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
Cryptanalysis of mono-alphabetic ciphers

Elaborated:
st. gr. FAF-213 Botnari Ciprian

Verified:
asist. univ. Cătălin Mîțu

Chişinău – 2023

Table of Contents

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 weakness of mono-alphabetic encryption systems lies in the frequency of occurrence of characters in the text. If an encrypted text is long enough and the language in which the plaintext is written is known, the system can be broken by an attack based on the frequency of occurrence of letters in a language (frequency analysis attack), this frequency being an intensively studied problem (not necessarily for cryptographic purposes) and as a result various ordering structures have been constructed relative to the frequency of occurrence of letters in each European and other languages. Typically, the longer a cipher text is, the closer the frequency of letters used approaches this general ordering. A comparison between the two ordering relationships (that of the characters in the text and that of the letters of the current language alphabet) leads to some correspondences (letter plain text - cipher text letter), which uniquely establishes the encryption key.

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*

Table 1. *Frequency of English letters*

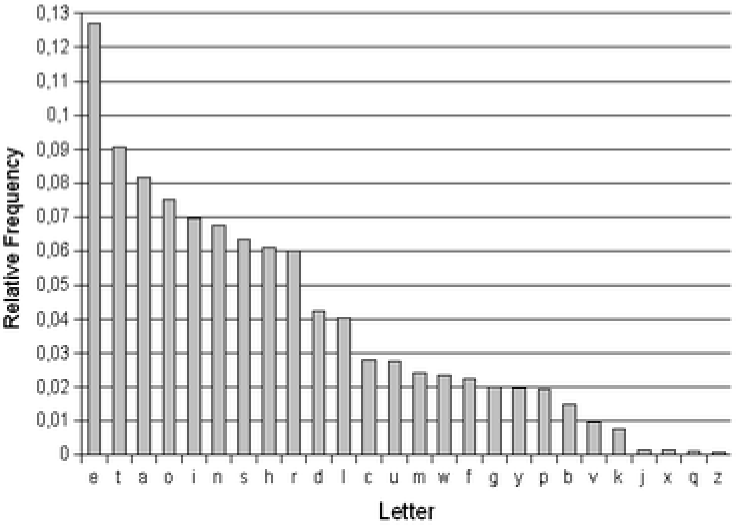


Figure 1. *Frequency of English letters*

We can use information about the frequency of occurrence of letters in a language to try to break a mono-alphabetic substitution cipher. This can be done because, for example, if for a message written in English the letter "E", which has the highest frequency, was encrypted with "X", then every "X" in the encrypted text was an "E" in the plaintext. Therefore, the most common letter in the cipher text should be "X". Thus, if we intercept an encrypted message, and the most common letter in it is "P", we can assume that "P" was used to encrypt "E", and so we can replace all the "P "s with "E". Of course, not every text has exactly the same frequency and, as seen above, "T" and "A" also have high frequencies, so it could be that "P" is one of them. However, it is unlikely to be "Z", which is rarely encountered in English. By repeating this process with the next most frequent letter, we can make progress in cracking a message. If we were to put all the letters in order and replace them according to the frequency table, we would most likely not get the expected result. The cryptanalyst must use other "personality traits" of the letters to crack the cryptogram.

Examination of letter pairs (digraphs), the most common being TH, HE, AN, IN, ER, ON, RE, ED, ND, HA, AT, EN. Triplets (tri-graphs) can also be very useful, the most common of which in English are THE, AND, THA, ENT, ION, TIO, FOR, NDE, HAS, NCE, TIS, OFT, MEN. In addition, in English there are only a few letters that appear as doublets (SS, EE, TT, OO and FF being the most common). There are only two words with a one-letter meaning in English: 'A' and 'I'. Other common words also start to appear as we make some substitutions.

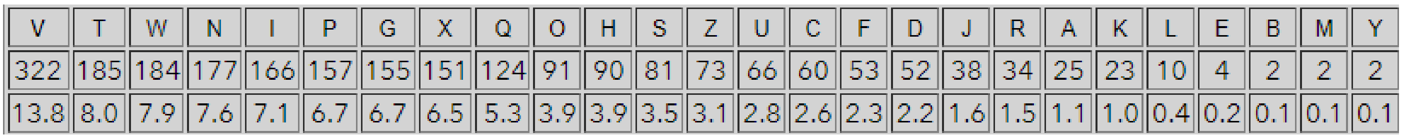
For example, "T*E" may appear frequently after making substitutions for "T" and "E". In this case "T*E" is very likely to be "THE", a very common word in English. The frequency analysis process uses various subtle properties of language, and for this reason it is almost impossible for a computer to do all the work. Inevitably, the element of human input is needed in this process to make informed decisions about which letters to replace.

Implementation

We intercepted a **c** cryptogram, which we know was obtained from the use of a mono-alphabetic cipher over a message written in English:

c = *ZNOVIG RVPWVIG hifuwnsnjf vzvijvo oxivhwsf cinz wqv csnrvixgj ncznovig oxusnzthf. Wqv tzatpptonip' ivuniwp rviv pnzvwxzvp nuvgvotgo ivto, tgo, xc gvhvpptif, hifuw-tgtsfmvo. Af wqv vgo nc wqv hvgwdif,hifuwnsnjf qto avhnzv xzuniwtgw vgndjq cni znpw pwtwvp wn lvvu cdss-wxzv hxuqvi pvhivwtixvp nhhduxvo xg ztlxgj du gvr lvfp, vghxuqvixgj tgoovhxuqvixgj zvpptjvp, tgo pnskxgj xgwvihvuwvo oxputwhqvp. Pnzvwxzvpwqv hifuwtgtsfpwp rviv pvutitwv cinz wqv hxuqvi pvhivwtixvp tgo rvivhtssvo xg ngsf rqvg gvvovo. Uviqtup wqv znpw vstanitwv nijtgxmtwxng rtpKvgxhv'p. Xw cvss dgovi wqv xzzvoxtwv hngwins nc wqv Hndghxs nc Wvg, wqvunrvicds tgo zfpwvixndp anof wqtw idsvo wqv ivudasxh stijvsf wqindjq xwpvccxhxvgw pvhivw unsxhv. Kvgxhv nrvo qvi uivvzxgvghv stijvsf wn JxnktggxPnin, rqn rtp uviqtup wqv Rvpw'p cxipw jivtw hifuwtgtsfpw. Pnin,tuunxgwvo hxuqvi pvhivwtif xg 1506, vgenfvo ivztiltasv pdhhvpp xgpnskxgj wqv hxuqvip nc gdzvindp uixghxutsxwxvp. Qxp pnsdwxng nc t oxputwhqnc Ztil Tgwqngf Hnsntgt, hqxvc nc wqv tizf nc wqv Qnsf Inztg VzuviniZtyxzxsxtg X, ivbdvpwxgj 20,000 odhtwp ni wqv uivpvghv nc wqv vzuvinirxwq wqv tizf, jtkv tg xgpxjqw xgwn Hnsnggt'p uinasvzp. Pn jivtw rtpPnin'p ctzv wqtw nwqvi hndiwp pqtiuvgvo wqvxi hxuqvip, tgo tp vtisf tp1510 wqv ututs hdixt rtp pvgoxgj qxz hxuqvip wqtw gn ngv xg Inzv hndsopnskv. Adw Kvgxhv qto gn zngnunsf. Xg 1589, Qvgif nc Gtktiiv, rqn rtp ovpwxgvo wn avhnzv wqv znpwunudsti lxgj xg wqv qxpwnif nc Citghv (qv hnxgvo wqv psnjtg "T hqxhlvg xgvkvif uvtptgw'p unw vkvif Pdgotf"), tphvgovo wn wqv wqingv tp Qvgif XKtgo cndgo qxzpvsc vzainxsvo pwxss zniv cxvihvsf xg qxp axwwvi hngwvpwrxwq wqv Qnsf Svtjdv, t Htwqnsxh cthwxng wqtw ivcdpvo wn hnghvov wqtw tUinwvpwtgw hndso rvti wqv hinrg. Wqv Svtjdv, qvtovo af wqv Odlv ncZtfvggv, qvso Utixp tgo tss wqv nwqvi stijv hxwxvp nc Citghv, tgo rtpivhvxkxgj stijv witgpcdpxngp nc zvg tgo zngvf cinz Uqxsxu nc Putxg.Qvgif rtp wxjqwsf qvzzvo xg, tgo xw rtp tw wqxp edghwdiv wqtw pnzvhniivpungovghv avwrvvg Uqxsxu tgo wrn nc qxp sxtxpng nccxhvip,Hnzztgovi Edtg ov Znivn tgo Tzatpptoni Ztgnppv, cvss xgwn Qvgif'pqtgop.Xw rtp xg hxuqvi, adw qv qto xg qxp jnkvigzvgw tw wqv wxzv ngvCitghnxp Kxvwv, wqv pvxjgvdi ov st Axjnwxviv, t 49-fvti-nso strfvi cinzUnxwnd rqn qto ixpvg wn avhnzv hndgpvsni nc wqv utisvzvgw, ni hndiw ncedpwxhv, nc Wndip tgo t uixkf hndgpvsni wn Qvgif. Kxvwv qto cni fvtiptzdpvo qxzpvsc rxwq ztwqvztwxhp tp t qnaaf—"Gvkvi rtp t ztg znivanig cni ztwqvztwxhp," ptxo Wtssvzvgw ovp Ivtdy. Tp wqv ztg rqn cxipwdpvo svwwvip cni bdtgwxwxvp xg tsjvait, jxkxgj wqtw pwdof xwp hqtithwvixpwxhsnnl, Kxvwv xp wnotf ivzvzavivo tp wqv Ctwqvi nc Tsjvait. T fvti avcniv,qv qto pnskvo t Putgxpq oxputwhq tooivppvo wn Tsvpptgoin Ctigvpv, wqvOdlv nc Utizt, rqn qvtovo wqv Putgxpq cnihvp nc wqv Svtjdv. Qvgifwdigvo wqv gvr xgwvihvuwp nkvi wn qxz wn pvv xc Kxvwv hndso ivuvtw qxppdhhvpp.*

The first step is to find the frequencies of all the letters that appear in the cryptogram, as shown in Table 2.1.



V	T	W	N	I	P	G	X	Q	O	H	S	Z	U	C	F	D	J	R	A	K	L	E	B	M	Y
322	185	184	177	166	157	155	151	124	91	90	81	73	66	60	53	52	38	34	25	23	10	4	2	2	2
13.8	8.0	7.9	7.6	7.1	6.7	6.7	6.5	5.3	3.9	3.9	3.5	3.1	2.8	2.6	2.3	2.2	1.6	1.5	1.1	1.0	0.4	0.2	0.1	0.1	0.1

Table 2.1. *Frequency of cryptogram letters*

Now that we have all the letter frequencies in the ciphertext, we can start making some substitutions. We see that the most frequent letter in the ciphertext is "V" followed by "T" and "W". From the figure above and tables 2.1 , we can guess that first letter represents "e". For "t", and "a" the situation is a little bit more complicated, since the frequency is extremely close. If we replace „T” with „t” and „W” with „a” we get:

*ZNOeIG RePaeIG HIFUaNSNJF eZeIJeO OXIeHaSF CINZ aQe CSNReIXGJ NCZNOeIG OXUSNZtHF. aQe tZAtPPtONIP' IeUNIaP ReIe PNZeaXZeP NUeGeOtGO IetO, tGO, XC GeHePPtIF, HIFUa-tGtSFMeO. AF aQe eGO NC aQe HeGaDIF,HIFUaNSNJF QtO AeHNZe XZUNIatGa eGNDJQ CNI ZNPa PataeP aN LeeU CDSS-aXZe HXUQeI PeHIeatIXeP NHHDUXeO XG ZtLXGJ DU GeR LeFP, eGHXUQeIXGJ tGOOeHXUQeIXGJ ZePPtJeP, tGO PNSKXGJ XGaeIHeUaeO OXPUtaHQeP. PNZeaXZePaQe HIFUatGtSFPaP ReIe PeUtItae CINZ aQe HXUQeI PeHIeatIXeP tGO ReIeHtSSeO XG NGSF RQeG GeeOeO. UeIQtUP aQe ZNPa eStANItae NIJtGXMtaXNG RtPKeGXHe'P. Xa CeSS DGOeI aQe XZZeOXtae HNGaINS NC aQe HNDGHXS NC aeG, aQeUNReICDS tGO ZFPaeIXNDP ANOF aQta IDSeO aQe IeUDASXH StIJeSF aQINDJQ XaPeCCXHXeGa PeHIea UNSXHe. KeGXHe NReO QeI UIeeZXGeGHe StIJeSF aN JXNKtGGXPNIN, RQN RtP UeIQtUP aQe RePa'P CXIPa JIeta HIFUatGtSFPa. PNIN,tUUNXGaeO HXUQeI PeHIeatIF XG 1506, eGENFeO IeZtILtASe PDHHePP XGPNSKXGJ aQe HXUQeIP NC GDZeINDP UIXGHXUtSXaXeP. QXP PNSDaXNG NC **t** OXPUtaHQNC ZtIL tGaQNGF HNSNtGt, HQXeC NC aQe tIZF NC aQe QNSF INZtG eZUeINIZtYXZXSXtG X, IeBDePaXGJ 20,000 ODHtaP NI aQe UIePeGHe NC aQe eZUeINIRXaQ aQe tIZF, JtKe tG XGPXJQa XGaN HNSNGGt'P UINASeZP. PN JIeta RtPPNIN'P CtZe aQta NaQeI HNDIaP PQtIUeGeO aQeXI HXUQeIP, tGO tP etISF tP1510 aQe UtUtS HDIXt RtP PeGOXGJ QXZ HXUQeIP aQta GN NGe XG INZe HNDSOPNSKe. ADa KeGXHe QtO GN ZNGNUNSF. XG 1589, QeGIF NC GtKtIIe, RQN RtP OePaXGeO aN AeHNZe aQe ZNPaUNUDStI LXGJ XG aQe QXPaNIF NC CItGHe (Qe HNXGeO aQe PSNJtG "**t** HQXHLeG XGeKeIF UetPtGa'P UNa eKeIF PDGOtF"), tPHeGOeO aN aQe aQINGe tP QeGIF XKtGO CNDGO QXZPeSC eZAINXSeO PaXSS ZNIe CXeIHeSF XG QXP AXaaeI HNGaePaRXaQ aQe QNSF SetJDe**, t** HtaQNSXH CtHaXNG aQta IeCDPeO aN HNGHeOe aQta tUINaePatGa HNDSO RetI aQe HINRG. aQe SetJDe, QetOeO AF aQe ODLe NCZtFeGGe, QeSO UtIXP tGO tSS aQe NaQeI StIJe HXaXeP NC CItGHe, tGO RtPIeHeXKXGJ StIJe aItGPCDPXNGP NC ZeG tGO ZNGeF CINZ UQXSXU NC PUtXG.QeGIF RtP aXJQaSF QeZZeO XG, tGO Xa RtP ta aQXP EDGHaDIe aQta PNZeHNIIePUNGOeGHe AeaReeG UQXSXU tGO aRN NC QXP SXtXPNG NCCXHeIP,HNZZtGOeI EDtG Oe ZNIeN tGO tZAtPPtONI ZtGNPPe, CeSS XGaN QeGIF'PQtGOP.Xa RtP XG HXUQeI, ADa Qe QtO XG QXP JNKeIGZeGa ta aQe aXZe NGeCItGHNXP KXeae, aQe PeXJGeDI Oe St AXJNaXeIe**, t** 49-FetI-NSO StRFeI CINZUNXaND RQN QtO IXPeG aN AeHNZe HNDGPeSNI NC aQe UtISeZeGa, NI HNDIa NCEDPaXHe, NC aNDIP tGO **t** UIXKF HNDGPeSNI aN QeGIF. KXeae QtO CNI FetIPtZDPeO QXZPeSC RXaQ ZtaQeZtaXHP tP **t** QNAAF—"GeKeI RtP **t** ZtG ZNIeANIG CNI ZtaQeZtaXHP," PtXO atSSeZeGa OeP IetDY. tP aQe ZtG RQN CXIPaDPeO SeaaeIP CNI BDtGaXaXeP XG tSJeAIt, JXKXGJ aQta PaDOF XaP HQtItHaeIXPaXHSNNL, KXeae XP aNOtF IeZeZAeIeO tP aQe CtaQeI NC tSJeAIt. **t** FetI AeCNIe,Qe QtO PNSKeO **t** PUtGXPQ OXPUtaHQ tOOIePPeO aN tSePPtGOIN CtIGePe, aQeODLe NC UtIZt, RQN QetOeO aQe PUtGXPQ CNIHeP NC aQe SetJDe. QeGIFaDIGeO aQe GeR XGaeIHeUaP NKeI aN QXZ aN Pee XC KXeae HNDSO IeUeta QXPPDHHePP.*

Notice there are some words that are just letter „t”. Since only „a” is a word in English, we adjust the permutations: T → a, W → t. Now the result is:

*ZNOeIG RePteIG HIFUtNSNJF eZeIJeO OXIeHtSF CINZ **tQe** CSNReIXGJ NCZNOeIG OXUSNZaHF. **tQe** aZAaPPaONIP' IeUNItP ReIe PNZetXZeP NUeGeOaGO IeaO, aGO, XC GeHePPaIF, HIFUt-aGaSFMeO. AF **tQe** eGO NC **tQe** HeGtDIF,HIFUtNSNJF QaO AeHNZe XZUNItaGt eGNDJQ CNI ZNPt PtateP **tN** LeeU CDSS-tXZe HXUQeI PeHIetaIXeP NHHDUXeO XG ZaLXGJ DU GeR LeFP, eGHXUQeIXGJ aGOOeHXUQeIXGJ ZePPaJeP, aGO PNSKXGJ XGteIHeUteO OXPUatHQeP. PNZetXZePtQe HIFUtaGaSFPtP ReIe PeUaIate CINZ **tQe** HXUQeI PeHIetaIXeP aGO ReIeHaSSeO XG NGSF RQeG GeeOeO. UeIQaUP **tQe** ZNPt eSaANIate NIJaGXMatXNG RaPKeGXHe'P. Xt CeSS DGOeI **tQe** XZZeOXate HNGtINS NC **tQe** HNDGHXS NC teG, tQeUNReICDS aGO ZFPteIXNDP ANOF tQat IDSeO **tQe** IeUDASXH SaIJeSF tQINDJQ XtPeCCXHXeGt PeHIet UNSXHe. KeGXHe NReO QeI UIeeZXGeGHe*

