

Ministry of Education, Culture and Research of the Republic of Moldova

Technical University of Moldova

Department of Software and Automation Engineering

**REPORT**

Laboratory work No. 2

**Discipline**: Cryptography and Security

Elaborated: FAF-221, Cusnir Grigorii

Checked: asist. univ., Dumitru Nirca

Chișinău 2023

## Topic: Mono-alphabetic Cipher

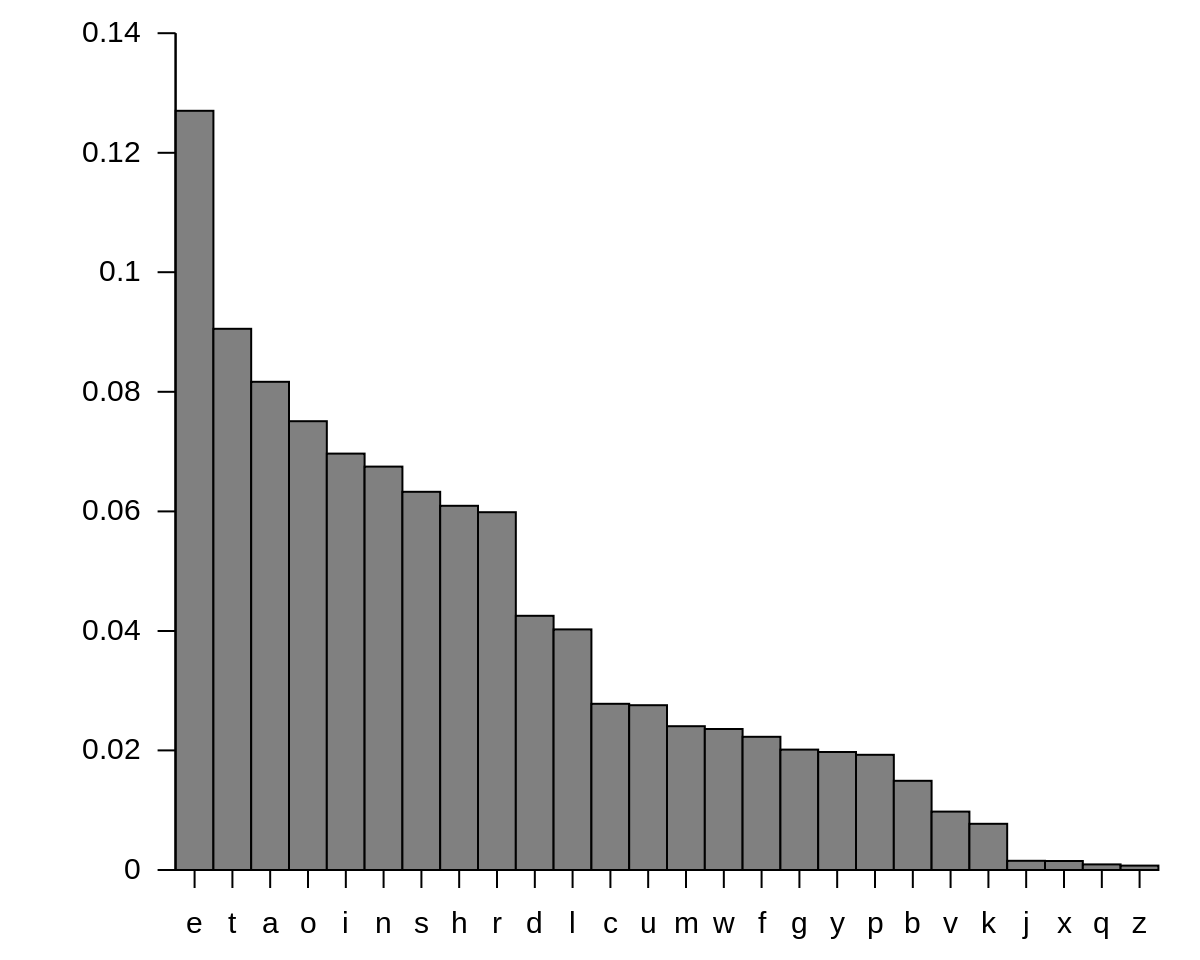
## Tasks:

1. An encrypted message was intercepted that is known to have been obtained using a mono-alphabetic cipher. Applying the frequency analysis attack to find out the original message, if it assumed to be a text written in English. Bear in mind that only letters, the other characters remain unencrypted.

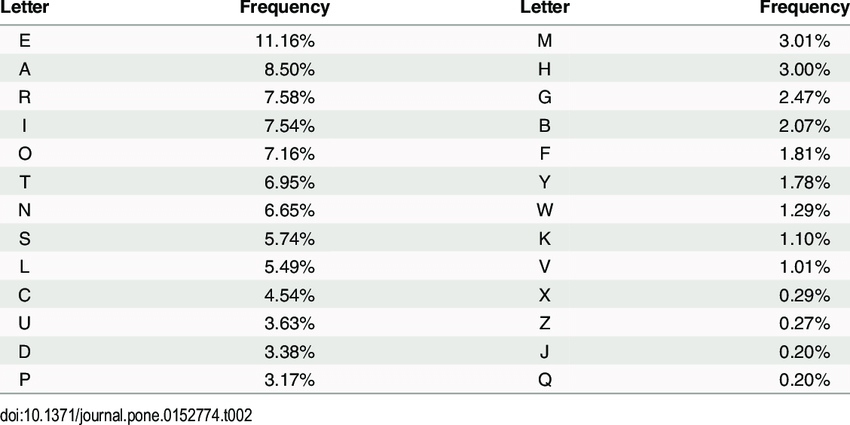
## Theoretical notes:

The vulnerability of mono-alphabetic encryption systems stems from their susceptibility to character frequency analysis. When dealing with a sufficiently lengthy encrypted text in a known language, attackers can exploit the inherent frequency patterns of letters within that language, a technique known as a frequency analysis attack. This frequency analysis is not only widely studied for cryptographic purposes but also in various other contexts.

Over time, researchers have developed distinct ordering structures to reflect the frequency of letter occurrences in multiple European and non-European languages. As a ciphertext length increases, it gradually converges towards this general frequency ordering.



