Ministerul Educatiei, Culturii și Cercetarii al Republicii

Moldova Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică şi Microelectronică

Departamentul Ingineria Software și Automatica

Report

Laboratory work nr.2

Cryptography and Security Course.

Elaborated:

Chihai Nichita, FAF-213

Verified:

Cătălin MÎŢU

Chișinău – 2023

Theme: Cryptanalysis of mono-alphabetic ciphers.

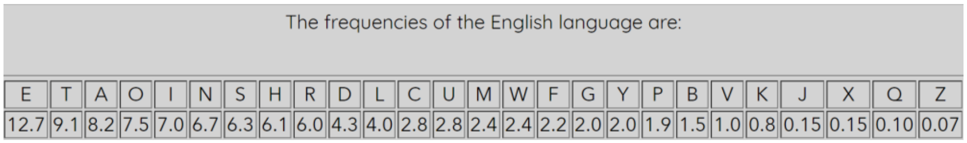
Tasks:

A message was intercepted, and it is known to have been obtained using a monoalphabetic cipher. By applying frequency analysis attack, the original message can be deciphered if it is assumed to be a text written in English. Please note that only the letters were encrypted, while the other characters remained unencrypted.

Mono-alphabetic Substitution: V-10

Intercepted text:

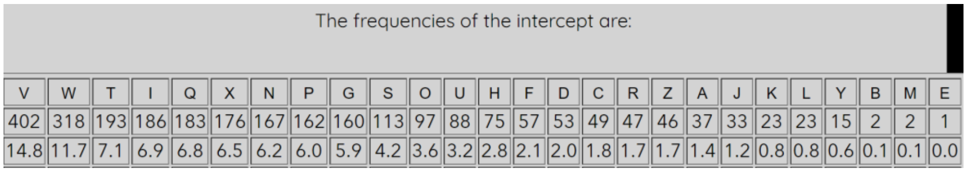
Kxjvgviv rtp anig xg wqv kxsstjv nc Ptxgw-Undihtxg, tandw qtscrtfavwrvvg Utixp tgo Ztipvxssvp, ng Tuixs 5, 1523. Tw 24, qv vgwvivo wqvpvikxhv nc wqv Odlv nc Gvkvip, wn rqnpv qndpv qv ivztxgvo twwthqvo wqvivpw nc qxp sxcv, vyhvuw cni uvixnop tw hndiw tgo tp t oxusnztw. Xg 1549, tw26, qv rvgw wn Inzv ng t wrn-fvti oxusnztwxh zxppxng.Xw rtp qviv wqtw qv rtp cxipw wqinrg xgwn hngwthw rxwq hifuwnsnjf, tgoqv pvvzp wn qtkv pwvvuvo qxzpvsc xg xw. Qv ivto wqv annlp nc Wixwqvzxdp,Avstpn, tgo nwqvi rixwvip, tgo wqv dgudasxpqvo ztgdphixuw nc Tsaviwx. Qvvkxovgwsf hngkvipvo rxwq wqv vyuviwp nc wqv ututs hdixt, cni qv wvssptgvhonwvp wqtw qv hndso qtkv qvtio ngsf xg wqv pqnuwtsl nc wqvpvhifuwnsnjxpwp. Tw 47, Kxjvgviv bdxw wqv hndiw, wdigvo nkvi qxp tggdxwf nc1,000 sxkivp t fvti wn wqv unni nc Utixp, ztiixvo wqv zdhq fndgjvi ZtixvKtiv, tgo ovknwvo qxzpvsc wn qxp rixwxgj. Qxp Witxhwv ovp Hqxccivp, rqxhqrtp rixwwvg xg 1585 ovpuxwv wqv oxpwithwxng nc t fvti-nso ataf otdjqwvi,tuuvtivo, vsvjtgwsf idaixhtwvo, xg 1586, tgo rtp ivuixgwvo wqv cnssnrxgjfvti. Qxp tdwnlvf pfpwvz dpvo wqv ustxgwvyw tp wqv lvf. Xw uinkxovo tuixzxgj lvf. Wqxp hngpxpwvo nc t pxgjsv svwwvi, lgnrg wn anwq vghxuqvivitgo ovhxuqvivi, rxwq rqxhq wqv ovhxuqvivi hndso ovhxuqvi wqv cxipwhifuwnjitz svwwvi tgo pn jvw t pwtiw ng qxp, rnil. Rxwq wqxp, qv rndso jvwwqv cxipw ustxgwvyw svwwvi, wqvg dpv wqxp tp wqv lvf wn ovhxuqvi wqv pvhngohifuwnjitz svwwvi, dpv wqtw ustxgwvyw tp wqv lvf wn ovhxuqvi wqv wqxiohifuwnjitz svwwvi, tgo pn ng.Wqv pfpwvz rnilp rvss tgo tccniop ctxi jdtitgwvvp nc pvhdixwf; xw qtpavvg vzanoxvo xg t gdzavi nc znovig hxuqvi zthqxgvp.Xg puxwv nc Kxjvgviv'p hsvti vyunpxwxng nc qxp wvhqgxbdv, xw rtp vgwxivsfcnijnwwvg tgo ngsf vgwvivo wqv pwivtz nc hifuwnsnjf stwv xg wqv 19wqhvgwdif tcwvi xw qto avvg ivxgkvgwvo. Rixwvip ng hifuwnsnjf wqvg toovoxgpdsw wn xgedif af ovjitoxgj Kxjvgviv'p pfpwvz xgwn ngv zdhq znivvsvzvgwtif.Wqv hxuqvi gnr dgxkviptssf htssvo wqv Kxjvgviv vzusnfp ngsf pwtgotio tsuqtavwp tgo t pqniw ivuvtwxgj lvfrnio—t pfpwvz ctizniv pdphvuwxasv wn pnsdwxng wqtg Kxjvgviv'p tdwnlvf. Xwp wtasvtdhngpxpwp nc t znovig wtadst ivhwt: 26 pwtgotio qnixmngwts tsuqtavwp,vthq psxo ngv puthv wn wqv svcw nc wqv ngv tankv. Wqvpv tiv wqv hxuqvitsuqtavwp. T gnizts tsuqtavw cni wqv ustxgwvyw pwtgop tw wqv wnu. Tgnwqvignizts tsuqtavw, rqxhq zvivsf ivuvtwp wqv xgxwxts svwwvip nc wqv qnixmngwtshxuqviwvyw tsuqtavwp, idgp onrg wqv svcw pxov. Wqxp xp wqv lvf tsuqtavw.Anwq hniivpungovgwp zdpw lgnr wqv lvfrnio. Wqv vghxuqvivi ivuvtwpwqxp tankv wqv ustxgwvyw svwwvip dgwxs vthq ngv qtp t lvfsvwwvi. Qv pvvlpwqv ustxgwvyw svwwvi xg wqv wnu tsuqtavw tgo wqv lvfsvwwvi xg wqv pxov. Wqvgqv withvp onrg cinz wqv wnu tgo xg cinz wqv pxov. Wqv hxuqviwvyw svwwvipwtgop tw wqv xgwvipvhwxng nc wqv hnsdzg tgo wqv inr. Wqv vghxuqviviivuvtwp wqxp uinhvpp rxwq tss wqv svwwvip nc wqv ustxgwvyw. Wn ovhxuqvi, wqvhsvil avjxgp rxwq wqv lvfsvwwvi, idgp xg tsngj wqv hxuqviwvyw tsuqtavwdgwxs qv pwixlvp wqv hxuqvi svwwvi, wqvg cnssnrp wqv hnsdzg nc svwwvipdurtio dgwxs qv vzvijvp tw wqv ustxgwvyw svwwvi tw wqv wnu.Unsftsuqtavwxh hxuqvip rviv, rqvg dpvo rxwq zxyvo tsuqtavwp tgorxwqndw rnio oxkxpxngp, dgaivtltasv wn wqv hifuwtgtsfpwp nc wqvIvgtxpptghv. Rqf, wqvg, oxo wqv gnzvghstwni ivxjg pduivzv cni 300fvtip? Rqf oxo hifuwnjituqvip gnw dpv wqv unsftsuqtavwxh pfpwvzxgpwvto?