*SaIJeSF **tN** JXNKaGGXPNIN, RQN RaP UeIQaUP **tQe** RePt'P CXIPt JIeat HIFUtaGaSFPt. PNIN,aUUNXGteO HXUQeI PeHIetaIF XG 1506, eGENFeO IeZaILaASe PDHHePP XGPNSKXGJ **tQe** HXUQeIP NC GDZeINDP UIXGHXUaSXtXeP. QXP PNSDtXNG NC **a** OXPUatHQNC ZaIL aGtQNGF HNSNaGa, HQXeC NC **tQe** aIZF NC **tQe** QNSF INZaG eZUeINIZaYXZXSXaG X, IeBDePtXGJ 20,000 ODHatP NI **tQe** UIePeGHe NC **tQe** eZUeINIRXtQ **tQe** aIZF, JaKe aG XGPXJQt XGtN HNSNGGa'P UINASeZP. PN JIeat RaPPNIN'P CaZe tQat NtQeI HNDItP PQaIUeGeO tQeXI HXUQeIP, aGO aP eaISF aP1510 **tQe** UaUaS HDIXa RaP PeGOXGJ QXZ HXUQeIP tQat GN NGe XG INZe HNDSOPNSKe. ADt KeGXHe QaO GN ZNGNUNSF. XG 1589, QeGIF NC GaKaIIe, RQN RaP OePtXGeO **tN** AeHNZe **tQe** ZNPtUNUDSaI LXGJ XG **tQe** QXPtNIF NC CIaGHe (Qe HNXGeO **tQe** PSNJaG "**a** HQXHLeG XGeKeIF UeaPaGt'P UNt eKeIF PDGOaF"), aPHeGOeO **tN** **tQe** tQINGe aP QeGIF XKaGO CNDGO QXZPeSC eZAINXSeO PtXSS ZNIe CXeIHeSF XG QXP AXtteI HNGtePtRXtQ **tQe** QNSF SeaJDe, **a** HatQNSXH CaHtXNG tQat IeCDPeO **tN** HNGHeOe tQat aUINtePtaGt HNDSO ReaI **tQe** HINRG. **tQe** SeaJDe, QeaOeO AF **tQe** ODLe NCZaFeGGe, QeSO UaIXP aGO aSS **tQe** NtQeI SaIJe HXtXeP NC CIaGHe, aGO RaPIeHeXKXGJ SaIJe tIaGPCDPXNGP NC ZeG aGO ZNGeF CINZ UQXSXU NC PUaXG.QeGIF RaP tXJQtSF QeZZeO XG, aGO Xt RaP at tQXP EDGHtDIe tQat PNZeHNIIePUNGOeGHe AetReeG UQXSXU aGO tRN NC QXP SXaXPNG NCCXHeIP,HNZZaGOeI EDaG Oe ZNIeN aGO aZAaPPaONI ZaGNPPe, CeSS XGtN QeGIF'PQaGOP.Xt RaP XG HXUQeI, ADt Qe QaO XG QXP JNKeIGZeGt at **tQe** tXZe NGeCIaGHNXP KXete, **tQe** PeXJGeDI Oe Sa AXJNtXeIe, **a** 49-FeaI-NSO SaRFeI CINZUNXtND RQN QaO IXPeG **tN** AeHNZe HNDGPeSNI NC **tQe** UaISeZeGt, NI HNDIt NCEDPtXHe, NC tNDIP aGO **a** UIXKF HNDGPeSNI **tN** QeGIF. KXete QaO CNI FeaIPaZDPeO QXZPeSC RXtQ ZatQeZatXHP aP **a** QNAAF— "GeKeI RaP **a** ZaG ZNIeANIG CNI ZatQeZatXHP," PaXO taSSeZeGt OeP IeaDY. aP **tQe** ZaG RQN CXIPtDPeO SetteIP CNI BDaGtXtXeP XG aSJeAIa, JXKXGJ tQat PtDOF XtP HQaIaHteIXPtXHSNNL, KXete XP tNOaF IeZeZAeIeO aP **tQe** CatQeI NC aSJeAIa. **a** FeaI AeCNIe,Qe QaO PNSKeO **a** PUaGXPQ OXPUatHQ aOOIePPeO **tN** aSePPaGOIN CaIGePe, tQeODLe NC UaIZa, RQN QeaOeO **tQe** PUaGXPQ CNIHeP NC **tQe** SeaJDe. QeGIFtDIGeO **tQe** GeR XGteIHeUtP NKeI **tN** QXZ **tN** Pee XC KXete HNDSO IeUeat QXPPDHHePP.*

„the” is the most used word in English, thus we can assume tQe is the and Q is h. Also for „tN” the only possible solution is „to”, therefore N is o. After the updated substituions, the cryptogram is:

*ZoOeIG RePteIG HIFUtoSoJF eZeIJeO OXIeHtSF CIoZ the CSoReIXGJ oCZoOeIG OXUSoZaHF. the aZAaPPaOoIP' IeUoItP ReIe PoZetXZeP oUeGeOaGO IeaO, aGO, XC GeHePPaIF, HIFUt-aGaSFMeO. AF the eGO oC the HeGtDIF,HIFUtoSoJF haO AeHoZe XZUoItaGt eGoDJh CoI ZoPt PtateP to LeeU CDSS-tXZe HXUheI PeHIetaIXeP oHHDUXeO XG ZaLXGJ DU GeR LeFP, eGHXUheIXGJ aGOOeHXUheIXGJ ZePPaJeP, aGO PoSKXGJ XGteIHeUteO OXPUatHheP. PoZetXZePthe HIFUtaGaSFPtP ReIe PeUaIate CIoZ the HXUheI PeHIetaIXeP aGO ReIeHaSSeO XG oGSF RheG GeeOeO. UeIhaUP the ZoPt eSaAoIate oIJaGXMatXoG RaPKeGXHe'P. **Xt** CeSS DGOeI the XZZeOXate HoGtIoS oC the HoDGHXS oC teG, theUoReICDS aGO ZFPteIXoDP AoOF that IDSeO the IeUDASXH SaIJeSF thIoDJh XtPeCCXHXeGt PeHIet UoSXHe. KeGXHe oReO heI UIeeZXGeGHe SaIJeSF to JXoKaGGXPoIo, **Rho** RaP UeIhaUP the RePt'P CXIPt JIeat HIFUtaGaSFPt. PoIo,aUUoXGteO HXUheI PeHIetaIF XG 1506, eGEoFeO IeZaILaASe PDHHePP XGPoSKXGJ the HXUheIP oC GDZeIoDP UIXGHXUaSXtXeP. hXP PoSDtXoG oC a OXPUatHhoC ZaIL aGthoGF HoSoaGa, HhXeC oC the aIZF oC the hoSF IoZaG eZUeIoIZaYXZXSXaG X, IeBDePtXGJ 20,000 ODHatP oI the UIePeGHe oC the eZUeIoIRXth the aIZF, JaKe aG XGPXJht XGto HoSoGGa'P UIoASeZP. Po JIeat RaPPoIo'P CaZe that **otheI** HoDItP PhaIUeGeO theXI HXUheIP, aGO aP eaISF aP1510 the UaUaS HDIXa RaP PeGOXGJ hXZ HXUheIP that Go **oGe** XG IoZe HoDSOPoSKe. ADt KeGXHe haO Go ZoGoUoSF. XG 1589, heGIF oC GaKaIIe, **Rho** RaP OePtXGeO to AeHoZe the ZoPtUoUDSaI LXGJ XG the hXPtoIF oC CIaGHe (he HoXGeO the PSoJaG "a HhXHLeG XGeKeIF UeaPaGt'P Uot eKeIF PDGOaF"), aPHeGOeO to the thIoGe aP heGIF XKaGO CoDGO hXZPeSC eZAIoXSeO PtXSS ZoIe CXeIHeSF XG hXP AXtteI HoGtePtRXth the hoSF SeaJDe, a HathoSXH CaHtXoG that IeCDPeO to HoGHeOe that aUIotePtaGt HoDSO ReaI the HIoRG. the SeaJDe, heaOeO AF the ODLe oCZaFeGGe, heSO UaIXP aGO aSS the **otheI** SaIJe HXtXeP oC CIaGHe, aGO RaPIeHeXKXGJ SaIJe tIaGPCDPXoGP oC ZeG aGO ZoGeF CIoZ UhXSXU oC PUaXG.heGIF RaP tXJhtSF heZZeO XG, aGO **Xt** RaP at thXP EDGHtDIe that PoZeHoIIePUoGOeGHe AetReeG UhXSXU aGO tRo oC hXP SXaXPoG oCCXHeIP,HoZZaGOeI EDaG Oe ZoIeo aGO aZAaPPaOoI ZaGoPPe, CeSS XGto heGIF'PhaGOP.**Xt** RaP*