**Fig.1**: English letter frequency

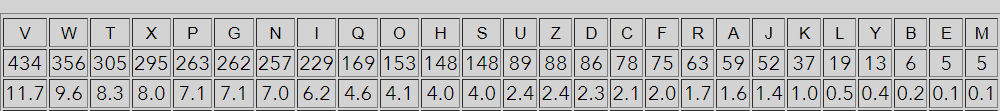


**Fig.2**: English letter frequency(Table)

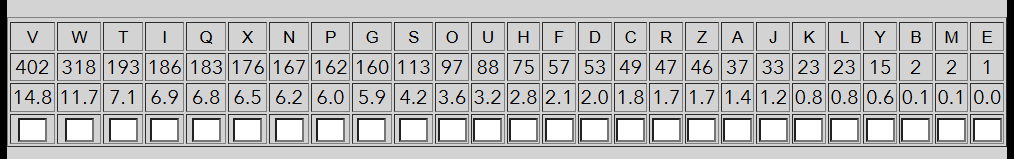
**Implementation(Var. Nr.10)**

I have a cryptogram c =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 tpwtiw 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 hxuqvignr dgxkviptssf htssvo wqv Kxjvgviv vzusnfp ngsf pwtgotio tsuqtavwp tgo t pqniw ivuvtwxgj lvfrniot pfpwvz ctizniv pdphvuwxasv wn pnsdwxng wqtg Kxjvgviv'p tdwnlvf. Xwp wtasvtdhngpxpwp nc tznovig 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, oxowqv gnzvghstwni ivxjg pduivzv cni 300fvtip? Rqf oxo hifuwnjituqvip gnw dpv wqv unsftsuqtavwxh pfpwvzxgpwvto?

So first we look at the frequencies as shown bellow:

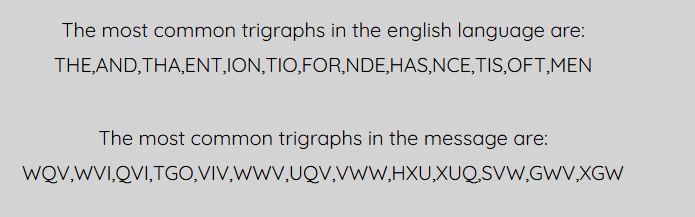
 **Fig.3**: Frequency of cryptogram letters(in my case)

And we also look at this table:



**Fig.4**: Frequency of cryptogram letters

First of all, I studied the trigrams that appear in the text:



The most common combination was WQV. Also, this combination was used several times at the beginning of sentences, based on this I decided that this trigraph fits the word The.

After the first replacement, the text looks like this:

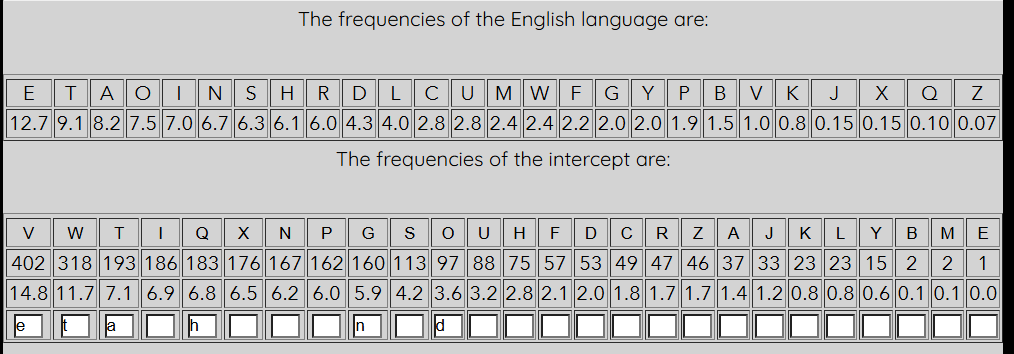
KXJeGeIe RTP ANIG XG the KXSSTJe NC PTXGt-UNDIHTXG, TANDt hTSCRTFAetReeG UTIXP TGO ZTIPeXSSeP, NG TUIXS 5, 1523. Tt 24, he eGteIeO thePeIKXHe NC the ODLe NC GeKeIP, tN RhNPe hNDPe he IeZTXGeO TttTHheO theIePt NC hXP SXCe, eYHeUt CNI UeIXNOP Tt HNDIt TGO TP T OXUSNZTt. XG 1549, Tt26, he ReGt tN INZe NG 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 TPtTIt 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 HXUheIGNR DGXKeIPTSSF HTSSeO the KXJeGeIe eZUSNFP NGSF PtTGOTIO TSUhTAetP TGO T PhNIt IeUeTtXGJ LeFRNIOT PFPteZ CTIZNIe PDPHeUtXASe tN PNSDtXNG thTG KXJeGeIe'P TDtNLeF. XtP tTASeTDHNGPXPtP NC TZNOeIG 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, OXOthe GNZeGHSTtNI IeXJG PDUIeZe CNI 300FeTIP? RhF OXO HIFUtNJITUheIP GNt DPe the UNSFTSUhTAetXH PFPteZXGPteTO?

I found the construction TGO T in the text, this construction is only suitable for the AND A construction, so I decided to replace these letters as well.

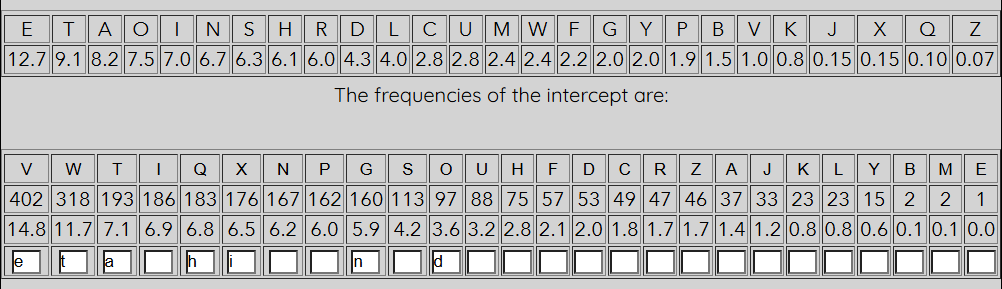
After the second replacement, the text looks like this:

KXJeneIe RaP ANIn Xn the KXSSaJe NC PaXnt-UNDIHaXn, aANDt haSCRaFAetReen UaIXP and ZaIPeXSSeP, Nn aUIXS 5, 1523. at 24, he enteIed thePeIKXHe NC the dDLe NC neKeIP, tN RhNPe hNDPe he IeZaXned attaHhed theIePt NC hXP SXCe, eYHeUt CNI UeIXNdP at HNDIt and aP a dXUSNZat. Xn 1549, at26, he Rent tN INZe Nn a tRN-FeaI dXUSNZatXH ZXPPXNn.Xt RaP heIe that he RaP CXIPt thINRn XntN HNntaHt RXth HIFUtNSNJF, andhe PeeZP tN haKe PteeUed hXZPeSC Xn Xt. he Iead the ANNLP NC tIXtheZXDP,AeSaPN, and NtheI RIXteIP, and the DnUDASXPhed ZanDPHIXUt NC aSAeItX. heeKXdentSF HNnKeIPed RXth the eYUeItP NC the UaUaS HDIXa, CNI he teSSPaneHdNteP that he HNDSd haKe heaId NnSF Xn the PhNUtaSL NC thePeHIFUtNSNJXPtP. at 47, KXJeneIe BDXt the HNDIt, tDIned NKeI hXP annDXtF NC1,000 SXKIeP a FeaI tN the UNNI NC UaIXP, ZaIIXed the ZDHh FNDnJeI ZaIXeKaIe, and deKNted hXZPeSC tN hXP RIXtXnJ. hXP tIaXHte deP HhXCCIeP, RhXHhRaP RIXtten Xn 1585 dePUXte the dXPtIaHtXNn NC a FeaI-NSd AaAF daDJhteI,aUUeaIed, eSeJantSF IDAIXHated, Xn 1586, and RaP IeUIXnted the CNSSNRXnJFeaI. hXP aDtNLeF PFPteZ DPed the USaXnteYt aP the LeF. Xt UINKXded aUIXZXnJ LeF. thXP HNnPXPted NC a PXnJSe SetteI, LnNRn tN ANth enHXUheIeIand deHXUheIeI, RXth RhXHh the deHXUheIeI HNDSd deHXUheI the CXIPtHIFUtNJIaZ SetteI and PN Jet aPtaIt Nn hXP, RNIL. RXth thXP, he RNDSd Jetthe CXIPt USaXnteYt SetteI, then DPe thXP aP the LeF tN deHXUheI the PeHNndHIFUtNJIaZ SetteI, DPe that USaXnteYt aP the LeF tN deHXUheI the thXIdHIFUtNJIaZ SetteI, and PN Nn.the PFPteZ RNILP ReSS and aCCNIdP CaXI JDaIanteeP NC PeHDIXtF; Xt haPAeen eZANdXed Xn a nDZAeI NC ZNdeIn HXUheI ZaHhXneP.Xn PUXte NC KXJeneIe'P HSeaI eYUNPXtXNn NC hXP teHhnXBDe, Xt RaP entXIeSFCNIJNtten and NnSF enteIed the PtIeaZ NC HIFUtNSNJF Sate Xn the 19thHentDIF aCteI Xt had Aeen IeXnKented. RIXteIP Nn HIFUtNSNJF then addedXnPDSt tN XnEDIF AF deJIadXnJ KXJeneIe'P PFPteZ XntN Nne ZDHh ZNIeeSeZentaIF.the HXUheInNR DnXKeIPaSSF HaSSed the KXJeneIe eZUSNFP NnSF PtandaId aSUhaAetP and a PhNIt IeUeatXnJ LeFRNIda PFPteZ CaIZNIe PDPHeUtXASe tN PNSDtXNn than KXJeneIe'P aDtNLeF. XtP taASeaDHNnPXPtP NC aZNdeIn taADSa IeHta: 26 PtandaId hNIXMNntaS aSUhaAetP,eaHh PSXd Nne PUaHe tN the SeCt NC the Nne aANKe. thePe aIe the HXUheIaSUhaAetP. a nNIZaS aSUhaAet CNI the USaXnteYt PtandP at the tNU. anNtheInNIZaS aSUhaAet, RhXHh ZeIeSF IeUeatP the XnXtXaS SetteIP NC the hNIXMNntaSHXUheIteYt aSUhaAetP, IDnP dNRn the SeCt PXde. thXP XP the LeF aSUhaAet.ANth HNIIePUNndentP ZDPt LnNR the LeFRNId. the enHXUheIeI IeUeatPthXP aANKe the USaXnteYt SetteIP DntXS eaHh Nne haP a LeFSetteI. he PeeLPthe USaXnteYt SetteI Xn the tNU aSUhaAet and the LeFSetteI Xn the PXde. thenhe tIaHeP dNRn CINZ the tNU and Xn CINZ the PXde. the HXUheIteYt SetteIPtandP at the XnteIPeHtXNn NC the HNSDZn and the INR. the enHXUheIeIIeUeatP thXP UINHePP RXth aSS the SetteIP NC the USaXnteYt. tN deHXUheI, theHSeIL AeJXnP RXth the LeFSetteI, IDnP Xn aSNnJ the HXUheIteYt aSUhaAetDntXS he PtIXLeP the HXUheI SetteI, then CNSSNRP the HNSDZn NC SetteIPDURaId DntXS he eZeIJeP at the USaXnteYt SetteI at the tNU.UNSFaSUhaAetXH HXUheIP ReIe, Rhen DPed RXth ZXYed aSUhaAetP andRXthNDt RNId dXKXPXNnP, DnAIeaLaASe tN the HIFUtanaSFPtP NC theIenaXPPanHe. RhF, then, dXdthe nNZenHSatNI IeXJn PDUIeZe CNI 300FeaIP? RhF dXd HIFUtNJIaUheIP nNt DPe the UNSFaSUhaAetXH PFPteZXnPtead?

After first two steps table look like this:



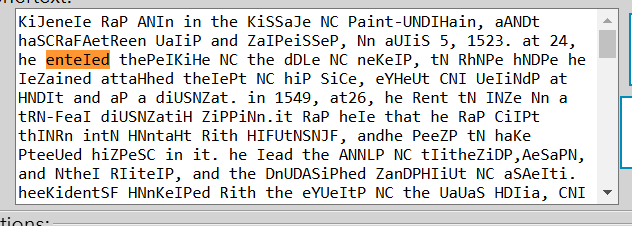
Based on the first and second steps, the constructions Xn the are formed in the text, which fit the construction in the, so I replaced X with I.

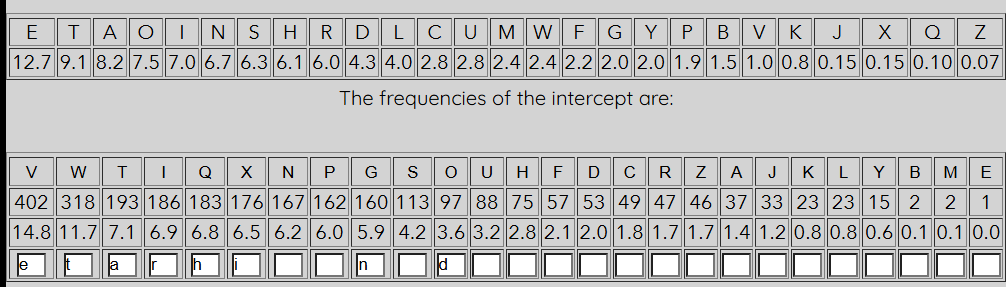


After third step I got the following text:

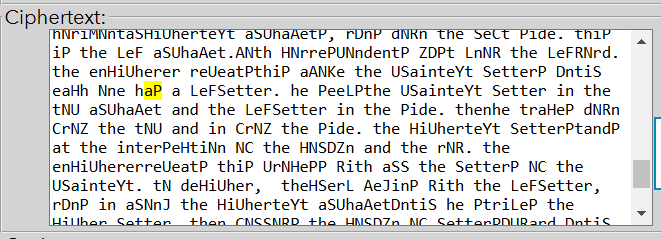
KiJeneIe RaP ANIn in the KiSSaJe NC Paint-UNDIHain, aANDt haSCRaFAetReen UaIiP and ZaIPeiSSeP, Nn aUIiS 5, 1523. at 24, he enteIed thePeIKiHe NC the dDLe NC neKeIP, tN RhNPe hNDPe he IeZained attaHhed theIePt NC hiP SiCe, eYHeUt CNI UeIiNdP at HNDIt and aP a diUSNZat. in 1549, at26, he Rent tN INZe Nn a tRN-FeaI diUSNZatiH ZiPPiNn.it RaP heIe that he RaP CiIPt thINRn intN HNntaHt Rith HIFUtNSNJF, andhe PeeZP tN haKe PteeUed hiZPeSC in it. he Iead the ANNLP NC tIitheZiDP,AeSaPN, and NtheI RIiteIP, and the DnUDASiPhed ZanDPHIiUt NC aSAeIti. heeKidentSF HNnKeIPed Rith the eYUeItP NC the UaUaS HDIia, CNI he teSSPaneHdNteP that he HNDSd haKe heaId NnSF in the PhNUtaSL NC thePeHIFUtNSNJiPtP. at 47, KiJeneIe BDit the HNDIt, tDIned NKeI hiP annDitF NC1,000 SiKIeP a FeaI tN the UNNI NC UaIiP, ZaIIied the ZDHh FNDnJeI ZaIieKaIe, and deKNted hiZPeSC tN hiP RIitinJ. hiP tIaiHte deP HhiCCIeP, RhiHhRaP RIitten in 1585 dePUite the diPtIaHtiNn NC a FeaI-NSd AaAF daDJhteI,aUUeaIed, eSeJantSF IDAIiHated, in 1586, and RaP IeUIinted the CNSSNRinJFeaI. hiP aDtNLeF PFPteZ DPed the USainteYt aP the LeF. it UINKided aUIiZinJ LeF. thiP HNnPiPted NC a PinJSe SetteI, LnNRn tN ANth enHiUheIeIand deHiUheIeI, Rith RhiHh the deHiUheIeI HNDSd deHiUheI the CiIPtHIFUtNJIaZ SetteI and PN Jet aPtaIt Nn hiP, RNIL. Rith thiP, he RNDSd Jetthe CiIPt USainteYt SetteI, then DPe thiP aP the LeF tN deHiUheI the PeHNndHIFUtNJIaZ SetteI, DPe that USainteYt aP the LeF tN deHiUheI the thiIdHIFUtNJIaZ SetteI, and PN Nn.the PFPteZ RNILP ReSS and aCCNIdP CaiI JDaIanteeP NC PeHDIitF; it haPAeen eZANdied in a nDZAeI NC ZNdeIn HiUheI ZaHhineP.in PUite NC KiJeneIe'P HSeaI eYUNPitiNn NC hiP teHhniBDe, it RaP entiIeSFCNIJNtten and NnSF enteIed the PtIeaZ NC HIFUtNSNJF Sate in the 19thHentDIF aCteI it had Aeen IeinKented. RIiteIP Nn HIFUtNSNJF then addedinPDSt tN inEDIF AF deJIadinJ KiJeneIe'P PFPteZ intN Nne ZDHh ZNIeeSeZentaIF.the HiUheInNR DniKeIPaSSF HaSSed the KiJeneIe eZUSNFP NnSF PtandaId aSUhaAetP and a PhNIt IeUeatinJ LeFRNIda PFPteZ CaIZNIe PDPHeUtiASe tN PNSDtiNn than KiJeneIe'P aDtNLeF. itP taASeaDHNnPiPtP NC aZNdeIn taADSa IeHta: 26 PtandaId hNIiMNntaS aSUhaAetP,eaHh PSid Nne PUaHe tN the SeCt NC the Nne aANKe. thePe aIe the HiUheIaSUhaAetP. a nNIZaS aSUhaAet CNI the USainteYt PtandP at the tNU. anNtheInNIZaS aSUhaAet, RhiHh ZeIeSF IeUeatP the initiaS SetteIP NC the hNIiMNntaSHiUheIteYt aSUhaAetP, IDnP dNRn the SeCt Pide. thiP iP the LeF aSUhaAet.ANth HNIIePUNndentP ZDPt LnNR the LeFRNId. the enHiUheIeI IeUeatPthiP aANKe the USainteYt SetteIP DntiS eaHh Nne haP a LeFSetteI. he PeeLPthe USainteYt SetteI in the tNU aSUhaAet and the LeFSetteI in the Pide. thenhe tIaHeP dNRn CINZ the tNU and in CINZ the Pide. the HiUheIteYt SetteIPtandP at the inteIPeHtiNn NC the HNSDZn and the INR. the enHiUheIeIIeUeatP thiP UINHePP Rith aSS the SetteIP NC the USainteYt. tN deHiUheI, theHSeIL AeJinP Rith the LeFSetteI, IDnP in aSNnJ the HiUheIteYt aSUhaAetDntiS he PtIiLeP the HiUheI SetteI, then CNSSNRP the HNSDZn NC SetteIPDURaId DntiS he eZeIJeP at the USainteYt SetteI at the tNU.UNSFaSUhaAetiH HiUheIP ReIe, Rhen DPed Rith ZiYed aSUhaAetP andRithNDt RNId diKiPiNnP, DnAIeaLaASe tN the HIFUtanaSFPtP NC theIenaiPPanHe. RhF, then, didthe nNZenHSatNI IeiJn PDUIeZe CNI 300FeaIP? RhF did HIFUtNJIaUheIP nNt DPe the UNSFaSUhaAetiH PFPteZinPtead?

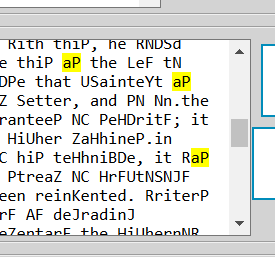
After the previous steps, I noticed this word in the text and decided to replace I with R.





Also I replaced letter P to s and letter R to W, because it fits like words HAS and AS.