The frequencies of the English language are:

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

Figure 1: Frequency of the English Alphabet letters.



The frequencies of the intercept are:

V	W	T	I	Q	X	N	P	G	S	O	U	H	F	D	C	R	Z	A	J	K	L	Y	B	M	E
402	318	193	186	183	176	167	162	160	113	97	88	75	57	53	49	47	46	37	33	23	23	15	2	2	1
14.8	11.7	7.1	6.9	6.8	6.5	6.2	6.0	5.9	4.2	3.6	3.2	2.8	2.1	2.0	1.8	1.7	1.7	1.4	1.2	0.8	0.8	0.6	0.1	0.1	0.0

Figure 2: Frequency of the intercepted text.

Having this data we can start the substitution of the letters. The letter V and W have the most frequency, so we can assume that these are the letters E and T respectively from the English Alphabet. If we make the substitution we get:

KXJeGeIe RTP ANIG XG tQe KXSSTJe NC PTXGt-UNDIHTXG, TANDt QTSCRTFAetReeG UTIXP TGO ZTIPeXSSeP, NG TUIXS 5, 1523. Tt 24, Qe eGteIeO tQePeIKXHe NC **tQe** ODLe NC GeKeIP, tN RQNPe QNDPe Qe IeZTXGeO TttTHQeO tQeIePt NC QXP SXCe, eYHeUt CNI UeIXNOP Tt HNDIt TGO TP T OXUSNZTt. XG 1549, Tt26, Qe ReGt tN INZe NG T tRN-FeTI OXUSNZTtXH ZXPPXNG.Xt RTP QeIe tQTt Qe RTP CXIPt tQINRG XGtN HNGtTHt RXtQ HIFUtNSNJF, TGOQe PeeZP tN QTKe PteeUeO QXZPeSC XG Xt. Qe IeTO tQe ANNLP NC tIXtQeZXDP,AeSTPN, TGO NtQeI RIXteIP, TGO tQe DGUDASXPQeO ZTGDPHIXUt NC TSAeItX. QeeKXOeGtSF HNGKeIPeO RXtQ tQe eYUeItP NC tQe UTUTS HDIXT, CNI Qe teSSPTGeHONteP tQTt Qe HNDSO QTKe QeTIO NGSF XG tQe PQNUtTSL NC tQePeHIFUtNSNJXPtP. Tt 47, KXJeGeIe BDXt tQe HNDIt, tDIGeO NKeI QXP TGGDXtF NC1,000 SXKIeP T FeTI tN tQe UNNI NC UTIXP, ZTIIXeO tQe ZDHQ FNDGJeI ZTIXeKTIe, TGO OeKNteO QXZPeSC tN QXP RIXtXGJ. QXP tITXHte OeP HQXCCIeP, RQXHQRTP RIXtteG XG 1585 OePUXte tQe OXPtITHtXNG NC T FeTI-NSO ATAF OTDJQteI,TUUeTIeO, eSeJTGtSF IDAIXHTteO, XG 1586, TGO RTP IeUIXGteO tQe CNSSNRXGJFeTI. QXP TDtNLeF PFPteZ DPeO tQe USTXGteYt TP tQe LeF. Xt UINKXOeO TUIXZXGJ LeF. tQXP HNGPXPteO NC T PXGJSe SetteI, LGNRG tN ANtQ eGHXUQeIeITGO OeHXUQeIeI, RXtQ RQXHQ tQe OeHXUQeIeI HNDSO OeHXUQeI tQe CXIPtHIFUtNJITZ SetteI TGO PN Jet T PtTIt NG QXP, RNIL. RXtQ tQXP, Qe RNDSO JettQe CXIPt USTXGteYt SetteI, tQeG DPe tQXP TP tQe LeF tN OeHXUQeI tQe PeHNGOHIFUtNJITZ SetteI, DPe tQTt USTXGteYt TP tQe LeF tN OeHXUQeI tQe tQXIOHIFUtNJITZ SetteI, TGO PN NG.tQe PFPteZ RNILP ReSS TGO TCCNIOP CTXI JDTITGteeP NC PeHDIXtF; Xt QTPAeeG eZANOXeO XG T GDZAeI NC ZNOeIG HXUQeI ZTHQXGeP.XG PUXte NC KXJeGeIe'P HSeTI eYUNPXtXNG NC QXP teHQGXBDe, Xt RTP eGtXIeSFCNIJNtteG TGO NGSF eGteIeO tQe PtIeTZ NC HIFUtNSNJF STte XG tQe 19tQHeGtDIF TCteI Xt QTO AeeG IeXGKeGteO. RIXteIP NG HIFUtNSNJF tQeG TOOeOXGPDSt tN XGEDIF AF OeJITOXGJ KXJeGeIe'P PFPteZ XGtN NGe ZDHQ ZNIeeSeZeGtTIF.tQe HXUQeI GNR DGXKeIPTSSF HTSSeO tQe KXJeGeIe eZUSNFP NGSF PtTGOTIO TSUQTAetP TGO T PQNIt IeUeTtXGJ LeFRNIO—T PFPteZ CTIZNIe PDPHeUtXASe tN PNSDtXNG tQTG KXJeGeIe'P TDtNLeF. XtP tTASeTDHNGPXPtP NC T ZNOeIG tTADST IeHtT: 26 PtTGOTIO QNIXMNGtTS TSUQTAetP,eTHQ PSXO NGe PUTHe tN tQe SeCt NC tQe NGe TANKe. tQePe TIe tQe HXUQeITSUQTAetP. T GNIZTS TSUQTAet CNI tQe USTXGteYt PtTGOP Tt tQe tNU. TGNtQeIGNIZTS TSUQTAet, RQXHQ ZeIeSF IeUeTtP tQe XGXtXTS SetteIP NC tQe QNIXMNGtTSHXUQeIteYt TSUQTAetP, IDGP ONRG tQe SeCt PXOe. tQXP XP tQe LeF TSUQTAet.ANtQ HNIIePUNGOeGtP ZDPt LGNR tQe LeFRNIO. tQe eGHXUQeIeI IeUeTtPtQXP TANKe tQe USTXGteYt SetteIP DGtXS eTHQ NGe QTP T LeFSetteI. Qe PeeLPtQe USTXGteYt SetteI XG tQe tNU TSUQTAet TGO tQe LeFSetteI XG tQe PXOe. tQeGQe tITHeP ONRG CINZ tQe tNU TGO XG CINZ tQe PXOe. tQe HXUQeIteYt SetteIPtTGOP Tt tQe XGteIPeHtXNG NC tQe HNSDZG TGO tQe INR. tQe eGHXUQeIeIIeUeTtP tQXP UINHePP RXtQ TSS tQe SetteIP NC tQe USTXGteYt. tN OeHXUQeI, tQeHSeIL AeJXGP RXtQ tQe LeFSetteI, IDGP XG TSNGJ tQe HXUQeIteYt TSUQTAetDGtXS Qe PtIXLeP tQe HXUQeI SetteI, tQeG CNSSNRP tQe HNSDZG NC SetteIPDURTIO DGtXS Qe eZeIJeP Tt tQe USTXGteYt SetteI Tt tQe tNU.UNSFTSUQTAetXH HXUQeIP ReIe, RQeG DPeO RXtQ ZXYeO TSUQTAetP TGORXtQNDt RNIO OXKXPXNGP, DGAIeTLTASe tN tQe HIFUtTGTSFPtP NC tQeIeGTXPPTGHe. RQF, tQeG, OXO tQe GNZeGHSTtNI IeXJG PDUIeZe CNI 300FeTIP? RQF OXO HIFUtNJITUQeIP GNt DPe tQe UNSFTSUQTAetXH

PFPteZXGPteTO?

