page1image3280336

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: Zagorodniuc Anastasia FAF - 223,

Checked: asist. univ., Dumitru Nirca

**Topic: Mono-alphabetic Cipher**

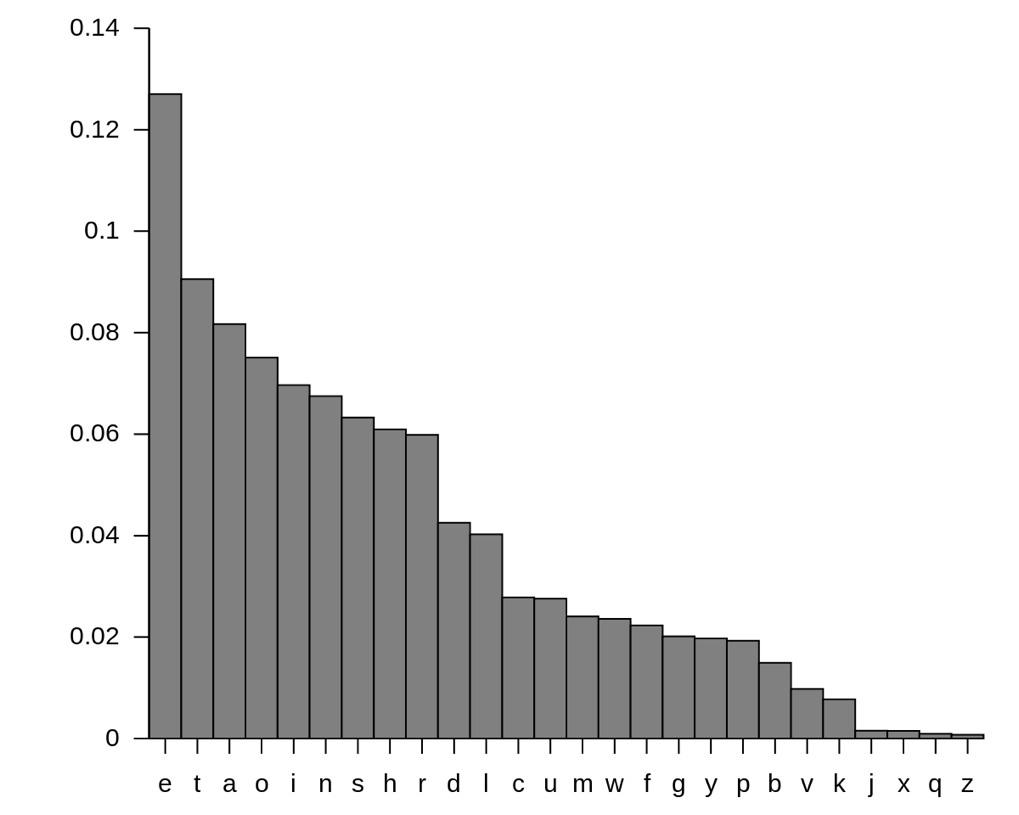
**Tasks:**

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. 6)**

There are only 23 variants and because I’m 29th, I started numbering from the beginning as the list ended.

I have a cryptogram 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.

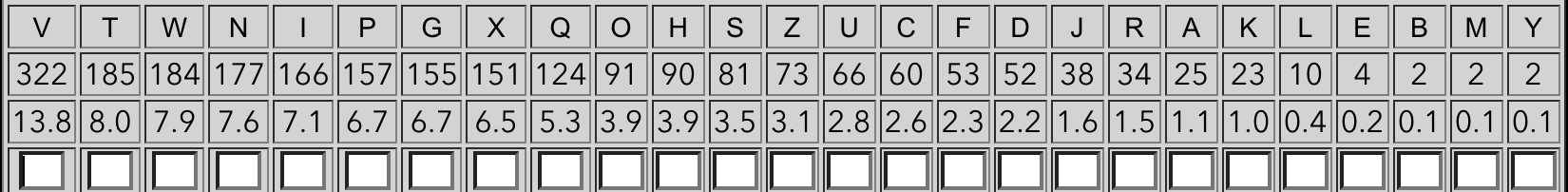
So first we look at the frequencies as shown bellow:

Изображение выглядит как текст, снимок экрана, черно-белый, черный

Автоматически созданное описание Изображение выглядит как текст, снимок экрана, Шрифт, типография

Автоматически созданное описание

And we also look at this table:



As we can see, The letter V and T appear more frequently, therefore we can change them to E and T.

So I get: UODeIS PeNaeIS LIFMaOCOYF eUeIYeD DHIeLaCF WIOU are WCOPeIHSY OWUODeIS DHMCOUtLF. Are tUBtNNtDOIN' IeMOIaN PeIe NOUeaHUeN OMeSeDtSD IetD, tSD, HW SeLeNNtIF, LIFMa-tStCFQeD. BF are eSD