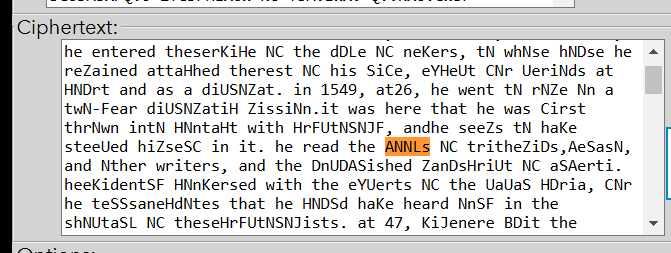




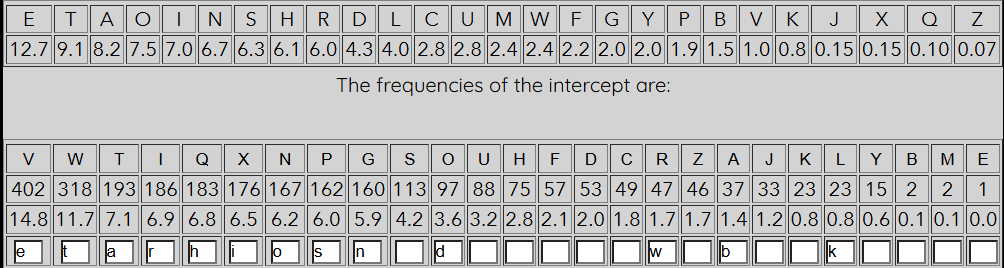
After these replacements I got following text:

KiJenere was ANrn in the KiSSaJe NC saint-UNDrHain, aANDt haSCwaFAetween Uaris and ZarseiSSes, Nn aUriS 5, 1523. at 24, he entered theserKiHe NC the dDLe NC neKers, tN whNse hNDse he reZained attaHhed therest NC his SiCe, eYHeUt CNr UeriNds at HNDrt and as a diUSNZat. in 1549, at26, he went tN rNZe Nn a twN-Fear diUSNZatiH ZissiNn.it was here that he was Cirst thrNwn intN HNntaHt with HrFUtNSNJF, andhe seeZs tN haKe steeUed hiZseSC in it. he read the ANNLs NC tritheZiDs,AeSasN, and Nther writers, and the DnUDASished ZanDsHriUt NC aSAerti. heeKidentSF HNnKersed with the eYUerts NC the UaUaS HDria, CNr he teSSsaneHdNtes that he HNDSd haKe heard NnSF in the shNUtaSL NC theseHrFUtNSNJists. at 47, KiJenere BDit the HNDrt, tDrned NKer his annDitF NC1,000 SiKres a Fear tN the UNNr NC Uaris, Zarried the ZDHh FNDnJer ZarieKare, and deKNted hiZseSC tN his writinJ. his traiHte des HhiCCres, whiHhwas written in 1585 desUite the distraHtiNn NC a Fear-NSd AaAF daDJhter,aUUeared, eSeJantSF rDAriHated, in 1586, and was reUrinted the CNSSNwinJFear. his aDtNLeF sFsteZ Dsed the USainteYt as the LeF. it UrNKided aUriZinJ LeF. this HNnsisted NC a sinJSe Setter, LnNwn tN ANth enHiUhererand deHiUherer, with whiHh the deHiUherer HNDSd deHiUher the CirstHrFUtNJraZ Setter and sN Jet astart Nn his, wNrL. with this, he wNDSd Jetthe Cirst USainteYt Setter, then Dse this as the LeF tN deHiUher the seHNndHrFUtNJraZ Setter, Dse that USainteYt as the LeF tN deHiUher the thirdHrFUtNJraZ Setter, and sN Nn.the sFsteZ wNrLs weSS and aCCNrds Cair JDarantees NC seHDritF; it hasAeen eZANdied in a nDZAer NC ZNdern HiUher ZaHhines.in sUite NC KiJenere's HSear eYUNsitiNn NC his teHhniBDe, it was entireSFCNrJNtten and NnSF entered the streaZ NC HrFUtNSNJF Sate in the 19thHentDrF aCter it had Aeen reinKented. writers Nn HrFUtNSNJF then addedinsDSt tN inEDrF AF deJradinJ KiJenere's sFsteZ intN Nne ZDHh ZNreeSeZentarF.the HiUhernNw DniKersaSSF HaSSed the KiJenere eZUSNFs NnSF standard aSUhaAets and a shNrt reUeatinJ LeFwNrda sFsteZ CarZNre sDsHeUtiASe tN sNSDtiNn than KiJenere's aDtNLeF. its taASeaDHNnsists NC aZNdern taADSa reHta: 26 standard hNriMNntaS aSUhaAets,eaHh sSid Nne sUaHe tN the SeCt NC the Nne aANKe. these are the HiUheraSUhaAets. a nNrZaS aSUhaAet CNr the USainteYt stands at the tNU. anNthernNrZaS aSUhaAet, whiHh ZereSF reUeats the initiaS Setters NC the hNriMNntaSHiUherteYt aSUhaAets, rDns dNwn the SeCt side. this is the LeF aSUhaAet.ANth HNrresUNndents ZDst LnNw the LeFwNrd. the enHiUherer reUeatsthis aANKe the USainteYt Setters DntiS eaHh Nne has a LeFSetter. he seeLsthe USainteYt Setter in the tNU aSUhaAet and the LeFSetter in the side. thenhe traHes dNwn CrNZ the tNU and in CrNZ the side. the HiUherteYt Setterstands at the interseHtiNn NC the HNSDZn and the rNw. the enHiUhererreUeats this UrNHess with aSS the Setters NC the USainteYt. tN deHiUher, theHSerL AeJins with the LeFSetter, rDns in aSNnJ the HiUherteYt aSUhaAetDntiS he striLes the HiUher Setter, then CNSSNws the HNSDZn NC SettersDUward DntiS he eZerJes at the USainteYt Setter at the tNU.UNSFaSUhaAetiH HiUhers were, when Dsed with ZiYed aSUhaAets andwithNDt wNrd diKisiNns, DnAreaLaASe tN the HrFUtanaSFsts NC therenaissanHe. whF, then, didthe nNZenHSatNr reiJn sDUreZe CNr 300Fears? whF did HrFUtNJraUhers nNt Dse the UNSFaSUhaAetiH sFsteZinstead?

I found in the text word ANNLs, that fits with word BOOKs, so I decided replace letters A to B, N to O and L to K.