We observe that there are a lot of words like "tQe", in English the most common word of 3 letters is the, making the substitution Q -> h, we obtain:

KXJeGeIe RTP ANIG XG the KXSSTJe NC PTXGt-UNDIHTXG, TANDt hTSCRTFAetReeG UTIXP TGO ZTIPeXSSeP, NG TUIXS 5, 1523. Tt 24, he eGteIeO thePeIKXHe NC the ODLe NC GeKeIP, **tN** RhNPe hNDPe he IeZTXGeO TttTHheO theIePt NC hXP SXCe, eYHeUt CNI UeIXNOP Tt HNDIt TGO TP T OXUSNZTt. XG 1549, Tt26, he ReGt tN INZe NG T tRN-FeTI OXUSNZTtXH ZXPPXNG.Xt RTP **heIe** thTt he RTP CXIPt thINRG XGtN HNGtTHt RXth HIFUtNSNJF, TGOhe PeeZP tN hTKe PteeUeO hXZPeSC XG Xt. he IeTO the ANNLP NC tIXtheZXDP,AeSTPN, TGO NtheI RIXteIP, TGO the DGUDASXPheO ZTGDPHIXUt NC TSAeItX. heeKXOeGtSF HNGKeIPeO RXth the eYUeItP NC the UTUTS HDIXT, CNI he teSSPTGeHONteP thTt he HNDSO hTKe heTIO NGSF XG the PhNUtTSL NC thePeHIFUtNSNJXPtP. Tt 47, KXJeGeIe BDXt the HNDIt, tDIGeO NKeI hXP TGGDXtF NC1,000 SXKIeP T FeTI tN the UNNI NC UTIXP, ZTIIXeO the ZDHh FNDGJeI ZTIXeKTIe, TGO OeKNteO hXZPeSC tN hXP RIXtXGJ. hXP tITXHte OeP HhXCCIeP, RhXHhRTP RIXtteG XG 1585 OePUXte the OXPtITHtXNG NC T FeTI-NSO ATAF OTDJhteI,TUUeTIeO, eSeJTGtSF IDAIXHTteO,XG 1586, TGO RTP IeUIXGteO the CNSSNRXGJFeTI. hXP TDtNLeF PFPteZ DPeO the USTXGteYt TP the LeF. Xt UINKXOeO TUIXZXGJ LeF. thXP HNGPXPteO NC T PXGJSe SetteI, LGNRG tN ANth eGHXUheIeITGO OeHXUheIeI, RXth RhXHh the OeHXUheIeI HNDSO OeHXUheI the CXIPtHIFUtNJITZ SetteI TGO PN Jet T PtTIt NG hXP, RNIL. RXth thXP, he RNDSO Jetthe CXIPt USTXGteYt SetteI, theG DPe thXP TP the LeF tN OeHXUheI the PeHNGOHIFUtNJITZ SetteI, DPe thTt USTXGteYt TP the LeF tN OeHXUheI the thXIOHIFUtNJITZ SetteI, TGO PN NG.the PFPteZ RNILP ReSS TGO TCCNIOP CTXI JDTITGteeP NC PeHDIXtF; Xt hTPAeeG eZANOXeO XG T GDZAeI NC ZNOeIG HXUheI ZTHhXGeP.XG PUXte NC KXJeGeIe'P HSeTI eYUNPXtXNG NC hXP teHhGXBDe, Xt RTP eGtXIeSFCNIJNtteG TGO NGSF eGteIeO the PtIeTZ NC HIFUtNSNJF STte XG the 19thHeGtDIF TCteI Xt hTO AeeG IeXGKeGteO. RIXteIP NG HIFUtNSNJF theG TOOeOXGPDSt tN XGEDIF AF OeJITOXGJ KXJeGeIe'P PFPteZ XGtN NGe ZDHh ZNIeeSeZeGtTIF.the HXUheI GNR DGXKeIPTSSF HTSSeO the KXJeGeIe eZUSNFP NGSF PtTGOTIO TSUhTAetP TGO T PhNIt IeUeTtXGJ LeFRNIO—T PFPteZ CTIZNIe PDPHeUtXASe tN PNSDtXNG thTGKXJeGeIe'P TDtNLeF. XtP tTASeTDHNGPXPtP NC T ZNOeIG tTADST IeHtT: 26 PtTGOTIO hNIXMNGtTS TSUhTAetP,eTHh PSXO NGe PUTHe tN the SeCt NC the NGe TANKe. thePe TIe the HXUheITSUhTAetP. T GNIZTS TSUhTAet CNI the USTXGteYt PtTGOP Tt the tNU. TGNtheIGNIZTS TSUhTAet, RhXHh ZeIeSF IeUeTtP the XGXtXTS SetteIP NC the hNIXMNGtTSHXUheIteYt TSUhTAetP, IDGP ONRG the SeCt PXOe. thXP XP the LeF TSUhTAet.ANth HNIIePUNGOeGtP ZDPt LGNR the LeFRNIO. the eGHXUheIeI IeUeTtPthXP TANKe the USTXGteYt SetteIP DGtXS eTHh NGe hTP T LeFSetteI. he PeeLPthe USTXGteYt SetteI XG the tNU TSUhTAet TGO the LeFSetteI XG the PXOe. theGhe tITHeP ONRG CINZ the tNU TGO XG CINZ the PXOe. the HXUheIteYt SetteIPtTGOP Tt the XGteIPeHtXNG NC the HNSDZG TGO the INR. the eGHXUheIeIIeUeTtP thXP UINHePP RXth TSS the SetteIP NC the USTXGteYt. tN OeHXUheI, theHSeIL AeJXGP RXth the LeFSetteI, IDGP XG TSNGJ the HXUheIteYt TSUhTAetDGtXS he PtIXLeP the HXUheI SetteI, theG CNSSNRP the HNSDZG NC SetteIPDURTIO DGtXS he eZeIJeP Tt the USTXGteYt SetteI Tt the tNU.UNSFTSUhTAetXH HXUheIP ReIe, RheG DPeO RXth ZXYeO TSUhTAetP TGORXthNDt RNIO OXKXPXNGP, DGAIeTLTASe tN the HIFUtTGTSFPtP NC theIeGTXPPTGHe. RhF, theG, OXO the GNZeGHSTtNI IeXJG PDUIeZe CNI 300FeTIP? RhF OXO HIFUtNJITUheIP GNt DPe the UNSFTSUhTAetXH PFPteZXGPteTO?