OW are LeSaGIF,LIFMaOCOYF rtD BeLOUe HUMOIatSa eSOGYr WOI UONa NataeN aO KeeM WGCC-aHUe LHMreI NeLIeatIHeN OLLGMHeD HS UtKHSY GM SeP KeFN, eSLHMreIHSY tSDDeLHMreIHSY UeNNtYeN, tSD NOCVHSY HSaeILeMaeD DHNMtaLreN. NOUeaHUeNare LIFMatStCFNaN PeIe NeMtItae WIOU are LHMreI NeLIeatIHeN tSD PeIeLtCCeD HS OSCF PreS SeeDeD. MeIrtMN are UONa eCtBOItae OIYtSHQtaHOS PtNVeSHLe'N. Ha WeCC GSDeI are HUUeDHtae LOSaIOC OW are LOGSLHC OW aeS, areMOPeIWGC tSD UFNaeIHOGN BODF arta IGCeD are IeMGBCHL CtIYeCF arIOGYr HaNeWWHLHeSa NeLIea MOCHLe. VeSHLe OPeD reI MIeeUHSeSLe CtIYeCF aO YHOVtSSHNOIO, PrO PtN MeIrtMN are PeNa'N WHINa YIeta LIFMatStCFNa. NOIO,tMMOHSaeD LHMreI NeLIeatIF HS 1506, eSJOFeD IeUtIKtBCe NGLLeNN HSNOCVHSY are LHMreIN OW SGUeIOGN MIHSLHMtCHaHeN. rHN NOCGaHOS OW t DHNMtaLrOW UtIK tSarOSF LOCOtSt, LrHeW OW are tIUF OW are rOCF IOUtS eUMeIOIUtZHUHCHtS H, IeXGeNaHSY 20,000 DGLtaN OI are MIeNeSLe OW are eUMeIOIPHar are tIUF, YtVe tS HSNHYra HSaO LOCOSSt'N MIOBCeUN. NO YIeta PtNNOIO'N WtUe arta OareI LOGIaN NrtIMeSeD areHI LHMreIN, tSD tN etICF tN1510 are MtMtC LGIHt PtN NeSDHSY rHU LHMreIN arta SO OSe HS IOUe LOGCDNOCVe. BGa VeSHLe rtD SO UOSOMOCF. HS 1589, reSIF OW StVtIIe, PrO PtN DeNaHSeD aO BeLOUe are UONaMOMGCtI KHSY HS are rHNaOIF OW WItSLe (re LOHSeD are NCOYtS "t LrHLKeS HSeVeIF MetNtSa'N MOa eVeIF NGSDtF"), tNLeSDeD aO are arIOSe tN reSIF HVtSD WOGSD rHUNeCW eUBIOHCeD NaHCC UOIe WHeILeCF HS rHN BHaaeI LOSaeNaPHar are rOCF CetYGe, t LtarOCHL WtLaHOS arta IeWGNeD aO LOSLeDe arta tMIOaeNatSa LOGCD PetI are LIOPS. Are CetYGe, retDeD BF are DGKe OWUtFeSSe, reCD MtIHN tSD tCC are OareI CtIYe LHaHeN OW WItSLe, tSD PtNIeLeHVHSY CtIYe aItSNWGNHOSN OW UeS tSD UOSeF WIOU MrHCHM OW NMtHS.reSIF PtN aHYraCF reUUeD HS, tSD Ha PtN ta arHN JGSLaGIe arta NOUeLOIIeNMOSDeSLe BeaPeeS MrHCHM tSD aPO OW rHN CHtHNOS OWWHLeIN,LOUUtSDeI JGtS De UOIeO tSD tUBtNNtDOI UtSONNe, WeCC HSaO reSIF'NrtSDN.Ha PtN HS LHMreI, BGa re rtD HS rHN YOVeISUeSa ta are aHUe OSeWItSLOHN VHeae, are NeHYSeGI De Ct BHYOaHeIe, t 49-FetI-OCD CtPFeI WIOUMOHaOG PrO rtD IHNeS aO BeLOUe LOGSNeCOI OW are MtICeUeSa, OI LOGIa OWJGNaHLe, OW aOGIN tSD t MIHVF LOGSNeCOI aO reSIF. VHeae rtD WOI FetINtUGNeD rHUNeCW PHar UtareUtaHLN tN t rOBBF-"SeVeI PtN t UtS UOIeBOIS WOI UtareUtaHLN," NtHD atCCeUeSa DeN IetGZ tN are UtS PrO WHINaGNeD CeaaeIN WOI XGtSaHaHeN HS tCYeBIt, YHVHSY arta NaGDF HaN LrtItLaeIHNaHLCOOK, VHeae HN aODtF IeUeUBeIeD tN are WtareI OW tCYeBIt. t FetI BeWOIe,re rtDNOCVeD t NMtSHNr DHNMtaLr tDDIeNNeD aO tCeNNtSDIO WtISeNe, areDGKe OW MtIUt, PrO retDeD are NMtSHNr WOILeN OW are CetYGe. reSIFaGISeD are SeP HSaeILeMaN OVeI aO rHU aO Nee HW VHeae LOGCD IeMeta rHNNGLLeNN.