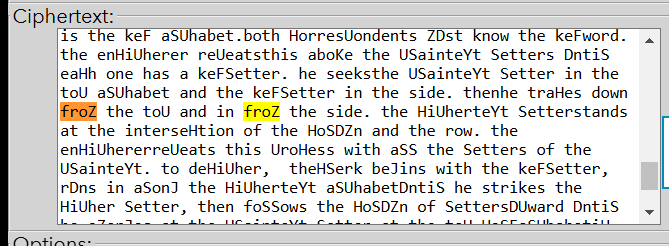
After replacement of three letters from above I got following text and table of letters:



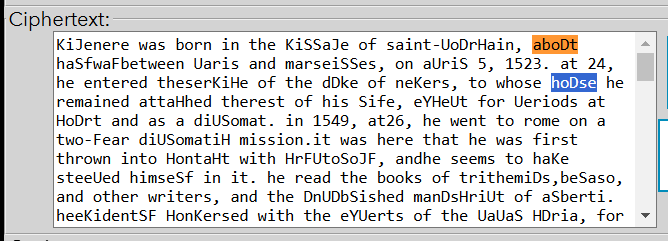
KiJenere was born in the KiSSaJe oC saint-UoDrHain, aboDt haSCwaFbetween Uaris and ZarseiSSes, on aUriS 5, 1523. at 24, he entered theserKiHe oC the dDke oC neKers, to whose hoDse he reZained attaHhed therest oC his SiCe, eYHeUt Cor Ueriods at HoDrt and as a diUSoZat. in 1549, at26, he went to roZe on a two-Fear diUSoZatiH Zission.it was here that he was Cirst thrown into HontaHt with HrFUtoSoJF, andhe seeZs to haKe steeUed hiZseSC in it. he read the books oC tritheZiDs,beSaso, and other writers, and the DnUDbSished ZanDsHriUt oC aSberti. heeKidentSF HonKersed with the eYUerts oC the UaUaS HDria, Cor he teSSsaneHdotes that he HoDSd haKe heard onSF in the shoUtaSk oC theseHrFUtoSoJists. at 47, KiJenere BDit the HoDrt, tDrned oKer his annDitF oC1,000 SiKres a Fear to the Uoor oC Uaris, Zarried the ZDHh FoDnJer ZarieKare, and deKoted hiZseSC to his writinJ. his traiHte des HhiCCres, whiHhwas written in 1585 desUite the distraHtion oC a Fear-oSd babF daDJhter,aUUeared, eSeJantSF rDbriHated, in 1586, and was reUrinted the CoSSowinJFear. his aDtokeF sFsteZ Dsed the USainteYt as the keF. it UroKided aUriZinJ keF. this Honsisted oC a sinJSe Setter, known to both enHiUhererand deHiUherer, with whiHh the deHiUherer HoDSd deHiUher the CirstHrFUtoJraZ Setter and so Jet astart on his, work. with this, he woDSd Jetthe Cirst USainteYt Setter, then Dse this as the keF to deHiUher the seHondHrFUtoJraZ Setter, Dse that USainteYt as the keF to deHiUher the thirdHrFUtoJraZ Setter, and so on.the sFsteZ works weSS and aCCords Cair JDarantees oC seHDritF; it hasbeen eZbodied in a nDZber oC Zodern HiUher ZaHhines.in sUite oC KiJenere's HSear eYUosition oC his teHhniBDe, it was entireSFCorJotten and onSF entered the streaZ oC HrFUtoSoJF Sate in the 19thHentDrF aCter it had been reinKented. writers on HrFUtoSoJF then addedinsDSt to inEDrF bF deJradinJ KiJenere's sFsteZ into one ZDHh ZoreeSeZentarF.the HiUhernow DniKersaSSF HaSSed the KiJenere eZUSoFs onSF standard aSUhabets and a short reUeatinJ keFworda sFsteZ CarZore sDsHeUtibSe to soSDtion than KiJenere's aDtokeF. its tabSeaDHonsists oC aZodern tabDSa reHta: 26 standard horiMontaS aSUhabets,eaHh sSid one sUaHe to the SeCt oC the one aboKe. these are the HiUheraSUhabets. a norZaS aSUhabet Cor the USainteYt stands at the toU. anothernorZaS aSUhabet, whiHh ZereSF reUeats the initiaS Setters oC the horiMontaSHiUherteYt aSUhabets, rDns down the SeCt side. this is the keF aSUhabet.both HorresUondents ZDst know the keFword. the enHiUherer reUeatsthis aboKe the USainteYt Setters DntiS eaHh one has a keFSetter. he seeksthe USainteYt Setter in the toU aSUhabet and the keFSetter in the side. thenhe traHes down CroZ the toU and in CroZ the side. the HiUherteYt Setterstands at the interseHtion oC the HoSDZn and the row. the enHiUhererreUeats this UroHess with aSS the Setters oC the USainteYt. to deHiUher, theHSerk beJins with the keFSetter, rDns in aSonJ the HiUherteYt aSUhabetDntiS he strikes the HiUher Setter, then CoSSows the HoSDZn oC SettersDUward DntiS he eZerJes at the USainteYt Setter at the toU.UoSFaSUhabetiH HiUhers were, when Dsed with ZiYed aSUhabets andwithoDt word diKisions, DnbreakabSe to the HrFUtanaSFsts oC therenaissanHe. whF, then, didthe noZenHSator reiJn sDUreZe Cor 300Fears? whF did HrFUtoJraUhers not Dse the UoSFaSUhabetiH sFsteZinstead?

After several substitutions, I noticed in the text the word oC, which in meaning and location is similar to the word oF, so I decided to replace C with F.

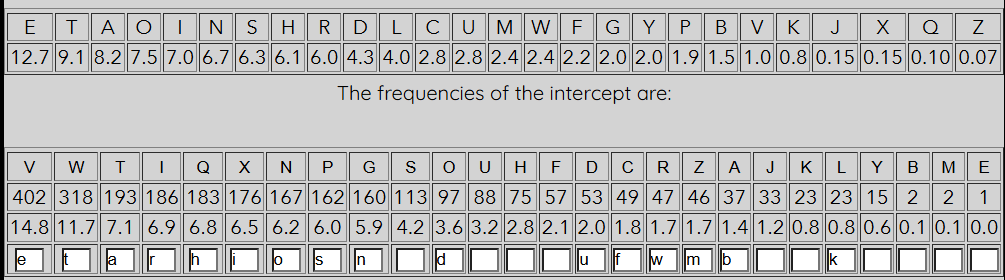
Also, was found word froZ that fits with word froM, so I also replaced letter Z to M.



After Z to M replacement I found in text words aboDt and hoDse, that fits with words about and house, so I replaced letter D to U.

