwvo wqvz ndw ng wqv atpxp nc pwidhwdivxgpwv
pn snjxhts tgo dpvcds rtp wqxp hstppxcxhtwxng wqtw xwqtp avhnzv pwtgotio.
gnzvghstwdiv ng qxp htwvjnixvp, pnwqtw wqv gtzvp qv zxgwvo qtkv wqv jivtw
ivstwxngpavwrvvg wqv ktixndp jvgvit nc hxuqvip vkxovgw ng pxjqw. Tg vytzu
wqvhnzusvzvgwtif utxi "zngn-tsuqtavw" tgo "unsftsuqtavw"; wqv Civghqrviv
unsftsuqtavwxh pfpwvzp af wqv tsznpw nacdphtwnif"ondasv pdapwxwdwxng," rq
tapnsdwvsf gnwqxgj tw tss tandw wqvpfpwvz. Cixvoztg’p znpw xzuniwtgw hnxg
rnio"hifuwtgtsfpxp," rqxhq qv ovkxpvo xg 1920 wn hsvti du t hqingxh pndih
hifuwnsnjf|wqv tzaxjdxwf nc wqv kvia "ovhxuqvi," wqvg dpvown zvtg anwq td
dgtdwqnixmvo ivodhwxngp nc t hifuwnjitz wn ustxgwvyw.Qv wxwsvo qxp annl V
Hifuwtgtsfpxp, tgo wqv wviz qtp pnuinpuvivo wqtw wnotf xw hxihdstwvp xg j
tgo uixgw.
""";


        System.out.println("To better tell which letters were already rep
        text = text.toUpperCase();
        //System.out.println(text);
        System.out.println(" V -> e: Since in English the frequency of E
        text = text.replace(’V’, ’e’);
        //System.out.println(text);



        System.out.println("W -> t, Q -> h, WGe -> the: The trigraphs WQV
        text = text.replace(’W’, ’t’);
        text = text.replace(’Q’, ’h’);
        //System.out.println(text);

        System.out.println("T -> a, G -> n, O -> D, TGO -> and: The 2nd m
        text = text.replace(’T’, ’a’);
        text = text.replace(’G’, ’n’);
        text = text.replace(’O’, ’d’);
        //System.out.println(text);

        System.out.println("N -> o, nN. -> no.: In text we have \"nN. 22\
        text = text.replace(’N’, ’o’);
        //System.out.println(text);

        System.out.println("X -> i, Xn -> in: Another telling instance is
        text = text.replace(’X’, ’i’);
        //System.out.println(text);

        System.out.println("P -> s: From the phrase \"thiP iP ... haP Pai
        text = text.replace(’P’, ’s’);
        //System.out.println(text);

        System.out.println("R -> w: From the words \"neR\" and \"Ras\", w
        text = text.replace(’R’, ’w’);
        //System.out.println(text);

        System.out.println("Z -> m: From the words \"hiZ\", \"Zost\" and
        text = text.replace(’Z’, ’m’);

        System.out.println("I -> r: From the context \"wIitten in 1920\"
        text = text.replace(’I’, ’r’);
        //System.out.println(text);

        System.out.println("J -> g,  U -> p: From the context \"Ae reJard
        text = text.replace(’J’, ’g’);
        text = text.replace(’U’, ’p’);

        System.out.println("S -> l: From the words \"entitSed\" and \"sin
        text = text.replace(’S’, ’l’);
        //System.out.println(text);

        System.out.println("K -> v: From the words \"proKing\" and \"howe
        text = text.replace(’K’, ’v’);

        System.out.println("D -> u, A -> b\": From the phrase \"mDst Ae r
        text = text.replace(’D’, ’u’);
        text = text.replace(’A’, ’b’);
        //System.out.println(text);

        System.out.println("H -> c: From the word \"publiHation\", we can
        text = text.replace(’H’, ’c’);

        System.out.println("C -> f: From the words \"oC\" and \"useCul\",
        text = text.replace(’C’, ’f’);

        System.out.println("F -> y: From the word \"polFalphabet\", we ca
        text = text.replace(’F’, ’y’);

        System.out.println("Y -> x: From the phrase \"an eYample is\" we
        text = text.replace(’Y’, ’x’);
```

```
        System.out.println("M -> z: From the word \"unauthoriMed\", we ca
        text = text.replace('M', 'z');
        //System.out.println(text);

        System.out.println("L -> k: From the words \"Lnowledge\" and \"li
        text = text.replace('L', 'k');

        System.out.println("B -> q: From the word \"freBuency\", we can s
        text = text.replace('B', 'q');

        System.out.println("E -> j: And the last letter, from the words \
        text = text.replace('E', 'j');
        System.out.println(text);




    }
```