After that substitution we observe that there are also two common English words "tN" and "heIe" which are to and here, so making the substitution N -> o and I -> r, we obtain:

KXJeGere RTP AorG XG the KXSSTJe oC PTXGt-UoDrHTXG, TAoDt hTSCRTFAetReeG UTrXP TGO ZTrPeXSSeP, oG TUrXS 5, 1523. Tt 24, he eGtereO thePerKXHe oC the ODLe oC GeKerP, to RhoPe hoDPe he reZTXGeO TttTHheO therePt oC hXP SXCe, eYHeUt Cor UerXoOP Tt HoDrt TGO TP T OXUSoZTt. XG 1549, Tt26, he ReGt to roZe oG T tRo-FeTr OXUSoZTtXH ZXPPXoG.Xt RTP here **thTt** he RTP CXrPt throRG XGto HoGtTHt RXth HrFUtoSoJF, TGOhe PeeZP to hTKe PteeUeO hXZPeSC XG Xt. he **reTO** the AooLP oC trXtheZXDP,AeSTPo, TGO other RrXterP, TGO the DGUDASXPheO ZTGDPHrXUt oC TSAertX. heeKXOeGtSF HoGKerPeO RXth the eYUertP oC the UTUTS HDrXT, Cor he teSSPTGeHOoteP thTt he HoDSO hTKe heTrO oGSF XG the PhoUtTSL oC thePeHrFUtoSoJXPtP. Tt 47, KXJeGere BDXt the HoDrt, tDrGeO oKer hXP TGGDXtF oC1,000 SXKreP T FeTr to the Uoor oC UTrXP, ZTrrXeO the ZDHh FoDGJer ZTrXeKTre, TGO OeKoteO hXZPeSC to hXP RrXtXGJ. hXP trTXHte OeP HhXCCreP, RhXHhRTP RrXtteG XG 1585 OePUXte the

OXPtrTHtXoG oC T FeTr-oSO ATAF OTDJhter,TUUeTreO, eSeJTGtSF rDArXHTteO, XG 1586, TGO RTP reUrXGteO the CoSSoRXGJFeTr. hXP TDtoLeF PFPteZ DPeO the USTXGteYt TP the LeF. Xt UroKXOeO TUrXZXGJ LeF. thXP HoGPXPteO oC T PXGJSe Setter, LGoRG to Aoth eGHXUhererTGO OeHXUherer, RXth RhXHh the OeHXUherer HoDSO OeHXUher the CXrPtHrFUtoJrTZ Setter TGO Po Jet T PtTrt oG hXP, RorL. RXth thXP, he RoDSO Jetthe CXrPt USTXGteYt Setter, theG DPe thXP TP the LeF to OeHXUher the PeHoGOHrFUtoJrTZ Setter, DPe thTt USTXGteYt TP the LeF to OeHXUher the thXrOHrFUtoJrTZ Setter, TGO Po oG.the PFPteZ RorLP ReSS TGO TCCorOP CTXr JDTrTGteeP oC PeHDrXtF; Xt hTPAeeG eZAoOXeO XG T GDZAer oC ZoOerG HXUher ZTHhXGeP.XG PUXte oC KXJeGere'P HSeTr eYUoPXtXoG oC hXP teHhGXBDe, Xt RTP eGtXreSFCorJotteG TGO oGSF eGtereO the PtreTZ oC HrFUtoSoJF STte XG the 19thHeGtDrF TCter Xt hTO AeeG reXGKeGteO. RrXterP oG HrFUtoSoJF theG TOOeOXGPDSt to XGEDrF AF OeJrTOXGJ KXJeGere'P PFPteZ XGto oGeZDHh ZoreeSeZeGtTrF.the HXUher GoR DGXKerPTSSF HTSSeO the KXJeGere eZUSoFP oGSF PtTGOTrO TSUhTAetP TGO T Phort reUeTtXGJ LeFRorO—T PFPteZ CTrZore PDPHeUtXASe to PoSDtXoG thTG KXJeGere'P TDtoLeF. XtP tTASeTDHoGPXPtP oC T ZoOerG tTADST reHtT: 26 PtTGOTrO horXMoGtTS TSUhTAetP,eTHh PSXO oGe PUTHe to the SeCt oC the oGe TAoKe. thePe Tre the HXUherTSUhTAetP. T GorZTS TSUhTAet Cor the USTXGteYt PtTGOP Tt the toU. TGotherGorZTS TSUhTAet, RhXHh ZereSF reUeTtP the XGXtXTS SetterP oC the horXMoGtTSHXUherteYt TSUhTAetP, rDGP OoRG the SeCt PXOe. thXP XP the LeF TSUhTAet.Aoth HorrePUoGOeGtP ZDPt LGoR the LeFRorO. the eGHXUherer reUeTtPthXP TAoKe the USTXGteYt SetterP DGtXS eTHh oGe hTP T LeFSetter. he PeeLPthe USTXGteYt Setter XG the toU TSUhTAet TGO the LeFSetter XG the PXOe. theGhe trTHeP OoRG CroZ the toU TGO XG CroZ the PXOe. the HXUherteYt SetterPtTGOP Tt the XGterPeHtXoG oC the HoSDZG TGO the roR. the eGHXUhererreUeTtP thXP UroHePP RXth TSS the SetterP oC the USTXGteYt. to OeHXUher, theHSerL AeJXGP RXth the LeFSetter, rDGP XG TSoGJ the HXUherteYt TSUhTAetDGtXS he PtrXLeP the HXUher Setter, theG CoSSoRP the HoSDZG oC SetterPDURTrO DGtXS he eZerJeP Tt the USTXGteYt Setter Tt the toU.UoSFTSUhTAetXH HXUherP Rere, RheG DPeO RXth ZXYeO TSUhTAetP TGORXthoDt RorO OXKXPXoGP, DGAreTLTASe to the HrFUtTGTSFPtP oC thereGTXPPTGHe. RhF, theG, OXO the GoZeGHSTtor reXJG PDUreZe Cor 300FeTrP? RhF OXO HrFUtoJrTUherP Got DPe the UoSFTSUhTAetXH PFPteZXGPteTO?

In this ciphertext we can observe again two common English words “thTt” and “reTO” which are likely to be that and read, making the substitution we get the new ciphertext:

KXJeGere RaP AorG XG the KXSSaJe oC PaXGt-UoDrHaXG, aAoDt haSCRaFAetReeG UarXP aGd ZarPeXSSeP, oG aUrXS 5, 1523. at 24, he eGtered thePerKXHe oC the dDLe oC GeKerP, to RhoPe hoDPe he reZaXGed attaHhed therePt oC hXP SXCe, eYHeUt **Cor** UerXodP at HoDrt aGd aP a dXUSoZat. XG 1549, at26, he ReGt to roZe oG a tRo-Fear dXUSoZatXH ZXPPXoG.Xt RaP here that he RaP CXrPt throRG XGto HoGtaHt RXth HrFUtoSoJF, aGdhe PeeZP to haKe PteeUed hXZPeSC XG Xt. he read the AooLP oC trXtheZXDP,AeSaPo, aGd other RrXterP, aGd the DGUDASXPhed ZaGDPHrXUt oC aSAertX. heeKXdeGtSF HoGKerPed RXth the eYUertP oC the UaUaS HDrXa, Cor he teSSPaGeHdoteP that he HoDSd haKe heard oGSF XG the PhoUtaSL oC thePeHrFUtoSoJXPtP. at 47, KXJeGere BDXt the HoDrt, tDrGed oKer hXP aGGDXtF oC1,000 SXKreP a Fear to the Uoor oC UarXP, ZarrXed the ZDHh FoDGJer ZarXeKare, aGd deKoted hXZPeSC to hXP RrXtXGJ. hXP traXHte deP HhXCCreP, RhXHhRaP RrXtteG XG 1585 dePUXte the dXPtraHtXoG oC a Fear-oSd AaAF daDJhter,aUUeared, eSeJaGtSF rDArXHated, XG 1586, aGd RaP reUrXGted the CoSSoRXGJFear. hXP aDtoLeF PFPteZ DPed the USaXGteYt aP the LeF. Xt UroKXded aUrXZXGJ LeF. thXP HoGPXPted oC a PXGJSe Setter, LGoRG to Aoth eGHXUhereraGd deHXUherer, RXth RhXHh the deHXUherer HoDSd deHXUher the CXrPtHrFUtoJraZ Setter aGd Po Jet a Ptart oG hXP, RorL. RXth thXP, he RoDSd Jetthe CXrPt USaXGteYt Setter, theG DPe thXP aP the LeF to deHXUher the PeHoGdHrFUtoJraZ Setter, DPe that USaXGteYt aP the LeF to deHXUher the thXrdHrFUtoJraZ Setter, aGd Po oG.the PFPteZ RorLP ReSS aGd aCCordP CaXr JDaraGteeP oC PeHDrXtF; Xt haPAeeG eZAodXed XG a GDZAer oC ZoderG HXUher ZaHhXGeP.XG PUXte oC KXJeGere'P HSear eYUoPXtXoG oC hXP teHhGXBDe, Xt RaP eGtXreSFCorJotteG aGd oGSF **eGtered** the PtreaZ oC HrFUtoSoJF Sate XG the 19thHeGtDrF aCter Xt had AeeG reXGKeGted. RrXterP oG HrFUtoSoJF theG addedXGPDSt to XGEDrF AF deJradXGJ KXJeGere'P PFPteZ XGto oGe ZDHh ZoreeSeZeGtarF.the HXUher GoR DGXKerPaSSF HaSSed the KXJeGere eZUSoFP oGSF PtaGdard aSUhaAetP aGd a Phort reUeatXGJ LeFRord—a PFPteZ CarZore PDPHeUtXASe to PoSDtXoG thaG KXJeGere'P aDtoLeF. XtP taASeaDHoGPXPtP oC a ZoderG taADSa reHta: 26 PtaGdard horXMoGtaS aSUhaAetP,eaHh PSXd oGe PUaHe to the SeCt oC the oGe aAoKe. thePe are the HXUheraSUhaAetP. a GorZaS aSUhaAet Cor the USaXGteYt PtaGdP at the toU. aGotherGorZaS aSUhaAet, RhXHh ZereSF reUeatP the XGXtXaS SetterP oC the horXMoGtaSHXUherteYt aSUhaAetP, rDGP doRG the SeCt PXde. thXP XP the LeF aSUhaAet.Aoth HorrePUoGdeGtP ZDPt LGoR the LeFRord. the eGHXUherer reUeatPthXP aAoKe the USaXGteYt SetterP DGtXS eaHh oGe haP a LeFSetter. he PeeLPthe USaXGteYt Setter XG the toU aSUhaAet aGd the LeFSetter XG the PXde. theGhe traHeP doRG CroZ the toU aGd XG CroZ the PXde. the HXUherteYt SetterPtaGdP at the XGterPeHtXoG oC the HoSDZG aGd the roR. the eGHXUhererreUeatP thXP UroHePP RXth aSS the SetterP oC the USaXGteYt. to deHXUher, theHSerL AeJXGP RXth the LeFSetter, rDGP XG aSoGJ the HXUherteYt aSUhaAetDGtXS he PtrXLeP the HXUher Setter, theG CoSSoRP the HoSDZG oC SetterPDURard DGtXS he eZerJeP at the USaXGteYt Setter at the toU.UoSFaSUhaAetXH HXUherP Rere, RheG DPed RXth ZXYed aSUhaAetP aGdRXthoDt Rord dXKXPXoGP, DGAreaLaASe to the HrFUtaGaSFPtP oC thereGaXPPaGHe. RhF, theG, dXd the GoZeGHSator reXJG PDUreZe Cor 300FearP? RhF dXd HrFUtoJraUherP Got DPe the UoSFaSUhaAetXH PFPteZXGPtead?

Again we can find in the ciphertext two common English words “eGtered” and “Cor” whiich are likely to be entered and for, G -> n and C -> f, making the substitution we obtain:

KXJenere RaP Aorn Xn the KXSSaJe of PaXnt-UoDrHaXn, aAoDt haSfRaFAetReen UarXP and ZarPeXSSeP, on aUrXS 5, 1523. at 24, he entered thePerKXHe of the dDLe of neKerP, to RhoPe hoDPe he reZaXned attaHhed therePt of **hXP** SXfe, eYHeUt for UerXodP at HoDrt and aP a dXUSoZat. **Xn** 1549, at26, he Rent to roZe on a tRo-Fear dXUSoZatXH ZXPPXon.Xt RaP here that he RaP fXrPt throRn Xnto HontaHt RXth HrFUtoSoJF, andhe PeeZP to haKe PteeUed hXZPeSf Xn Xt. he read the AooLP of trXtheZXDP,AeSaPo, and other RrXterP, and the DnUDASXPhed ZanDPHrXUt of aSAertX. heeKXdentSF HonKerPed RXth the eYUertP of the UaUaS HDrXa, for he teSSPaneHdoteP that he HoDSd haKe heard onSF Xn the PhoUtaSL of thePeHrFUtoSoJXPtP. at 47, KXJenere BDXt the HoDrt, tDrned oKer hXP annDXtF of1,000 SXKreP a Fear to the Uoor of UarXP, ZarrXed the ZDHh FoDnJer ZarXeKare, and deKoted hXZPeSf to hXP RrXtXnJ. hXP traXHte deP HhXffreP, RhXHhRaP RrXtten Xn 1585 dePUXte the dXPtraHtXon of a Fear-oSd AaAF daDJhter,aUUeared, eSeJantSF rDArXHated, Xn 1586, and RaP reUrXnted the foSSoRXnJFear. hXP aDtoLeF PFPteZ DPed the USaXnteYt aP the LeF. Xt UroKXded aUrXZXnJ LeF. thXP HonPXPted of a PXnJSe Setter, LnoRn to Aoth enHXUhererand deHXUherer, RXth RhXHh the deHXUherer HoDSd deHXUher the fXrPtHrFUtoJraZ Setter and Po Jet a Ptart on hXP, RorL. RXth thXP, he RoDSd Jetthe fXrPt USaXnteYt Setter, then DPe thXP aP the LeF to deHXUher the PeHondHrFUtoJraZ Setter, DPe that USaXnteYt aP the LeF to deHXUher the thXrdHrFUtoJraZ Setter, and Po on.the PFPteZ RorLP ReSS and affordP faXr JDaranteeP of PeHDrXtF; Xt haPAeen eZAodXed Xn a nDZAer of Zodern HXUher ZaHhXneP.Xn PUXte of KXJenere'P HSear eYUoPXtXon of hXP teHhnXBDe, Xt RaP entXreSFforJotten and onSF entered the PtreaZ of HrFUtoSoJF Sate Xn the 19thHentDrF after Xt had Aeen reXnKented. RrXterP on HrFUtoSoJF then addedXnPDSt to XnEDrF AF deJradXnJ KXJenere'P PFPteZ Xnto one ZDHh ZoreeSeZentarF.the HXUher noR DnXKerPaSSF HaSSed the KXJenere eZUSoFP onSF Ptandard aSUhaAetP and a Phort reUeatXnJ LeFRord—a PFPteZ farZore PDPHeUtXASe to PoSDtXon than KXJenere'P aDtoLeF. XtP taASeaDHonPXPtP of a Zodern taADSa reHta: 26 Ptandard horXMontaS aSUhaAetP,eaHh PSXd one PUaHe to the Seft of the one aAoKe. thePe are the HXUheraSUhaAetP. a norZaS aSUhaAet for the USaXnteYt PtandP at the toU. anothernorZaS aSUhaAet, RhXHh ZereSF reUeatP the XnXtXaS SetterP of the horXMontaSHXUherteYt aSUhaAetP, rDnP doRn the Seft PXde. thXP XP the LeF aSUhaAet.Aoth HorrePUondentP ZDPt LnoR the LeFRord. the enHXUherer reUeatPthXP aAoKe the USaXnteYt SetterP DntXS eaHh one haP a LeFSetter. he PeeLPthe USaXnteYt Setter Xn the toU aSUhaAet and the LeFSetter Xn the PXde. thenhe traHeP doRn froZ the toU and Xn froZ the PXde. the HXUherteYt SetterPtandP at the XnterPeHtXon of the HoSDZn and the roR. the enHXUhererreUeatP thXP UroHePP RXth aSS the SetterP of the USaXnteYt. to deHXUher, theHSerL AeJXnP RXth the LeFSetter, rDnP Xn aSonJ the HXUherteYt aSUhaAetDntXS he PtrXLeP the HXUher Setter, then foSSoRP the HoSDZn of SetterPDURard DntXS he eZerJeP at the USaXnteYt Setter at the toU.UoSFaSUhaAetXH HXUherP Rere, Rhen DPed RXth ZXYed aSUhaAetP andRXthoDt Rord dXKXPXonP, DnAreaLaASe to the HrFUtanaSFPtP of therenaXPPanHe. RhF, then, dXd the noZenHSator reXJn PDUreZe for 300FearP? RhF dXd HrFUtoJraUherP not DPe the UoSFaSUhaAetXH PFPteZXnPtead?