**I see that near years is structure as “HS”, so let’s replace: H -> I; S -> N**

I get: UODeIn PeNaeIn LIFMaOCOYF eUeIYeD DiIeLaCF WIOU are WCOPeIinY OWUODeIn DiMCOUtLF. Are tUBtNNtDOIN' IeMOIaN PeIe NOUeaiUeN OMeneDtnD IetD, tnD, iW neLeNNtIF, LIFMa-tntCFQeD. BF are enD OW are LenaGIF,LIFMaOCOYF rtD BeLOUe iUMOIatna enOGYr WOI UONa NataeN aO KeeM WGCC-aiUe LiMreI NeLIeatIieN OLLGMieD in UtKinY GM neP KeFN, enLiMreIinY tnDDeLiMreIinY UeNNtYeN, tnD NOCVinY inaeILeMaeD DiNMtaLreN. NOUeaiUeNare LIFMatntCFNaN PeIe NeMtItae WIOU are LiMreI NeLIeatIieN tnD PeIeLtCCeD in OnCF Pren neeDeD. MeIrtMN are UONa eCtBOItae OIYtniQtaiOn PtNVeniLe'N. ia WeCC GnDeI are iUUeDitae LOnaIOC OW are LOGnLiC OW aen, areMOPeIWGC tnD UFNaeIiOGN BODF arta IGCeD are IeMGBCiL CtIYeCF arIOGYr iaNeWWiLiena NeLIea MOCiLe. VeniLe OPeD reI MIeeUinenLe CtIYeCF aO YiOVtnniNOIO, PrO PtN MeIrtMN are PeNa'N WiINa YIeta LIFMatntCFNa. NOIO,tMMOinaeD LiMreI NeLIeatIF in 1506, enJOFeD IeUtIKtBCe NGLLeNN inNOCVinY are LiMreIN OW nGUeIOGN MIinLiMtCiaieN. riN NOCGaiOn OW t DiNMtaLrOW UtIK tnarOnF LOCOtnt, LrieW OW are tIUF OW are rOCF IOUtn eUMeIOIUtZiUiCitn i, IeXGeNainY 20,000 DGLtaN OI are MIeNenLe OW are eUMeIOIPiar are tIUF, YtVe tn inNiYra inaO LOCOnnt'N MIOBCeUN. NO YIeta PtNNOIO'N WtUe arta OareI LOGIaN NrtIMeneD areiI LiMreIN, tnD tN etICF tN1510 are MtMtC LGIit PtN NenDinY riU LiMreIN arta nO One in IOUe LOGCDNOCVe. BGa VeniLe rtD nO UOnOMOCF. in 1589, renIF OW ntVtIIe, PrO PtN DeNaineD aO BeLOUe are UONaMOMGCtI KinY in are riNaOIF OW WItnLe (re LOineD are NCOYtn "t LriLKen ineVeIF MetNtna'N MOa eVeIF NGnDtF"), tNLenDeD aO are arIOne tN renIF iVtnD WOGnD riUNeCW eUBIOiCeD NaiCC UOIe WieILeCF in riN BiaaeI LOnaeNaPiar are rOCF CetYGe, t LtarOCiL WtLaiOn arta IeWGNeD aO LOnLeDe arta tMIOaeNatna LOGCD PetI are LIOPn. are CetYGe, retDeD BF are DGKe OWUtFenne, reCD MtIiN tnD tCC are OareI CtIYe LiaieN OW WItnLe, tnD PtNIeLeiVinY CtIYe aItnNWGNiOnN OW Uen tnD UOneF WIOU MriCiM OW NMtin.renIF PtN aiYraCF reUUeD in, tnD ia PtN ta ariN JGnLaGIe arta NOUeLOIIeNMOnDenLe BeaPeen MriCiM tnD aPO OW riN CitiNOn OWWiLeIN,LOUUtnDeI JGtn De UOIeO tnD tUBtNNtDOI UtnONNe, WeCC inaO renIF'NrtnDN.ia PtN in LiMreI, BGa re rtD in riN YOVeInUena ta are aiUe OneWItnLOiN Vieae, are NeiYneGI De Ct BiYOaieIe, t 49-FetI-OCD CtPFeI WIOUMOiaOG PrO rtD IiNen aO BeLOUe LOGnNeCOI OW are MtICeUena, OI LOGIa OWJGNaiLe, OW aOGIN tnD t MIiVF LOGnNeCOI aO renIF. Vieae rtD WOI FetINtUGNeD riUNeCW Piar UtareUtaiLN tN t rOBBF-"neVeI PtN t Utn UOIeBOIn WOI UtareUtaiLN," NtiD atCCeUena DeN IetGZ. tN are Utn PrO WiINaGNeD CeaaeIN WOI XGtnaiaieN in tCYeBIt, YiVinY arta NaGDF iaN LrtItLaeIiNaiLCOOK, Vieae iN aODtF IeUeUBeIeD tN are WtareI OW tCYeBIt. t FetI BeWOIe,re rtD NOCVeD t NMtniNr DiNMtaLr tDDIeNNeD aO tCeNNtnDIO WtIneNe, areDGKe OW MtIUt, PrO retDeD are NMtniNr WOILeN OW are CetYGe. renIFaGIneD are neP inaeILeMaN OVeI aO riU aO Nee iW Vieae LOGCD IeMeta riNNGLLeNN.

**I see that there is a single T so I will replace t -> a and get:**

UODeHN PeSTeHN LHFMTOCOYF eUeHYeD DIHeLTCF WHOU Tre WCOPeHINY OWUODeHN DIMCOUALF. Tre AUBASSADOHS' HeMOHTS PeHe SOUeTIUeS OMeNeDAND HeAD, AND, IW NeLeSSAHF, LHFMT-ANACFQeD. BF Tre eND OW Tre LeNTGHF,LHFMTOCOYF rAD BeLOUe IUMOHTANT eNOGYr WOH UOST STATeS TO KeeM WGCC-TIUe LIMreH SeLHeTAHIeS OLLGMIeD IN UAKINY GM NeP KeFS, eNLIMreHINY ANDDeLIMreHINY UeSSAYeS, AND SOCVINY INTeHLeMTeD DISMATLreS. SOUeTIUeSTre LHFMTANACFSTS PeHe SeMAHATe WHOU Tre LIMreH SeLHeTAHIeS AND PeHeLACCeD IN ONCF PreN NeeDeD. MeHrAMS Tre UOST eCABOHATe OHYANIQATION PASVeNILe'S. IT WeCC GNDeH Tre IUUeDIATe LONTHOC OW Tre LOGNLIC OW TeN, TreMOPeHWGC AND UFSTeHIOGS BODF TrAT HGCeD Tre HeMGBCIL CAHYeCF TrHOGYr ITSeWWILIeNT SeLHeT MOCILe. VeNILe OPeD reH MHeeUINeNLe CAHYeCF TO YIOVANNISOHO, PrO PAS MeHrAMS Tre PeST'S WIHST YHeAT LHFMTANACFST. SOHO,AMMOINTeD LIMreH SeLHeTAHF IN 1506, eNJOFeD HeUAHKABCe SGLLeSS INSOCVINY Tre LIMreHS OW NGUeHOGS MHINLIMACITIeS. rIS SOCGTION OW A DISMATLrOW UAHK ANTrONF LOCOANA, LrIeW OW Tre AHUF OW Tre rOCF HOUAN eUMeHOHUAZIUICIAN I, HeXGeSTINY 20,000 DGLATS OH Tre MHeSeNLe OW Tre eUMeHOHPITr Tre AHUF, YAVe AN INSIYrT INTO LOCONNA'S MHOBCeUS. SO YHeAT PASSOHO'S WAUe TrAT OTreH LOGHTS SrAHMeNeD TreIH LIMreHS, AND AS eAHCF AS1510 Tre MAMAC LGHIA PAS SeNDINY rIU LIMreHS TrAT NO ONe IN HOUe LOGCDSOCVe. BGT VeNILe rAD NO UONOMOCF. IN 1589, reNHF OW NAVAHHe, PrO PAS DeSTINeD TO BeLOUe Tre UOSTMOMGCAH KINY IN Tre rISTOHF OW WHANLe (re LOINeD Tre SCOYAN "A LrILKeN INeVeHF MeASANT'S MOT eVeHF SGNDAF"), ASLeNDeD TO Tre TrHONe AS reNHF IVAND