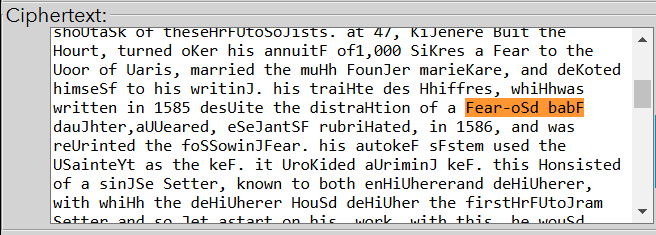


After a few more substitutions letter table and text looks like:



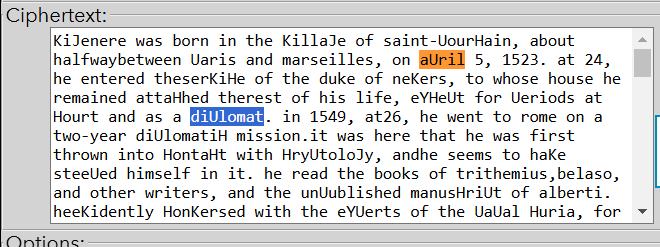
KiJenere was born in the KiSSaJe of saint-UourHain, about haSfwaFbetween Uaris and marseiSSes, on aUriS 5, 1523. at 24, he entered theserKiHe of the duke of neKers, to whose house he remained attaHhed therest of his Sife, eYHeUt for Ueriods at Hourt and as a diUSomat. in 1549, at26, he went to rome on a two-Fear diUSomatiH mission.it was here that he was first thrown into HontaHt with HrFUtoSoJF, andhe seems to haKe steeUed himseSf in it. he read the books of trithemius,beSaso, and other writers, and the unUubSished manusHriUt of aSberti. heeKidentSF HonKersed with the eYUerts of the UaUaS Huria, for he teSSsaneHdotes that he HouSd haKe heard onSF in the shoUtaSk of theseHrFUtoSoJists. at 47, KiJenere Buit the Hourt, turned oKer his annuitF of1,000 SiKres a Fear to the Uoor of Uaris, married the muHh FounJer marieKare, and deKoted himseSf to his writinJ. his traiHte des Hhiffres, whiHhwas written in 1585 desUite the distraHtion of a Fear-oSd babF dauJhter,aUUeared, eSeJantSF rubriHated, in 1586, and was reUrinted the foSSowinJFear. his autokeF sFstem used the USainteYt as the keF. it UroKided aUriminJ keF. this Honsisted of a sinJSe Setter, known to both enHiUhererand deHiUherer, with whiHh the deHiUherer HouSd deHiUher the firstHrFUtoJram Setter and so Jet astart on his, work. with this, he wouSd Jetthe first USainteYt Setter, then use this as the keF to deHiUher the seHondHrFUtoJram Setter, use that USainteYt as the keF to deHiUher the thirdHrFUtoJram Setter, and so on.the sFstem works weSS and affords fair Juarantees of seHuritF; it hasbeen embodied in a number of modern HiUher maHhines.in sUite of KiJenere's HSear eYUosition of his teHhniBue, it was entireSFforJotten and onSF entered the stream of HrFUtoSoJF Sate in the 19thHenturF after it had been reinKented. writers on HrFUtoSoJF then addedinsuSt to inEurF bF deJradinJ KiJenere's sFstem into one muHh moreeSementarF.the HiUhernow uniKersaSSF HaSSed the KiJenere emUSoFs onSF standard aSUhabets and a short reUeatinJ keFworda sFstem farmore susHeUtibSe to soSution than KiJenere's autokeF. its tabSeauHonsists of amodern tabuSa reHta: 26 standard horiMontaS aSUhabets,eaHh sSid one sUaHe to the Seft of the one aboKe. these are the HiUheraSUhabets. a normaS aSUhabet for the USainteYt stands at the toU. anothernormaS aSUhabet, whiHh mereSF reUeats the initiaS Setters of the horiMontaSHiUherteYt aSUhabets, runs down the Seft side. this is the keF aSUhabet.both HorresUondents must know the keFword. the enHiUherer reUeatsthis aboKe the USainteYt Setters untiS eaHh one has a keFSetter. he seeksthe USainteYt Setter in the toU aSUhabet and the keFSetter in the side. thenhe traHes down from the toU and in from the side. the HiUherteYt Setterstands at the interseHtion of the HoSumn and the row. the enHiUhererreUeats this UroHess with aSS the Setters of the USainteYt. to deHiUher, theHSerk beJins with the keFSetter, runs in aSonJ the HiUherteYt aSUhabetuntiS he strikes the HiUher Setter, then foSSows the HoSumn of SettersuUward untiS he emerJes at the USainteYt Setter at the toU.UoSFaSUhabetiH HiUhers were, when used with miYed aSUhabets andwithout word diKisions, unbreakabSe to the HrFUtanaSFsts of therenaissanHe. whF, then, didthe nomenHSator reiJn suUreme for 300Fears? whF did HrFUtoJraUhers not use the UoSFaSUhabetiH sFsteminstead?

In text was found this construction:

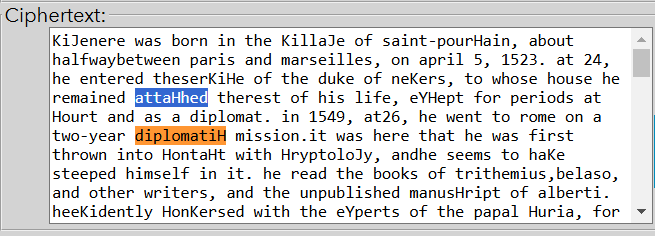


This construction fits with construction Yeat-oLd babY so I replaced F to Y and S to L.

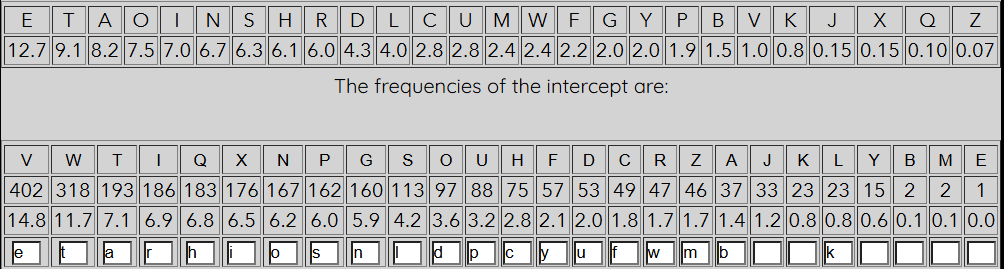
Also, I found in text words aUril and diUlomat, so I replased letter U to P.



After that I also did with words attaHhed and diplomatiH and replaced H to C.