Looking through the text there are two common Enlgish words, “Xn” and “hiP”, which again are most likely to be It and his, which means X -> i and P -> s, after makiong this change we get the following ciphertext:

KiJenere Ras **Aorn** in the KiSSaJe of saint-UoDrHain, aAoDt haSfRaFAetReen Uaris and ZarseiSSes, on aUriS 5, 1523. at 24, he entered theserKiHe of the dDLe of neKers, to Rhose hoDse he reZained attaHhed therest of his **Sife**, eYHeUt for Ueriods at HoDrt and as a diUSoZat. in 1549, at26, he Rent to roZe on a tRo-Fear diUSoZatiH Zission.it **Ras** here that he Ras first throRn into HontaHt Rith HrFUtoSoJF, andhe seeZs to haKe steeUed hiZseSf in it. he read the AooLs of tritheZiDs,AeSaso, and other Rriters, and the DnUDASished ZanDsHriUt of aSAerti. heeKidentSF HonKersed Rith the eYUerts of the UaUaS HDria, for he teSSsaneHdotes that he HoDSd haKe heard onSF in the shoUtaSL of theseHrFUtoSoJists. at 47, KiJenere BDit the HoDrt, tDrned oKer his annDitF of1,000 SiKres a Fear to the Uoor of Uaris, Zarried the ZDHh FoDnJer ZarieKare, and deKoted hiZseSf to his RritinJ. his traiHte des Hhiffres, RhiHhRas Rritten in 1585 desUite the distraHtion of a Fear-oSd AaAF daDJhter,aUUeared, eSeJantSF rDAriHated, in 1586, and Ras reUrinted the foSSoRinJFear. his aDtoLeF sFsteZ Dsed the USainteYt as the LeF. it UroKided aUriZinJ LeF. this Honsisted of a sinJSe Setter, LnoRn to Aoth enHiUhererand deHiUherer, Rith RhiHh the deHiUherer HoDSd deHiUher the firstHrFUtoJraZ Setter and so Jet a start on his, RorL. Rith this,heRoDSd Jetthe first USainteYt Setter, then Dse this as the LeF to deHiUher the seHondHrFUtoJraZ Setter, Dse that USainteYt as the LeF to deHiUher the thirdHrFUtoJraZ Setter, and so on.the sFsteZ RorLs ReSS and affords fair JDarantees of seHDritF; it hasAeen eZAodied in a nDZAer of Zodern HiUher ZaHhines.in sUite of KiJenere's HSear eYUosition of his teHhniBDe, it Ras entireSFforJotten and onSF entered the streaZ of HrFUtoSoJF Sate in the 19thHentDrF after it had Aeen reinKented. Rriters on HrFUtoSoJF then addedinsDSt to inEDrF AF deJradinJ KiJenere's sFsteZ into one ZDHh ZoreeSeZentarF.the HiUher noR DniKersaSSF HaSSed the KiJenere eZUSoFs onSF standard aSUhaAets and a short reUeatinJ LeFRord—a sFsteZ farZore sDsHeUtiASe to soSDtion than KiJenere's aDtoLeF. its taASeaDHonsists of a Zodern taADSa reHta: 26 standard horiMontaS aSUhaAets,eaHh sSid one sUaHe to the Seft of the one aAoKe. these are the HiUheraSUhaAets. a norZaS aSUhaAet for the USainteYt stands at the toU. anothernorZaS aSUhaAet, RhiHh ZereSF reUeats the initiaS Setters of the horiMontaSHiUherteYt aSUhaAets, rDns doRn the Seft side. this is the LeF aSUhaAet.Aoth HorresUondents ZDst LnoR the LeFRord. the enHiUherer reUeatsthis aAoKe the USainteYt Setters DntiS eaHh one has a LeFSetter. he seeLsthe USainteYt Setter in the toU aSUhaAet and the LeFSetter in the side. thenhe traHes doRn froZ the toU and in froZ the side. the HiUherteYt Setterstands at the interseHtion of the HoSDZn and the roR. the enHiUhererreUeats this UroHess Rith aSS the Setters of the USainteYt. to deHiUher, theHSerL AeJins Rith the LeFSetter, rDns in aSonJ the HiUherteYt aSUhaAetDntiS he striLes the HiUher Setter, then foSSoRs the HoSDZn of SettersDURard DntiS he eZerJes at the USainteYt Setter at the toU.UoSFaSUhaAetiH HiUhers Rere, Rhen Dsed Rith ZiYed aSUhaAets andRithoDt Rord diKisions, DnAreaLaASe to the HrFUtanaSFsts of therenaissanHe. RhF, then, did the noZenHSator reiJn sDUreZe for 300Fears? RhF did HrFUtoJraUhers not Dse the UoSFaSUhaAetiH sFsteZinstead?

After making the substitution there are several common words found, like “Sife”, “Ras” and “Aorn” which are respectively life, was and born, S -> l, R -> w, A ->b, making these substitutions we get the following ciphertext:

KiJenere was born in the KiiiaJe of saint-UoDrHain, **aboDt** haifwaFbetween Uaris and Zarseiiies, on aUrii 5, 1523. at 24, he entered theserKiHe of the dDLe of neKers, to whose hoDse he reZained attaHhed therest of his iife, eYHeUt for Ueriods at HoDrt and as a diUioZat. in 1549, at26, he went to roZe on a two-Fear diUioZatiH Zission.it was here that he was first thrown into HontaHt with HrFUtoioJF, andhe seeZs to haKe steeUed hiZseif in it. he read the booLs of tritheZiDs,beiaso, and other writers, and the DnUDbiished ZanDsHriUt of aiberti. heeKidentiF HonKersed with the eYUerts of the UaUai HDria, for he teiisaneHdotes that he HoDid haKe heard oniF in the shoUtaiL of theseHrFUtoioJists. at 47, KiJenere BDit the HoDrt, tDrned oKer his annDitF of1,000 iiKres a Fear to the Uoor of Uaris, Zarried the ZDHh FoDnJer ZarieKare, and deKoted hiZseif to his writinJ. his traiHte des Hhiffres, whiHhwas written in 1585 desUite the distraHtion of a Fear-oid babF daDJhter,aUUeared, eieJantiF rDbriHated, in 1586, and was reUrinted the foiiowinJFear. his aDtoLeF sFsteZ Dsed the UiainteYt as the **LeF**. it UroKided aUriZinJ LeF. this Honsisted of a sinJie ietter, **Lnown** to both enHiUhererand deHiUherer, with whiHh the deHiUherer HoDid deHiUher the firstHrFUtoJraZ ietter and so Jet a start on his, worL. with this, he woDid Jetthe first UiainteYt ietter, then Dse this as the LeF to deHiUher the seHondHrFUtoJraZ ietter, Dse that UiainteYt as the LeF to deHiUher the thirdHrFUtoJraZ ietter, and so on.the sFsteZ worLs weii and affords fair JDarantees of seHDritF; it hasbeen eZbodied in a nDZber of Zodern HiUher ZaHhines.in sUite of KiJenere's Hiear eYUosition of his teHhniBDe, it was entireiFforJotten and oniF entered the streaZ of HrFUtoioJF iate in the 19thHentDrF after it had been reinKented. writers on HrFUtoioJF then addedinsDit to inEDrF bF deJradinJ KiJenere's sFsteZ into one ZDHh ZoreeieZentarF.the HiUher now DniKersaiiF Haiied the KiJenere eZUioFs oniF standard aiUhabets and a short reUeatinJ LeFword—a sFsteZ farZore sDsHeUtibie to soiDtion than KiJenere's aDtoLeF. its tabieaDHonsists of a Zodern tabDia reHta: 26 standard horiMontai aiUhabets,eaHh siid one sUaHe to the ieft of the one aboKe. these are the HiUheraiUhabets. a norZai aiUhabet for the UiainteYt stands at the toU. anothernorZai aiUhabet, whiHh ZereiF reUeats the initiai ietters of the horiMontaiHiUherteYt aiUhabets, rDns down the ieft side. this is the LeF aiUhabet.both HorresUondents ZDst Lnow the LeFword. the enHiUherer reUeatsthis aboKe the UiainteYt ietters Dntii eaHh one has a LeFietter. he seeLsthe UiainteYt ietter in the toU aiUhabet and the LeFietter in the side. thenhe traHes down froZ the toU and in froZ the side. the HiUherteYt ietterstands at the interseHtion of the HoiDZn and the row. the enHiUhererreUeats this UroHess with aii the ietters of the UiainteYt. to deHiUher, theHierL beJins with the LeFietter, rDns in aionJ the HiUherteYt aiUhabetDntii he striLes the HiUher ietter, then foiiows the HoiDZn of iettersDUward Dntii he eZerJes at the UiainteYt ietter at the toU.UoiFaiUhabetiH HiUhers were, whenDsedwithZiYed aiUhabets andwithoDt word diKisions, DnbreaLabie to the HrFUtanaiFsts of therenaissanHe. whF, then, did the noZenHiator reiJn sDUreZe for 300Fears? whF did HrFUtoJraUhers not Dse the UoiFaiUhabetiH sFsteZinstead?

Analysing the ciphertext we can make the several substitutions, “aboDt”, “LeF”, “Lnown”, which are about way and books, making the following substitutions D -> u, F -> y, L -> k, we obtain we following ciphertext:

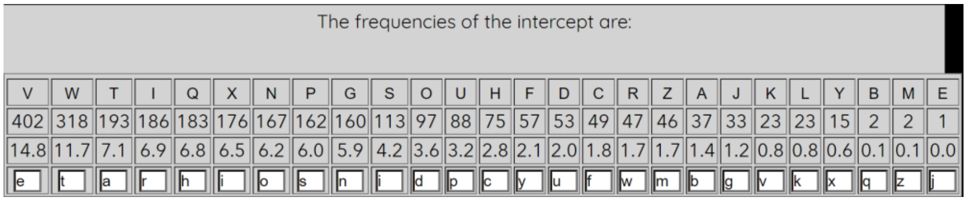
KiJenere was born in the KiiiaJe of saint-UourHain, about haifwaybetween Uaris and Zarseiiies, on aUrii 5, 1523. at 24, he entered theserKiHe of the duke of neKers, to whose house he reZained **attaHhed** therest of his iife, eYHeUt for Ueriods at Hourt and as a **diUioZa**t. in 1549, at26, he went to roZe on a two-year diUioZatiH **Zission**.it was here that he was first thrown into HontaHt with HryUtoioJy, andhe seeZs to **haKe** steeUed hiZseif in it. he read the books of tritheZius,beiaso, and other writers, and the unUubiished ZanusHriUt of aiberti. heeKidentiy HonKersed with the eYUerts of the UaUai Huria, for he teiisaneHdotes that he Houid haKe heard oniy in the shoUtaik of theseHryUtoioJists. at 47, KiJenere Buit the Hourt, turned oKer his annuity of1,000 iiKres a year to the Uoor of Uaris, Zarried the ZuHh younJer ZarieKare, and deKoted hiZseif to his writinJ. his traiHte des Hhiffres, whiHhwas written in 1585 desUite the distraHtion of a year-oid baby dauJhter,aUUeared, eieJantiy rubriHated, in 1586, and was reUrinted the foiiowinJyear. his autokey systeZ used the UiainteYt as the key. it UroKided aUriZinJ key. this Honsisted of a sinJie ietter, known to both enHiUhererand deHiUherer, with whiHh the deHiUherer Houid deHiUher the firstHryUtoJraZ ietter and so Jet a start on his, work. with this, he wouid Jetthe first UiainteYt ietter, then use this as the key to deHiUher the seHondHryUtoJraZ ietter, use that UiainteYt as the key to deHiUher the thirdHryUtoJraZ ietter, and so on.the systeZ works weii and affords fair Juarantees of seHurity; it hasbeen eZbodied in a nuZber of Zodern HiUher ZaHhines.in sUite of KiJenere's Hiear eYUosition of his teHhniBue, it was entireiyforJotten and oniy entered the streaZ of HryUtoioJy iate in the 19thHentury after it had been reinKented. writers on HryUtoioJy then addedinsuit to inEury by deJradinJ KiJenere's systeZ into one ZuHh ZoreeieZentary.the HiUher now uniKersaiiy Haiied the KiJenere eZUioys oniy standard aiUhabets and a short reUeatinJ keyword—a systeZ farZore susHeUtibie to soiution than KiJenere's autokey. its tabieauHonsists of a Zodern tabuia reHta: 26 "standard horiMontai aiUhabets,eaHh siid one sUaHe to the ieft of the one aboKe. these are the HiUheraiUhabets. a norZai aiUhabet for the UiainteYt stands at the toU. anothernorZai aiUhabet, whiHh Zereiy reUeats the initiai ietters of the horiMontaiHiUherteYt aiUhabets, runs down the ieft side. this is the key aiUhabet.both HorresUondents Zust know the keyword. the enHiUherer reUeatsthis aboKe the UiainteYt ietters untii eaHh one has a keyietter. he seeksthe UiainteYt ietter in the toU aiUhabet and the keyietter in the side. thenhe traHes down froZ the toU and in froZ the side. the HiUherteYt ietterstands at the interseHtion of the HoiuZn and the row. the enHiUhererreUeats this UroHess with aii the ietters of the UiainteYt. to deHiUher, theHierk beJins with the keyietter, runs in aionJ the HiUherteYt aiUhabetuntii he strikes the HiUher ietter, then foiiows the HoiuZn of iettersuUward untii he eZerJes at the UiainteYt ietter at the toU.UoiyaiUhabetiH HiUhers were, when used with ZiYed aiUhabets andwithout word diKisions, unbreakabie to the HryUtanaiysts of therenaissanHe. why, then, did the noZenHiator reiJn suUreZe for 300years? why did HryUtoJraUhers not use the UoiyaiUhabetiH systeZinstead?