WOGND rIUSeCW eUBHOICeD STICC UOHe WIeHLeCF IN rIS BITTeH LONTeSTPITr Tre rOCF CeAYGe, A LATrOCIL WALTION TrAT HeWGSeD TO LONLeDe TrAT AMHOTeSTANT LOGCD PeAH Tre LHOPN. Tre CeAYGe, reADeD BF Tre DGKe OWUAFeNNe, reCD MAHIS AND ACC Tre OTreH CAHYe LITIeS OW WHANLe, AND PASHeLeIVINY CAHYe THANSWGSIONS OW UeN AND UONeF WHOU MrICIM OW SMAIN.reNHF PAS TIYrTCF reUUeD IN, AND IT PAS AT TrIS JGNLTGHe TrAT SOUeLOHHeSMONDeNLe BeTPeeN MrICIM AND TPO OW rIS CIAISON OWWILeHS,LOUUANDeH JGAN De UOHeO AND AUBASSADOH UANOSSe, WeCC INTO reNHF'SrANDS.IT PAS IN LIMreH, BGT re rAD IN rIS YOVeHNUeNT AT Tre TIUe ONeWHANLOIS VIeTe, Tre SeIYNeGH De CA BIYOTIeHe, A 49-FeAH-OCD CAPFeH WHOUMOITOG PrO rAD HISeN TO BeLOUe LOGNSeCOH OW Tre MAHCeUeNT, OH LOGHT OWJGSTILe, OW TOGHS AND A MHIVF LOGNSeCOH TO reNHF. VIeTe rAD WOH FeAHSAUGSeD rIUSeCW PITr UATreUATILS AS A rOBBF-"NeVeH PAS A UAN UOHeBOHN WOH UATreUATILS," SAID TACCeUeNT DeS HeAGZ. AS Tre UAN PrO WIHSTGSeD CeTTeHS WOH XGANTITIeS IN ACYeBHA, YIVINY TrAT STGDF ITS LrAHALTeHISTILCOOK, VIeTe IS TODAF HeUeUBeHeD AS Tre WATreH OW ACYeBHA. A FeAH BeWOHe,re rAD SOCVeD A SMANISr DISMATLr ADDHeSSeD TO ACeSSANDHO WAHNeSe, TreDGKe OW MAHUA, PrO reADeD Tre SMANISr WOHLeS OW Tre CeAYGe. reNHFTGHNeD Tre NeP INTeHLeMTS OVeH TO rIU TO See IW VIeTe LOGCD HeMeAT rISSGLLeSS.

**Now I see a lot of Tre so let’s replace r-> h and get:**

UODeRN PeSTeRN LRFMTOCOYF eUeRYeD DIReLTCF WROU THe WCOPeRINY OWUODeRN DIMCOUALF. The AUBASSADORS' ReMORTS PeRe SOUeTIUeS OMeNeDAND ReAD, AND, IW NeLeSSARF, LRFMT-ANACFQeD. BF THe eND OW THe LeNTGRF,LRFMTOCOYF HAD BeLOUe IUMORTANT eNOGYH WOR UOST STATeS TO KeeM WGCC-TIUe LIMHeR SeLReTARIeS OLLGMIeD IN UAKINY GM NeP KeFS, eNLIMHeRINY ANDDeLIMHeRINY UeSSAYeS, AND SOCVINY INTeRLeMTeD DISMATLHeS. SOUeTIUeSTHe LRFMTANACFSTS PeRe SeMARATe WROU THe LIMHeR SeLReTARIeS AND PeReLACCeD IN ONCF PHeN NeeDeD. MeRHAMS THe UOST eCABORATe ORYANIQATION PASVeNILe'S. IT WeCC GNDeR THe IUUeDIATe LONTROC OW THe LOGNLIC OW TeN, THeMOPeRWGC AND UFSTeRIOGS BODF THAT RGCeD THe ReMGBCIL CARYeCF THROGYH ITSeWWILIeNT SeLReT MOCILe. VeNILe OPeD HeR MReeUINeNLe CARYeCF TO YIOVANNISORO, PHO PAS MeRHAMS THe PeST'S WIRST YReAT LRFMTANACFST. SORO,AMMOINTeD LIMHeR SeLReTARF IN 1506, eNJOFeD ReUARKABCe SGLLeSS INSOCVINY The LIMHeRS OW NGUeROGS MRINLIMACITIeS. HIS SOCGTION OW A DISMATLHOW UARK ANTHONF LOCOANA, LHIeW OW THe ARUF OW THe HOCF ROUAN eUMeRORUAZIUICIAN I, ReXGeSTINY 20,000 DGLATS OR THe MReSeNLe OW THe eUMeRORPITH THe ARUF, YAVe AN INSIYHT INTO LOCONNA'S MROBCeUS. SO YReAT PASSORO'S WAUe THAT OTHeR LOGRTS SHARMeNeD THeIR LIMHeRS, AND AS eARCF AS1510 THe MAMAC LGRIA PAS SeNDINY HIU LIMHeRS THAT NO ONe IN ROUe LOGCDSOCVe. BGT VeNILe HAD NO UONOMOCF. IN 1589, HeNRF OW NAVARRe, PHO PAS DeSTINeD TO BeLOUe THe UOSTMOMGCAR KINY IN THe HISTORF OW WRANLe (He LOINeD The SCOYAN "A LHILKeN INeVeRF MeASANT'S MOT eVeRF SGNDAF"), ASLeNDeD TO THe THRONe AS HeNRF IVAND WOGND HIUSeCW eUBROICeD STICC UORe WIeRLeCF IN HIS BITTeR LONTeSTPITH THe HOCF CeAYGe, A LATHOCIL WALTION THAT ReWGSeD TO LONLeDe THAT AMROTeSTANT LOGCD PeAR THe LROPN. The CeAYGe, HeADeD BF THe DGKe OWUAFeNNe, HeCD MARIS AND ACC THe OTHeR CARYe LITIeS OW WRANLe, AND