*XG HXUheI, ADt he haO XG hXP JoKeIGZeGt at the tXZe oGeCIaGHoXP KXete, the PeXJGeDI Oe Sa AXJotXeIe, a 49-FeaI-oSO SaRFeI CIoZUoXtoD **Rho** haO IXPeG to AeHoZe HoDGPeSoI oC the UaISeZeGt, oI HoDIt oCEDPtXHe, oC toDIP aGO a UIXKF HoDGPeSoI to heGIF. KXete haO CoI FeaIPaZDPeO hXZPeSC RXth ZatheZatXHP aP a hoAAF—"GeKeI RaP a ZaG ZoIeAoIG CoI ZatheZatXHP," PaXO taSSeZeGt OeP IeaDY. aP the ZaG **Rho** CXIPtDPeO SetteIP CoI BDaGtXtXeP XG aSJeAIa, JXKXGJ that PtDOF XtP HhaIaHteIXPtXHSooL, KXete XP toOaF IeZeZAeIeO aP the CatheI oC aSJeAIa. a FeaI AeCoIe,he haO PoSKeO a PUaGXPh OXPUatHh aOOIePPeO to aSePPaGOIo CaIGePe, theODLe oC UaIZa, **Rho** heaOeO the PUaGXPh CoIHeP oC the SeaJDe. heGIFtDIGeO the GeR XGteIHeUtP oKeI to hXZ to Pee XC KXete HoDSO IeUeat hXPPDHHePP.*

If we follow the frequency, **Xt** becomes obvious „it", as „a" has already been replaced, thus X → i.
For **Rho**, the only that makes sense is who, so R → w.
For **otheI** it's other, so I → r.
For **oGe** it's one, therefore G → n.
After the updated substituions, the cryptogram is:

*ZoOern **wePtern** HrFUtoSoJF eZerJeO OireHtSF CroZ the CSowerinJ oCZoOern OiUSoZaHF. the aZAaPPaOorP' reUortP were PoZetiZeP oUeneOanO reaO, **anO**, **iC** neHePParF, HrFUt-anaSFMeO. AF the enO **oC** the HentDrF,HrFUtoSoJF haO AeHoZe iZUortant enoDJh **Cor** ZoPt PtateP to LeeU CDSS-tiZe HiUher PeHretarieP oHHDUieO in ZaLinJ DU new LeFP, enHiUherinJ anOOeHiUherinJ ZePPaJeP, **anO** PoSKinJ interHeUteO OiPUatHheP. PoZetiZePthe HrFUtanaSFPtP were PeUarate CroZ the HiUher PeHretarieP **anO** wereHaSSeO in onSF when neeOeO. UerhaUP the ZoPt eSaAorate orJaniMation waPKeniHe'P. it CeSS DnOer the iZZeOiate HontroS **oC** the HoDnHiS **oC** ten, theUowerCDS **anO** ZFPterioDP AoOF that rDSeO the reUDASiH SarJeSF throDJh itPeCCiHient PeHret UoSiHe. KeniHe oweO her UreeZinenHe SarJeSF to JioKanniPoro, who waP UerhaUP the wePt'P CirPt Jreat HrFUtanaSFPt. Poro,aUUointeO HiUher PeHretarF in 1506, enEoFeO reZarLaASe PDHHePP inPoSKinJ the HiUherP **oC** nDZeroDP UrinHiUaSitieP. hiP PoSDtion **oC** a OiPUatHhoC ZarL anthonF HoSoana, HhieC **oC** the arZF **oC** the hoSF roZan eZUerorZaYiZiSian i, reBDePtinJ 20,000 ODHatP or the UrePenHe **oC** the eZUerorwith the arZF, JaKe an inPiJht into HoSonna'P UroASeZP. Po Jreat waPPoro'P CaZe that other HoDrtP PharUeneO their HiUherP, **anO** aP earSF aP1510 the UaUaS HDria waP PenOinJ hiZ HiUherP that no one in roZe HoDSOPoSKe. ADt KeniHe haO no ZonoUoSF. in 1589, henrF **oC** naKarre, who waP OePtineO to AeHoZe the ZoPtUoUDSar LinJ in the hiPtorF **oC** CranHe (he HoineO the PSoJan "a HhiHLen ineKerF UeaPant'P Uot eKerF PDnOaF"), aPHenOeO to the throne aP henrF iKanO CoDnO hiZPeSC eZAroiSeO PtiSS Zore CierHeSF in hiP Aitter HontePtwith the hoSF SeaJDe, a HathoSiH CaHtion that reCDPeO to HonHeOe that aUrotePtant HoDSO wear the Hrown. the SeaJDe, heaOeO AF the ODLe oCZaFenne, heSO UariP **anO** aSS the other SarJe HitieP **oC** CranHe, **anO** waPreHeiKinJ SarJe tranPCDPionP **oC** Zen **anO** ZoneF CroZ UhiSiU **oC** PUain.henrF waP tiJhtSF heZZeO in, **anO** it waP at thiP EDnHtDre that PoZeHorrePUonOenHe Aetween UhiSiU **anO** two **oC** hiP SiaiPon oCCiHerP,HoZZanOer EDan Oe Zoreo **anO** aZAaPPaOor ZanoPPe, CeSS into henrF'PhanOP.it waP in HiUher, ADt he haO in hiP JoKernZent at the tiZe oneCranHoiP Kiete, the PeiJneDr Oe Sa AiJotiere, a 49-Fear-oSO SawFer CroZUoitoD who haO riPen to AeHoZe HoDnPeSor **oC** the UarSeZent, or HoDrt oCEDPtiHe, **oC** toDrP **anO** a UriKF HoDnPeSor to henrF. Kiete haO **Cor** FearPaZDPeO hiZPeSC with ZatheZatiHP aP a hoAAF—"neKer waP a Zan ZoreAorn **Cor** ZatheZatiHP," PaiO taSSeZent OeP reaDY. aP the Zan who CirPtDPeO SetterP **Cor** BDantitieP in aSJeAra, JiKinJ that PtDOF itP HharaHteriPtiHSooL, Kiete iP toOaF reZeZAereO aP the Cather **oC** aSJeAra. a Fear AeCore,he haO PoSKeO a PUaniPh OiPUatHh aOOrePPeO to aSePPanOro CarnePe, theODLe **oC** UarZa, who heaOeO the PUaniPh CorHeP **oC** the SeaJDe. henrFtDrneO the new interHeUtP oKer to hiZ to Pee **iC** Kiete HoDSO reUeat hiPPDHHePP.*