Looking through this ciphertext we found the following common words, “attaHhed”, “Zission”, “diUlomat” and “haKe”, which are attached, mission, diplomat and have, H -> c, Z - > m, U -> p, K -> v, making theese subsitutions we will have the following ciphertext:

viJenere was born in the viiiaJe of saint-pourcain, about haifwaybetween paris and marseiiies, on aprii 5, 1523. at 24, he entered theservice of the duke of nevers, to whose house he remained attached therest of his iife, **eYcept** for periods at court and as a dipiomat. in 1549, at26, he went to rome on a two-year dipiomatic mission.it was here that he was first thrown into contact with cryptoioJy, andhe seems to have steeped himseif in it. he read the books of trithemius,beiaso, and other writers, and the unpubiished manuscript of aiberti. heevidentiy conversed with the eYperts of the papai curia, for he teiisanecdotes that he couid have heard oniy in the shoptaik of thesecryptoioJists. at 47, viJenere Buit the court, turned over his annuity of1,000 iivres a year to the poor of paris, married the much **younJer** marievare, and devoted himseif to his writinJ. his traicte des chiffres, whichwas written in 1585 despite the distraction of a year-oid baby dauJhter,appeared, eieJantiy rubricated, in 1586, and was reprinted the foiiowinJyear. his autokey system used the piainteYt as the key. it provided apriminJ key. this consisted of a sinJie ietter, known to both enciphererand decipherer, with which the decipherer couid decipher the firstcryptoJram ietter and so Jet a start on his, work. with this, he wouid Jetthe first piainteYt ietter, then use this as the key to decipher thesecondcryptoJram ietter, use that piainteYt as the key to decipher the thirdcryptoJram ietter, and so on.the systemworks weii and affords fair Juarantees of security; it hasbeen embodied in a number of modern cipher machines.in spite of viJenere's ciear eYposition of his **techniBue**, it was entireiyforJotten and oniy entered the stream of cryptoioJy iate in the 19thcentury after it had been reinvented. writers on cryptoioJy then addedinsuit to **inEury** by deJradinJ viJenere's system into one much moreeiementary.the cipher now universaiiy caiied the viJenere "empioys oniy standard aiphabets and a short repeatinJ keyword—a system farmore susceptibie to soiution than viJenere's autokey. its tabieauconsists of a modern tabuia recta: 26 standard **horiMontai** aiphabets,each siid one space to the ieft of the one above. these are the cipheraiphabets. a normai aiphabet for the piainteYt stands at the top. anothernormai aiphabet, which mereiy repeats the initiai ietters of the horiMontaicipherteYt aiphabets, runs down the ieft side. this is the key aiphabet.both correspondents must know the keyword. the encipherer repeatsthis above the piainteYt ietters untii each one has a keyietter. he seeksthe piainteYt ietter in the top aiphabet and the keyietter in the side. thenhe traces down from the top and in from the side. the cipherteYt ietterstands at the intersection of the coiumn and the row. the enciphererrepeats this process with aii the ietters of the piainteYt. to decipher, thecierk beJins with the keyietter, runs in aionJ the cipherteYt aiphabetuntii he strikes the cipher ietter, then foiiows the coiumn of iettersupward untii he emerJes at the piainteYt ietter at the top.poiyaiphabetic ciphers were, when used with miYed aiphabets andwithout word divisions, unbreakabie to the cryptanaiysts of therenaissance. why, then, did the nomenciator reiJn supreme for 300years? why did cryptoJraphers not use the poiyaiphabetic systeminstead?

Analysing the ciphertext we found the following common words, "eYcept", "younjer", "techniBue", "inEury" and "horiMontal" which are except, younger, technique, injury and horizontal, Y -> x, J -> g, B -> q, E ->j, M ->z. Making this substitution we get the final text, which is fully deciphered.

vigenere was born in the village of saint-pourcain, about half way between paris and marseilles, on april 5, 1523. at 24, he entered the service of the duke of nevers, to whose house he remained attached the rest of his life, except for periods at court and as a diplomat. in 1549, at 26, he went to rome on a two-year diplomatic mission.it was here that he was first thrown into contact with cryptology, and he seems to have steeped himself in it. he read the books of trithemius,belaso, and other writers, and the unpublished manuscript of alberti. he evidently conversed with the experts of the papal curia, for he tells anecdotes that he could have heard only in the shoptalk of thesecryptologists. at 47, vigenere quit the court, turned over his annuity of 1,000 livres a year to the poor of paris, married the much younger marievare, and devoted himself to his writing. his traicte des chiffres, which was written in 1585 despite the distraction of a year-old baby daughter,appeared, elegantly rubricated, in 1586, and was reprinted the following year. his autokey system used the plaintext as the key. it provided apriming key. this consisted of a single letter, known to both enciphererand decipherer, with which the decipherer could decipher the first cryptogram letter and so get a start on his, work. with this, he would get the first plaintext letter, then use this as the key to decipher the second cryptogram letter, use that plaintext as the key to decipher the third cryptogram letter, and so on.the system works well and affords fair guarantees of security; it has been embodied in a number of modern cipher machines.in spite of vigenere's clear exposition of his technique, it was entirely forgotten and only entered the stream of cryptology late in the 19th century after it had been reinvented. writers on cryptology then added insult to injury by degrading vigenere's system into one much more elementary.the cipher now universally called the vigenere employs only standard alphabets and a short repeating keyword—a system far more susceptible to solution than vigenere's autokey. its tableauconsists of a modern tabula recta: 26 standard horizontal alphabets,each slid one space to the left of the one above. these are the cipher alphabets. a normal alphabet for the plaintext stands at the top. another normal alphabet, which merely repeats the initial letters of the horizontal ciphertext alphabets, runs down the left side. this is the key alphabet.both correspondents must know the keyword. the encipherer repeats this above the plaintext letters until each one has a keyletter. he seeks the plaintext letter in the top alphabet and the key letter in the side. then he traces down from the top and in from the side. the ciphertext letter stands at the intersection of the column and the row. the encipherer repeats this process with all the letters of the plaintext. to decipher, the clerk begins with the key letter, runs in along the ciphertext alphabet until he strikes the cipher letter, then follows the column of letters upward until he emerges at the plaintext letter at the top.polyalphabetic ciphers were, when used with mixed alphabets and without word divisions, unbreakable to the cryptanalysts of the renaissance. why, then, did the nomenclator reign supreme for 300 years? why did cryptographers not use the polyalphabetic system instead?



The frequencies of the intercept are:

V	W	T	I	Q	X	N	P	G	S	O	U	H	F	D	C	R	Z	A	J	K	L	Y	B	M	E
402	318	193	186	183	176	167	162	160	113	97	88	75	57	53	49	47	46	37	33	23	23	15	2	2	1
14.8	11.7	7.1	6.9	6.8	6.5	6.2	6.0	5.9	4.2	3.6	3.2	2.8	2.1	2.0	1.8	1.7	1.7	1.4	1.2	0.8	0.8	0.6	0.1	0.1	0.0
e	t	a	r	h	i	o	s	n	i	d	p	c	y	u	f	w	m	b	g	v	k	x	q	z	j

Figure 3: Frequency of the intercept text with the substitutions that were made.

CONCLUSION

This laboratory work provided basic understading for the mono-alphabetic cipher tecnique, as I was able to decipher the provided text as per requirment. The algorithm consits of several parts, that involve the finding of the frequent letters and comparing them to the frequency of the alphabet that message was sent. Thus, finding common words, you can decipher the text efficiently.

Overall, this laboratory work was a great example of the mono-alphabetic cipher.