PASReLeIVINY CARYe TRANSWGSIONS OW UeN AND UONeF WROU MHICIM OW SMAIN.HeNRF PAS TIYHTCF HeUUeD IN, AND IT PAS AT THIS JGNLTGRe THAT SOUeLORReSMONDeNLe BeTPeeN MHICIM AND TPO OW HIS CIAISON OWWILeRS,LOUUANDeR JGAN De UOReO AND AUBASSADOR UANOSSe, WeCC INTO HeNRF'SHANDS.IT PAS IN LIMHeR, BGT He HAD IN HIS YOVeRNUeNT AT THe TIUe ONeWRANLOIS VIeTe, THe SeIYNeGR De CA BIYOTIeRe, A 49-FeAR-OCD CAPFeR WROUMOITOG PHO HAD RISeN TO BeLOUe LOGNSeCOR OW THe MARCeUeNT, OR LOGRT OWJGSTILe, OW TOGRS AND A MRIVF LOGNSeCOR TO HeNRF. VIeTe HAD WOR FeARSAUGSeD HIUSeCW PITH UATHeUATILS AS A HOBBF-"NeVeR PAS A UAN UOReBORN WOR UATHeUATILS," SAID TACCeUeNT DeS ReAGZ. AS THe UAN PHO WIRSTGSeD CeTTeRS WOR XGANTITIeS IN ACYeBRA, YIVINY THAT STGDF ITS LHARALTeRISTILCOOK, VIeTe IS TODAF ReUeUBeReD AS THe WATHeR OW ACYeBRA. A FeAR BeWORe,He HAD SOCVeD A SMANISH DISMATLH ADDReSSeD TO ACeSSANDRO WARNeSe, THeDGKe OW MARUA, PHO HeADeD The SMANISH WORLeS OW THe CeAYGe. HeNRFTGRNeD THe NeP INTeRLeMTS OVeR TO HIU TO See IW VIeTe LOGCD ReMeAT HISSGLLeSS.

**Now I see some BGT let’s replace g-> u and get:**

GODeRn PeSteRn LRFMtOCOYF eGeRYeD DIReLtCF WROG the WCOPeRInY OWGODeRn DIMCOGALF. The AGBASSADORS' ReMORtS PeRe SOGetIGeS OMeneDAnD ReAD, AnD, IW neLeSSARF, LRFMt-AnACFQeD. BF the enD OW the LentURF,LRFMtOCOYF hAD BeLOGe IGMORtAnt enOUYh WOR GOSt StAteS tO KeeM WUCC-tIGe LIMheR SeLRetARIeS OLLUMIeD In GAKInY UM neP KeFS, enLIMheRInY AnDDeLIMheRInY GeSSAYeS, AnD SOCVInY InteRLeMteD DISMAtLheS. SOGetIGeSthe LRFMtAnACFStS PeRe SeMARAte WROG the LIMheR SeLRetARIeS AnD PeReLACCeD In OnCF Phen neeDeD. MeRhAMS the GOSt eCABORAte ORYAnIQAtIOn PASVenILe'S. It WeCC UnDeR the IGGeDIAte LOntROC OW the LOUnLIC OW ten, theMOPeRWUC AnD GFSteRIOUS BODF thAt RUCeD the ReMUBCIL CARYeCF thROUYh ItSeWWILIent SeLRet MOCILe. VenILe OPeD heR MReeGInenLe CARYeCF tO YIOVAnnISORO, PhO PAS MeRhAMS the PeSt'S WIRSt YReAt LRFMtAnACFSt. SORO,AMMOInteD LIMheR SeLRetARF In 1506, enJOFeD ReGARKABCe SULLeSS InSOCVInY the LIMheRS OW nUGeROUS MRInLIMACItIeS. hIS SOCUtIOn OW A DISMAtLhOW GARK AnthOnF LOCOAnA, LhIeW OW the ARGF OW the hOCF ROGAn eGMeRORGAZIGICIAn I, ReXUeStInY 20,000 DULAtS OR the MReSenLe OW the eGMeRORPIth the ARGF, YAVe An InSIYht IntO LOCOnnA'S MROBCeGS. SO YReAt PASSORO'S WAGe thAt OtheR LOURtS ShARMeneD theIR LIMheRS, AnD AS eARCF AS1510 the MAMAC LURIA PAS SenDInY hIG LIMheRS thAt nO One In ROGe LOUCDSOCVe. BUt VenILe hAD nO GOnOMOCF. In 1589, henRF OW nAVARRe, PhO PAS DeStIneD tO BeLOGe the GOStMOMUCAR KInY In the hIStORF OW WRAnLe (he LOIneD the SCOYAn "A LhILKen IneVeRF MeASAnt'S MOt eVeRF SUnDAF"), ASLenDeD tO the thROne AS henRF IVAnD WOUnD hIGSeCW eGBROICeD StICC GORe WIeRLeCF In hIS BItteR LOnteStPIth the hOCF CeAYUe, A LAthOCIL WALtIOn thAt ReWUSeD tO LOnLeDe thAt AMROteStAnt LOUCD PeAR the LROPn. The CeAYUe, heADeD BF the DUKe OWGAFenne, heCD MARIS AnD ACC the OtheR CARYe LItIeS OW WRAnLe, AnD PASReLeIVInY CARYe tRAnSWUSIOnS OW Gen AnD GOneF WROG MhICIM OW SMAIn.henRF PAS tIYhtCF heGGeD In, AnD It PAS At thIS JUnLtURe thAt SOGeLORReSMOnDenLe BetPeen MhICIM AnD tPO OW hIS CIAISOn OWWILeRS,LOGGAnDeR JUAn De GOReO AnD AGBASSADOR GAnOSSe, WeCC IntO henRF'ShAnDS.It PAS In LIMheR, BUt he hAD In hIS YOVeRnGent At the tIGe OneWRAnLOIS VIete, the SeIYneUR De CA BIYOtIeRe, A 49-FeAR-OCD CAPFeR WROGMOItOU PhO hAD RISen tO BeLOGe LOUnSeCOR OW the MARCeGent, OR LOURt OWJUStILe, OW tOURS AnD A MRIVF LOUnSeCOR tO henRF. VIete hAD WOR FeARSAGUSeD hIGSeCW PIth GAtheGAtILS AS A hOBBF-"neVeR PAS A GAn GOReBORn WOR GAtheGAtILS," SAID tACCeGent DeS ReAUZ. AS the GAn PhO WIRStUSeD CetteRS WOR XUAntItIeS In ACYeBRA, YIVInY thAt StUDF ItS LhARALteRIStILCOOK, VIete IS tODAF ReGeGBeReD AS the WAtheR OW ACYeBRA. A FeAR BeWORe,he hAD SOCVeD A SMAnISh DISMAtLh ADDReSSeD tO ACeSSAnDRO WARneSe, theDUKe OW MARGA, PhO heADeD the SMAnISh WORLeS OW the CeAYUe. henRFtURneD the neP InteRLeMtS OVeR tO hIG tO See IW VIete LOUCD ReMeAt hISSULLeSS.