For **wePtern** it's western, so P → s.
For **anO** it's and, so O → d.
For **iC, oC, Cor** it's if, of, for so C → f.
After the updated substituions, the cryptogram is:

***Zodern** western HrFUtoSoJF eZerJed direHtSF froZ the fSowerinJ of**Zodern** diUSoZaHF. the **aZAassadors' reUorts** were soZetiZes oUenedand read, and, if **neHessarF**, HrFUt-anaSFMed. AF the end of the HentDrF,HrFUtoSoJF had AeHoZe iZUortant enoDJh for Zost states to LeeU fDSS-tiZe HiUher seHretaries oHHDUied in ZaLinJ DU new LeFs, enHiUherinJ anddeHiUherinJ ZessaJes, and soSKinJ interHeUted disUatHhes. soZetiZesthe HrFUtanaSFsts were seUarate froZ the HiUher seHretaries and wereHaSSed in onSF when needed. UerhaUs the Zost eSaAorate orJaniMation wasKeniHe's. it feSS Dnder the iZZediate HontroS of the HoDnHiS of ten, theUowerfDS and ZFsterioDs AodF that rDSed the reUDASiH SarJeSF throDJh itseffiHient seHret UoSiHe. KeniHe owed her UreeZinenHe SarJeSF to JioKannisoro, who was UerhaUs the west's first Jreat HrFUtanaSFst. soro,aUUointed HiUher seHretarF in 1506, enEoFed reZarLaASe sDHHess insoSKinJ the HiUhers of nDZeroDs UrinHiUaSities. his soSDtion of a disUatHhof ZarL anthonF HoSoana, Hhief of the arZF of the hoSF roZan eZUerorZaYiZiSian i, reBDestinJ 20,000 dDHats or the UresenHe of the eZUerorwith the arZF, JaKe an insiJht into HoSonna's UroASeZs. so Jreat wassoro's faZe that other HoDrts sharUened their HiUhers, and as earSF as1510 the UaUaS HDria was sendinJ hiZ HiUhers that no one in roZe HoDSdsoSKe. ADt KeniHe had no ZonoUoSF. in 1589, henrF of naKarre, who was destined to AeHoZe the ZostUoUDSar LinJ in the historF of franHe (he Hoined the sSoJan "a HhiHLen ineKerF Ueasant's Uot eKerF sDndaF"), asHended to the throne as henrF iKand foDnd hiZseSf eZAroiSed stiSS Zore fierHeSF in his Aitter Hontestwith the hoSF SeaJDe, a HathoSiH faHtion that refDsed to HonHede that aUrotestant HoDSd wear the Hrown. the SeaJDe, headed AF the dDLe ofZaFenne, heSd Uaris and aSS the other SarJe Hities of franHe, and wasreHeiKinJ SarJe transfDsions of Zen and ZoneF froZ UhiSiU of sUain.henrF was tiJhtSF heZZed in, and it was at this EDnHtDre that soZeHorresUondenHe Aetween UhiSiU and two of his Siaison offiHers,HoZZander EDan de Zoreo and aZAassador Zanosse, feSS into henrF'shands.it was in HiUher, ADt he had in his JoKernZent at the tiZe onefranHois Kiete, the seiJneDr de Sa AiJotiere, a 49-Fear-oSd SawFer froZUoitoD who had risen to AeHoZe HoDnseSor of the UarSeZent, or HoDrt ofEDstiHe, of toDrs and a UriKF HoDnseSor to henrF. Kiete had for FearsaZDsed hiZseSf with ZatheZatiHs as a hoAAF—"neKer was a Zan ZoreAorn for ZatheZatiHs," said taSSeZent des reaDY. as the Zan who firstDsed Setters for BDantities in aSJeAra, JiKinJ that stDdF its HharaHteristiHSooL, Kiete is todaF reZeZAered as the father of aSJeAra. a Fear Aefore,he had soSKed a sUanish disUatHh addressed to aSessandro farnese, thedDLe of UarZa, who headed the sUanish forHes of the SeaJDe. henrFtDrned the new interHeUts oKer to hiZ to see if Kiete HoDSd reUeat hissDHHess.*

For **Zodern** it’s modern, so Z → m.
For ***aZAassadors'*** it’s ambassadors’, so A → b.
For **reUorts** it’s reports so U → p.
For **neHessarF** it’s necessary so H → c, F → y.