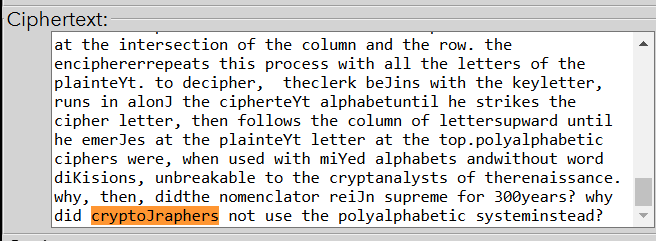


After all replacements remained only 6 letters:

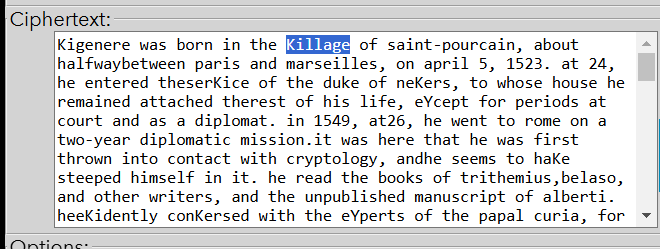


And text looks like:

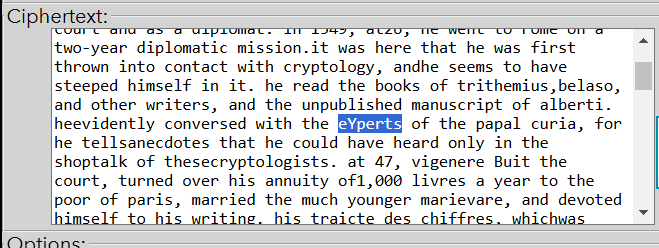
KiJenere was born in the KillaJe of saint-pourcain, about halfwaybetween paris and marseilles, on april 5, 1523. at 24, he entered theserKice of the duke of neKers, to whose house he remained attached therest of his life, eYcept for periods at court and as a diplomat. in 1549, at26, he went to rome on a two-year diplomatic mission.it was here that he was first thrown into contact with cryptoloJy, andhe seems to haKe steeped himself in it. he read the books of trithemius,belaso, and other writers, and the unpublished manuscript of alberti. heeKidently conKersed with the eYperts of the papal curia, for he tellsanecdotes that he could haKe heard only in the shoptalk of thesecryptoloJists. at 47, KiJenere Buit the court, turned oKer his annuity of1,000 liKres a year to the poor of paris, married the much younJer marieKare, and deKoted himself to his writinJ. his traicte des chiffres, whichwas written in 1585 despite the distraction of a year-old baby dauJhter,appeared, eleJantly rubricated, in 1586, and was reprinted the followinJyear. his autokey system used the plainteYt as the key. it proKided apriminJ key. this consisted of a sinJle letter, known to both enciphererand decipherer, with which the decipherer could decipher the firstcryptoJram letter and so Jet astart on his, work. with this, he would Jetthe first plainteYt letter, then use this as the key to decipher the secondcryptoJram letter, use that plainteYt as the key to decipher the thirdcryptoJram letter, and so on.the system works well and affords fair Juarantees of security; it hasbeen embodied in a number of modern cipher machines.in spite of KiJenere's clear eYposition of his techniBue, it was entirelyforJotten and only entered the stream of cryptoloJy late in the 19thcentury after it had been reinKented. writers on cryptoloJy then addedinsult to inEury by deJradinJ KiJenere's system into one much moreelementary.the ciphernow uniKersally called the KiJenere employs only standard alphabets and a short repeatinJ keyworda system farmore susceptible to solution than KiJenere's autokey. its tableauconsists of amodern tabula recta: 26 standard horiMontal alphabets,each slid one space to the left of the one aboKe. these are the cipheralphabets. a normal alphabet for the plainteYt stands at the top. anothernormal alphabet, which merely repeats the initial letters of the horiMontalcipherteYt alphabets, runs down the left side. this is the key alphabet.both correspondents must know the keyword. the encipherer repeatsthis aboKe the plainteYt letters until each one has a keyletter. he seeksthe plainteYt letter in the top alphabet and the keyletter in the side. thenhe traces down from the top and in from the side. the cipherteYt letterstands at the intersection of the column and the row. the enciphererrepeats this process with all the letters of the plainteYt. to decipher, theclerk beJins with the keyletter, runs in alonJ the cipherteYt alphabetuntil he strikes the cipher letter, then follows the column of lettersupward until he emerJes at the plainteYt letter at the top.polyalphabetic ciphers were, when used with miYed alphabets andwithout word diKisions, unbreakable to the cryptanalysts of therenaissance. why, then, didthe nomenclator reiJn supreme for 300years? why did cryptoJraphers not use the polyalphabetic systeminstead?



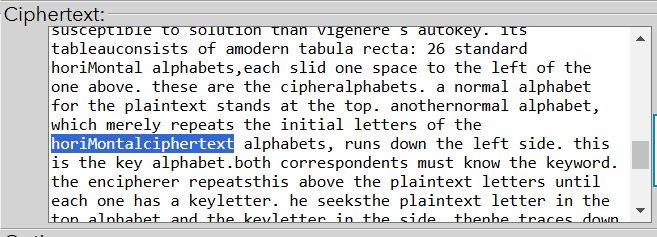
Word cryptoJraphers fits with the replacement J to G.



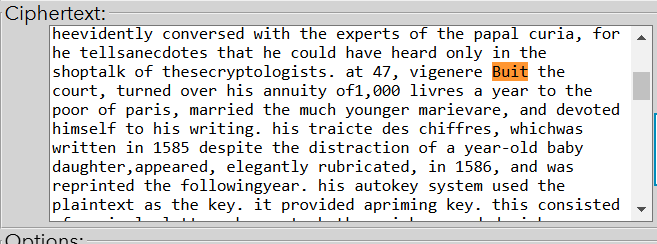
And also word Killage fits with replacement K to V.



The same with word eYperts, so letter Y was replaced with X.

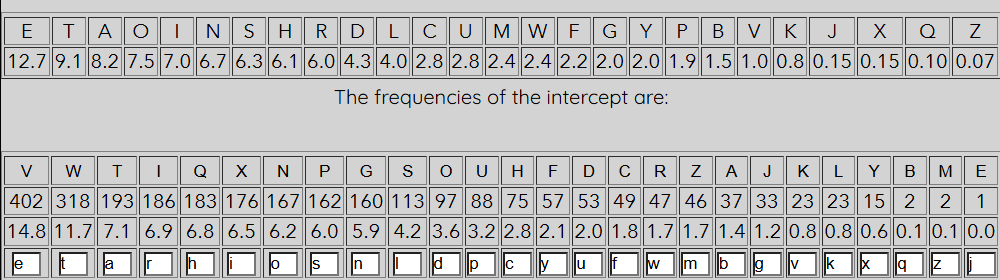


Word horiMontal fits to word horiZontal, so I replaced M to Z.



Also word Buit fits by word quit, so B was replaced to Q.

Last letter E was replaced with letter J, so after all replacements letter table looks like:



After all replacements and proper placement of capital letters and spaces final text looks like:

Vigenere was born in the village of saint-pourcain, about halfway 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, at26, 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 these cryptologists. 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 encipher and decipher, 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 keywords system for more susceptible to solution than vigenere's autokey. It's tableau consists 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 enciphered repeats this above the plaintext letters until each one has a key letter. 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 letterstands at the intersection of the column and the row. the enciphererrepeats 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?