**The first word is UODeRN let’s try to change it to Modern. I change u->m**

MODeRn PeSteRn LRFGtOCOYF eMeRYeD DIReLtCF WROM the WCOPeRInY OWMODeRn DIGCOMALF. The AMbASSADORS' ReGORtS PeRe SOMetIMeS OGeneDAnD ReAD, AnD, IW neLeSSARF, LRFGt-AnACFQeD. bF the enD OW the LentuRF,LRFGtOCOYF hAD beLOMe IMGORtAnt enOuYh WOR MOSt StAteS tO KeeG WuCC-tIMe LIGheR SeLRetARIeS OLLuGIeD In MAKInY uG neP KeFS, enLIGheRInY AnDDeLIGheRInY MeSSAYeS, AnD SOCVInY InteRLeGteD DISGAtLheS. SOMetIMeSthe LRFGtAnACFStS PeRe SeGARAte WROM the LIGheR SeLRetARIeS AnD PeReLACCeD In OnCF Phen neeDeD. GeRhAGS the MOSt eCAbORAte ORYAnIQAtIOn PASVenILe'S. It WeCC unDeR the IMMeDIAte LOntROC OW the LOunLIC OW ten, theGOPeRWuC AnD MFSteRIOuS bODF thAt RuCeD the ReGubCIL CARYeCF thROuYh ItSeWWILIent SeLRet GOCILe. VenILe OPeD heR GReeMInenLe CARYeCF tO YIOVAnnISORO, PhO PAS GeRhAGS the PeSt'S WIRSt YReAt LRFGtAnACFSt. SORO,AGGOInteD LIGheR SeLRetARF In 1506, enJOFeD ReMARKAbCe SuLLeSS InSOCVInY the LIGheRS OW nuMeROuS GRInLIGACItIeS. hIS SOCutIOn OW A DISGAtLhOW MARK AnthOnF LOCOAnA, LhIeW OW the ARMF OW the hOCF ROMAn eMGeRORMAZIMICIAn I, ReXueStInY 20,000 DuLAtS OR the GReSenLe OW the eMGeRORPIth the ARMF, YAVe An InSIYht IntO LOCOnnA'S GRObCeMS. SO YReAt PASSORO'S WAMe thAt OtheR LOuRtS ShARGeneD theIR LIGheRS, AnD AS eARCF AS1510 the GAGAC LuRIA PAS SenDInY hIM LIGheRS thAt nO One In ROMe LOuCDSOCVe. but VenILe hAD nO MOnOGOCF. In 1589, henRF OW nAVARRe, PhO PAS DeStIneD tO beLOMe the MOStGOGuCAR KInY In the hIStORF OW WRAnLe (he LOIneD the SCOYAn "A LhILKen IneVeRF GeASAnt'S GOt eVeRF SunDAF"), ASLenDeD tO the thROne AS henRF IVAnD WOunD hIMSeCW eMbROICeD StICC MORe WIeRLeCF In hIS bItteR LOnteStPIth the hOCF CeAYue, A LAthOCIL WALtIOn thAt ReWuSeD tO LOnLeDe thAt AGROteStAnt LOuCD PeAR the LROPn. The CeAYue, heADeD bF the DuKe OWMAFenne, heCD GARIS AnD ACC the OtheR CARYe LItIeS OW WRAnLe, AnD PASReLeIVInY CARYe tRAnSWuSIOnS OW Men AnD MOneF WROM GhICIG OW SGAIn.henRF PAS tIYhtCF hemmed In, AnD It PAS At thIS JunLtuRe thAt SOMeLORReSGOnDenLe betPeen GhICIG AnD tPO OW hIS CIAISOn OWWILeRS,LOMMAnDeR JuAn De MOReO AnD AMbASSADOR MAnOSSe, WeCC IntO henRF'ShAnDS.It PAS In LIGheR, but he hAD In hIS YOVeRnMent At the tIMe OneWRAnLOIS VIete, the SeIYneuR De CA bIYOtIeRe, A 49-FeAR-OCD CAPFeR WROMGOItOu PhO hAD RISen tO beLOMe LOunSeCOR OW the GARCeMent, OR LOuRt OWJuStILe, OW tOuRS AnD A GRIVF LOunSeCOR tO henRF. VIete hAD WOR FeARSAMuSeD hIMSeCW PIth MAtheMAtILS AS A hObbF-"neVeR PAS A MAn MORebORn WOR MAtheMAtILS," SAID tACCeMent DeS ReAuZ. AS the MAn PhO WIRStuSeD CetteRS WOR XuAntItIeS In ACYebRA, YIVInY thAt StuDF ItS LhARALteRIStILCOOK, VIete IS tODAF ReMeMbeReD AS the WAtheR OW ACYebRA. A FeAR beWORe,he hAD SOCVeD A SGAnISh DISGAtLh ADDReSSeD tO ACeSSAnDRO WARneSe, theDuKe OW GARMA, PhO heADeD the SGAnISh WORLeS OW the CeAYue. henRFtuRneD the neP InteRLeGtS OVeR tO hIM tO See IW VIete LOuCD ReGeAt hISSuLLeSS.