After the updated substituions, the cryptogram is:

*modern western cryptoSoJy **emerJed directSy** from the fSowerinJ ofmodern dipSomacy. the ambassadors' reports were sometimes openedand read, and, if necessary, crypt-anaSyMed. by the end of the centDry,cryptoSoJy had become important **enoDJh** for most states to Leep fDSS-time cipher secretaries occDpied in maLinJ Dp new Leys, encipherinJ anddecipherinJ messaJes, and soSKinJ intercepted dispatches. sometimesthe cryptanaSysts were separate from the cipher secretaries and werecaSSed in onSy when needed. perhaps the most eSaborate orJaniMation wasKenice's. it feSS Dnder the immediate controS of the coDnciS of ten, thepowerfDS and mysterioDs body that rDSed the repDbSic SarJeSy throDJh itsefficient secret poSice. Kenice owed her preeminence SarJeSy to JioKannisoro, who was perhaps the west's first Jreat cryptanaSyst. soro,appointed cipher secretary in 1506, enEoyed remarLabSe sDccess insoSKinJ the ciphers of nDmeroDs principaSities. his soSDtion of a dispatchof marL anthony coSoana, chief of the army of the hoSy roman emperormaYimiSian i, reBDestinJ 20,000 dDcats or the presence of the emperorwith the army, JaKe an insiJht into coSonna's probSems. so Jreat wassoro's fame that other coDrts sharpened their ciphers, and as earSy as1510 the papaS cDria was sendinJ him ciphers that no one in rome coDSdsoSKe. bDt Kenice had no monopoSy. in 1589, henry of naKarre, who was destined to become the mostpopDSar LinJ in the history of france (he coined the sSoJan "a chicLen ineKery peasant's pot eKery sDnday"), ascended to the throne as henry iKand foDnd himseSf embroiSed stiSS more fierceSy in his bitter contestwith the hoSy SeaJDe, a cathoSic faction that refDsed to concede that aprotestant coDSd wear the crown. the SeaJDe, headed by the* *dDLe ofmayenne, heSd paris and aSS the other SarJe cities of france, and wasreceiKinJ SarJe transfDsions of men and money from phiSip of spain.henry was tiJhtSy hemmed in, and it was at this EDnctDre that somecorrespondence between phiSip and two of his Siaison officers,commander EDan de moreo and ambassador manosse, feSS into henry'shands.it was in cipher, bDt he had in his JoKernment at the time onefrancois Kiete, the seiJneDr de Sa biJotiere, a 49-year-oSd Sawyer frompoitoD who had risen to become coDnseSor of the parSement, or coDrt ofEDstice, of toDrs and a priKy coDnseSor to henry. Kiete had for yearsamDsed himseSf with mathematics as a hobby—"neKer was a man moreborn for mathematics," said taSSement des reaDY. as the man who firstDsed Setters for BDantities in aSJebra, JiKinJ that stDdy its characteristicSooL, Kiete is today remembered as the father of aSJebra. a year before,he had soSKed a spanish dispatch addressed to aSessandro farnese, thedDLe of parma, who headed the spanish forces of the SeaJDe. henrytDrned the new intercepts oKer to him to see if Kiete coDSd repeat hissDccess.*

For **emerJed** it’s emerged, so J → g.
For **directSy** it’s directly, so S → l.
For **enoDJh** it’s enough so D → u.

After the updated substituions, the cryptogram is:

*modern western cryptology emerged directly from the flowering ofmodern diplomacy. the ambassadors' reports were sometimes openedand read, and, if necessary, crypt-**analyMed**. by the end of the century,cryptology had become important enough for most states to Leep full-time cipher secretaries occupied in **maLing** up new Leys, enciphering anddeciphering messages, and solKing intercepted dispatches. sometimesthe cryptanalysts were separate from the cipher secretaries and werecalled in only when needed. perhaps the most elaborate organiMation wasKenice's. it fell under the immediate control of the council of ten, thepowerful and mysterious body that ruled the republic largely through itsefficient secret police. Kenice owed her preeminence largely to gioKannisoro, who was perhaps the west's first great cryptanalyst. soro,appointed cipher secretary in 1506, **enEoyed** remarLable success insolKing the ciphers of numerous principalities. his solution of a dispatchof marL anthony coloana, chief of the army of the holy roman emperormaYimilian i, reBuesting 20,000 ducats or the presence of the emperorwith the army, gaKe an insight into colonna's problems. so great wassoro's fame that other courts sharpened their ciphers, and as early as1510 the papal curia was sending him ciphers that no one in rome couldsolKe. but Kenice had no monopoly. in 1589, henry of naKarre, who was destined to become the mostpopular Ling in the history of france (he coined the slogan "a chicLen in **eKery** peasant's pot **eKery** sunday"), ascended to the throne as henry iKand found himself embroiled still more fiercely in his bitter contestwith the holy league, a catholic faction that refused to concede that aprotestant could wear the crown. the league, headed by the duLe ofmayenne, held paris and all the other large cities of france, and wasreceiKing large transfusions of men and money from philip of spain.henry was tightly hemmed in, and it was at this Euncture that somecorrespondence between philip and two of his liaison officers,commander Euan de moreo and ambassador manosse, fell into henry'shands.it was in cipher, but he had in his goKernment at the time onefrancois Kiete, the seigneur de la bigotiere, a 49-year-old lawyer frompoitou who had risen to become counselor of the parlement, or court ofEustice, of tours and a priKy counselor to henry. Kiete had for yearsamused himself with mathematics as a hobby—"neKer was a man moreborn for mathematics," said tallement des reauY. as the man who firstused letters for Buantities in algebra, giKing that study its characteristiclooL, Kiete is today remembered as the father of algebra. a year before,he had solKed a spanish dispatch addressed to alessandro farnese, theduLe of parma, who headed the spanish forces of the league. henryturned the new intercepts oKer to him to see if Kiete could repeat hissuccess.*

For **analyMed** it’s analyzed, so M → z.
For **maLing** it’s making, so L → k.
For **enEoyed** it’s enjoyed so E → j.
For **eKery** it’s every so K → v.