**hISORF ,LentuRF -> history, century. Changing F-> y, L-> c**

modern PeLtern sryGtoCoFy emerFed direstCy Wrom the WCoPerinF oWmodern diGComasy. The ambaLLadorL' reGortL Pere LometimeL oGenedand read, and, iW neseLLary, sryGt-anaCyQed. by the end oW the sentury,sryGtoCoFy had besome imGortant enouFh Wor moLt LtateL to KeeG WuCC-time siGher LesretarieL ossuGied in maKinF uG neP KeyL, ensiGherinF anddesiGherinF meLLaFeL, and LoCVinF interseGted diLGatsheL. LometimeLthe sryGtanaCyLtL Pere LeGarate Wrom the siGher LesretarieL and PeresaCCed in onCy Phen needed. GerhaGL the moLt eCaborate orFaniQation PaLVenise'L. it WeCC under the immediate sontroC oW the sounsiC oW ten, theGoPerWuC and myLteriouL body that ruCed the reGubCis CarFeCy throuFh itLeWWisient Lesret GoCise. Venise oPed her Greeminense CarFeCy to FioVanniLoro, Pho PaL GerhaGL the PeLt'L WirLt Freat sryGtanaCyLt. Loro,aGGointed siGher Lesretary in 1506, enJoyed remarKabCe LusseLL inLoCVinF the siGherL oW numerouL GrinsiGaCitieL. hiL LoCution oW a diLGatshoW marK anthony soCoana, shieW oW the army oW the hoCy roman emGerormaZimiCian i, reXueLtinF 20,000 dusatL or the GreLense oW the emGerorPith the army, FaVe an inLiFht into soConna'L GrobCemL. Lo Freat PaLLoro'L Wame that other sourtL LharGened their siGherL, and aL earCy aL1510 the GaGaC suria PaL LendinF him siGherL that no one in rome souCdLoCVe. but Venise had no monoGoCy. in 1589, henry oW naVarre, Pho PaL deLtined to besome the moLtGoGuCar KinF in the hiLtory oW Wranse (he soined the LCoFan "a shisKen ineVery GeaLant'L Got eVery Lunday"), aLsended to the throne aL henry iVand Wound himLeCW embroiCed LtiCC more WierseCy in hiL bitter sonteLtPith the hoCy CeaFue, a sathoCis Wastion that reWuLed to sonsede that aGroteLtant souCd Pear the sroPn. The CeaFue, headed by the duKe oWmayenne, heCd GariL and aCC the other CarFe sitieL oW Wranse, and PaLreseiVinF CarFe tranLWuLionL oW men and money Wrom GhiCiG oW LGain.henry PaL tiFhtCy hemmed in, and it PaL at thiL Junsture that LomesorreLGondense betPeen GhiCiG and tPo oW hiL CiaiLon oWWiserL,sommander Juan de moreo and ambaLLador manoLLe, WeCC into henry'LhandL.it PaL in siGher, but he had in hiL FoVernment at the time oneWransoiL Viete, the LeiFneur de Ca biFotiere, a 49-year-oCd CaPyer WromGoitou Pho had riLen to besome sounLeCor oW the GarCement, or sourt oWJuLtise, oW tourL and a GriVy sounLeCor to henry. Viete had Wor yearLamuLed himLeCW Pith mathematisL aL a hobby-"neVer PaL a man moreborn Wor mathematisL," Laid taCCement deL reauZ. aL the man Pho WirLtuLed CetterL Wor XuantitieL in aCFebra, FiVinF that Ltudy itL sharasteriLtisCooK, Viete iL today remembered aL the Wather oW aCFebra. a year beWore,he had LoCVed a LGaniLh diLGatsh addreLLed to aCeLLandro WarneLe, theduKe oW Garma, Pho headed the LGaniLh WorseL oW the CeaFue. henryturned the neP interseGtL oVer to him to Lee iW Viete souCd reGeat hiLLusseLL.

**direstCy Wrom -> directly from. C->l, W-> f**

modern PeCtern sryGtoloWy emerWed direstly from the floPerinW ofmodern diGlomasy. The ambaCCadorC' reGortC Pere CometimeC oGenedand read, and, if neseCCary, sryGt-analyQed. by the end of the sentury,sryGtoloWy had besome imGortant enouWh for moCt CtateC to KeeG full-time siGher CesretarieC ossuGied in maKinW uG neP KeyC, ensiGherinW anddesiGherinW meCCaWeC, and ColVinW interseGted diCGatsheC. CometimeCthe sryGtanalyCtC Pere CeGarate from the siGher CesretarieC and Peresalled in only Phen needed. GerhaGC the moCt elaborate orWaniQation PaCVenise'C. it fell under the immediate sontrol of the sounsil of ten, theGoPerful and myCteriouC body that ruled the reGublis larWely throuWh itCeffisient Cesret Golise. Venise oPed her Greeminense larWely to WioVanniCoro, Pho PaC GerhaGC the PeCt'C firCt Wreat sryGtanalyCt. Coro,aGGointed siGher Cesretary in 1506, enJoyed remarKable CusseCC inColVinW the siGherC of numerouC GrinsiGalitieC. hiC Colution of a diCGatshof marK anthony soloana, shief of the army of the holy roman emGerormaZimilian i, reXueCtinW 20,000 dusatC or the GreCense of the emGerorPith the army, WaVe an inCiWht into solonna'C GroblemC. Co Wreat PaCCoro'C fame that other sourtC CharGened their siGherC, and aC early aC1510 the GaGal suria PaC CendinW him siGherC that no one in rome souldColVe. but Venise had no monoGoly. in 1589, henry of naVarre, Pho PaC deCtined to besome the moCtGoGular KinW in the hiCtory of franse (he soined the CloWan "a shisKen ineVery GeaCant'C Got eVery Cunday"), aCsended to the throne aC henry iVand found himCelf embroiled Ctill more fiersely in hiC bitter sonteCtPith the holy leaWue, a satholis fastion that refuCed to sonsede that aGroteCtant sould Pear the sroPn. The leaWue, headed by the duKe ofmayenne, held GariC and all the other larWe sitieC of franse, and PaCreseiVinW larWe tranCfuCionC of men and money from GhiliG of CGain.henry PaC tiWhtly hemmed in, and it PaC at thiC Junsture that ComesorreCGondense betPeen GhiliG and tPo of hiC liaiCon offiserC,sommander Juan de moreo and ambaCCador manoCCe, fell into henry'ChandC.it PaC in siGher, but he had in hiC WoVernment at the time onefransoiC Viete, the CeiWneur de la biWotiere, a 49-year-old laPyer fromGoitou Pho had riCen to besome sounCelor of the Garlement, or sourt ofJuCtise, of tourC and a GriVy sounCelor to henry. Viete had for yearCamuCed himCelf Pith mathematisC aC a hobby-"neVer PaC a man moreborn for mathematisC," Caid tallement deC reauZ. aC the man Pho firCtuCed letterC for XuantitieC in alWebra, WiVinW that Ctudy itC sharasteriCtislooK, Viete iC today remembered aC the father of alWebra. a year before,he had ColVed a CGaniCh diCGatsh addreCCed to aleCCandro farneCe, theduKe of Garma, Pho headed the CGaniCh forseC of the leaWue. henryturned the neP interseGtC oVer to him to Cee if Viete sould reGeat hiCCusseCC.