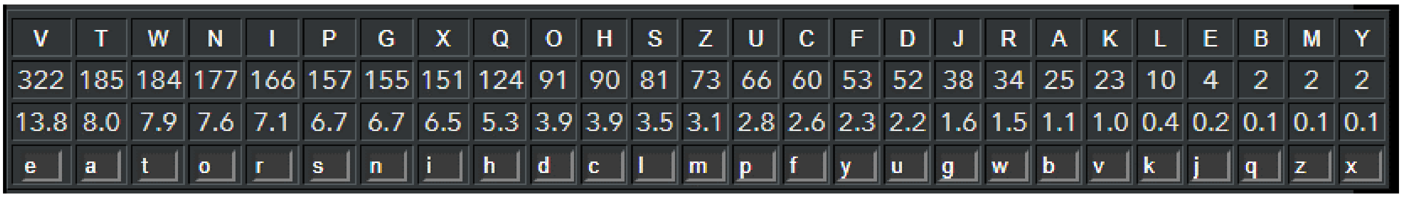
After the updated substituions, the cryptogram is:

*modern western cryptology emerged directly from the flowering ofmodern diplomacy. the ambassadors' reports were sometimes openedand read, and, if necessary, crypt-analyzed. by the end of the century,cryptology had become important enough for most states to keep full-time cipher secretaries occupied in making up new keys, enciphering anddeciphering messages, and solving intercepted dispatches. sometimesthe cryptanalysts were separate from the cipher secretaries and werecalled in only when needed. perhaps the most elaborate organization wasvenice's. it fell under the immediate control of the council of ten, thepowerful and mysterious body that ruled the republic largely through itsefficient secret police. venice owed her preeminence largely to giovannisoro, who was perhaps the west's first great cryptanalyst. soro,appointed cipher secretary in 1506, enjoyed remarkable success insolving the ciphers of numerous principalities. his solution of a dispatchof mark anthony coloana, chief of the army of the holy roman emperor **maYimilian** i, **reBuesting** 20,000 ducats or the presence of the emperorwith the army, gave an insight into colonna's problems. so great wassoro's fame that other courts sharpened their ciphers, and as early as1510 the papal curia was sending him ciphers that no one in rome couldsolve. but venice had no monopoly. in 1589, henry of navarre, who was destined to become the mostpopular king in the history of france (he coined the slogan "a chicken inevery peasant's pot every sunday"), ascended to the throne as henry ivand found himself embroiled still more fiercely in his bitter contestwith the holy league, a catholic faction that refused to concede that aprotestant could wear the crown. the league, headed by the duke ofmayenne, held paris and all the other large cities of france, and wasreceiving large transfusions of men and money from philip of spain.henry was tightly hemmed in, and it was at this juncture that somecorrespondence between philip and two of his liaison officers,commander juan de moreo and ambassador manosse, fell into henry'shands.it was in cipher, but he had in his government at the time onefrancois viete, the seigneur de la bigotiere, a 49-year-old lawyer frompoitou who had risen to become counselor of the parlement, or court ofjustice, of tours and a privy counselor to henry. viete had for yearsamused himself with mathematics as a hobby—"never was a man moreborn for mathematics," said tallement des **reauY**. as the man who firstused letters for **Buantities** in algebra, giving that study its characteristiclook, viete is today remembered as the father of algebra. a year before,he had solved a spanish dispatch addressed to alessandro farnese, theduke of parma, who headed the spanish forces of the league. henryturned the new intercepts over to him to see if viete could repeat hissuccess.*

For **reBuesting, Buantities** it's requesting, quantities so B → q.
For **maYimilian, reauY** it's maximilian, reaux, so Y → x.

After the updated substituions, the final cryptogram is:

modern western cryptology emerged directly from the flowering ofmodern diplomacy. the ambassadors' reports were sometimes openedand read, and, if necessary, crypt-analyzed. by the end of the century,cryptology had become important enough for most states to keep full-time cipher secretaries occupied in making up new keys, enciphering anddeciphering messages, and solving intercepted dispatches. sometimesthe cryptanalysts were separate from the cipher secretaries and werecalled in only when needed. perhaps the most elaborate organization wasvenice's. it fell under the immediate control of the council of ten, thepowerful and mysterious body that ruled the republic largely through itsefficient secret police. venice owed her preeminence largely to giovannisoro, who was perhaps the west's first great cryptanalyst. soro,appointed cipher secretary in 1506, enjoyed remarkable success insolving the ciphers of numerous principalities. his solution of a dispatchof mark anthony coloana, chief of the army of the holy roman emperormaximilian i, requesting 20,000 ducats or the presence of the emperorwith the army, gave an insight into colonna's problems. so great wassoro's fame that other courts sharpened their ciphers, and as early as1510 the papal curia was sending him ciphers that no one in rome couldsolve. but venice had no monopoly. in 1589, henry of navarre, who was destined to become the mostpopular king in the history of france (he coined the slogan "a chicken inevery peasant's pot every sunday"), ascended to the throne as henry ivand found himself embroiled still more fiercely in his bitter contestwith the holy league, a catholic faction that refused to concede that aprotestant could wear the crown. the league, headed by the duke ofmayenne, held paris and all the other large cities of france, and wasreceiving large transfusions of men and money from philip of spain.henry was tightly hemmed in, and it was at this juncture that somecorrespondence between philip and two of his liaison officers,commander juan de moreo and ambassador manosse, fell into henry'shands.it was in cipher, but he had in his government at the time onefrancois viete, the seigneur de la bigotiere, a 49-year-old lawyer *frompoitou who had risen to become counselor of the parlement, or court ofjustice, of tours and a privy counselor to henry. viete had for yearsamused himself with mathematics as a hobby—"never was a man moreborn for mathematics," said tallement des reaux. as the man who firstused letters for quantities in algebra, giving that study its characteristiclook, viete is today remembered as the father of algebra. a year before,he had solved a spanish dispatch addressed to alessandro farnese, theduke of parma, who headed the spanish forces of the league. henryturned the new intercepts over to him to see if viete could repeat hissuccess.*



V	T	W	N	I	P	G	X	Q	O	H	S	Z	U	C	F	D	J	R	A	K	L	E	B	M	Y
322	185	184	177	166	157	155	151	124	91	90	81	73	66	60	53	52	38	34	25	23	10	4	2	2	2
13.8	8.0	7.9	7.6	7.1	6.7	6.7	6.5	5.3	3.9	3.9	3.5	3.1	2.8	2.6	2.3	2.2	1.6	1.5	1.1	1.0	0.4	0.2	0.1	0.1	0.1
e	a	t	o	r	s	n	i	h	d	c	l	m	p	f	y	u	g	w	b	v	k	j	q	z	x

Table 2.2. *The reconstructed alphabet of the encrypted message*

Conclusion

In conclusion, the mono-alphabetic cipher, while serving as an introductory tool to understand encryption principles, falls short in providing robust data security. Through my laboratory experiments, I have realized that while it may seem less complex than other encryption methods, it is inherently vulnerable to attacks, such as frequency analysis. Its limited key space and predictable patterns make it inadequate for safeguarding sensitive or valuable information in the modern digital age. As technology advances, it becomes increasingly evident that more sophisticated encryption techniques are necessary to ensure data confidentiality and integrity.

Github

[Sufferal/cryptography-labs (github.com)]