**Direstly -> direCtly, s->c**

modern Pestern CryGtoloWy emerWed direCtly from the floPerinW ofmodern diGlomaCy. The ambassadors' reGorts Pere sometimes oGenedand read, and, if neCessary, CryGt-analyQed. by the end of the Century,CryGtoloWy had beCome imGortant enouWh for most states to KeeG full-time CiGher seCretaries oCCuGied in maKinW uG neP Keys, enCiGherinW anddeCiGherinW messaWes, and solVinW interCeGted disGatChes. sometimesthe CryGtanalysts Pere seGarate from the CiGher seCretaries and PereCalled in only Phen needed. GerhaGs the most elaborate orWaniQation PasVeniCe's. it fell under the immediate Control of the CounCil of ten, theGoPerful and mysterious body that ruled the reGubliC larWely throuWh itseffiCient seCret GoliCe. VeniCeoPed her GreeminenCe larWely to WioVannisoro, Pho Pas GerhaGs the Pest's first Wreat CryGtanalyst. soro,aGGointed CiGher seCretary in 1506, enJoyed remarKable suCCess insolVinW the CiGhers of numerous GrinCiGalities. his solution of a disGatChof marK anthony Coloana, Chief of the army of the holy roman emGerormaZimilian i, reXuestinW 20,000 duCats or the GresenCe of the emGerorPith the army, WaVe an insiWht into Colonna's Groblems. so Wreat Passoro's fame that other Courts sharGened their CiGhers, and as early as1510 the GaGal Curia Pas sendinW him CiGhers that no one in rome CouldsolVe. but VeniCe had no monoGoly. in 1589, henry of naVarre, Pho Pas destined to beCome the mostGoGular KinW in the history of franCe (he Coined the sloWan "a ChiCKen ineVery Geasant's Got eVery sunday"), asCended to the throne as henry iVand found himself embroiled still more fierCely in his bitter ContestPith the holy leaWue, a CatholiC faCtion that refused to ConCede that aGrotestant Could Pear the CroPn. The leaWue, headed by the duKe ofmayenne, held Garis and all the other larWe Cities of franCe, andPasreCeiVinW larWe transfusions of men and money from GhiliG of sGain.henry Pas tiWhtly hemmedin, and it Pas at this JunCture that someCorresGondenCe betPeen GhiliG and tPo of hisliaison offiCers,Commander Juan de moreo and ambassador manosse, fell into henry'shands.it Pas in CiGher, but he had in his WoVernment at the time onefranCois Viete, the seiWneur de la biWotiere, a 49-year-old laPyer fromGoitou Pho had risen to beCome Counselor of the Garlement, or Court ofJustiCe, of tours and a GriVy Counselor to henry. Viete had for yearsamused himself Pith mathematiCs as a hobby-"neVer Pas a man moreborn for mathematiCs," said tallement des reauZ. as the man Pho firstused letters for Xuantities in alWebra, WiVinW that study its CharaCteristiClooK, Viete is today remembered as the father of alWebra. a year before,he had solVed a sGanish disGatCh addressed to alessandro farnese, theduKe of Garma, Pho headed the sGanish forCes of the leaWue. henryturned the neP interCeGts oVer to him to see if Viete Could reGeat hissuCCess.

**G -> P, W-> G, X->Q, X->Z. And the final text is:**

Modern western cryptology emerged directly from the flowering of modern diplomacy. The ambassadors' reports were sometimes opened and 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 and deciphering messages, and solving intercepted dispatches. Sometimes the cryptanalysts were separate from the cipher secretaries and were called in only when needed. Perhaps the most elaborate organization was Venice’s. It fell under the immediate control of the council of ten, the powerful and mysterious body that ruled the republic largely through its efficient secret police. Venice owed her preeminence largely to Giovanni Oro, who was perhaps the west's first great cryptanalyst. Soro, appointed cipher secretary in 1506, enjoyed remarkable success in solving the ciphers of numerous principalities. his solution of a dispatch of mark Anthony Coloana, chief of the army of the holy roman emperor Maximilian, requesting 20,000 ducats or the presence of the emperor with the army, gave an insight into Colonna’s problems. So great was Soro's fame that other courts sharpened their ciphers, and as early as1510 the papal curia was sending him ciphers that no one in Rome could solve. But Venice had no monopoly. in 1589, henry of Navarre, who was destined to become the most popular king in the history of France (he coined the slogan "a chicken in every peasant's pot every Sunday"), ascended to the throne as henry viand found himself embroiled still more fiercely in his bitter contest with the holy league, a catholic faction that refused to concede that a protestant could wear the crown. The league, headed by the duke of Moyenne, held Paris and all the other large cities of France, and was receiving large transfusions of men and money from Philip of Spain. Henry was tightly hemmed in, and it was at this Juncture that some correspondence between Philip and two of his liaison officers, commander Juan de Moreo and ambassador mannose, fell into Henry's hands.It was in cipher, but he had in his government at the time one Francois Viète, the seigneur de la bigot ere, a 49-year-old lawyer from Poitou who had risen to become counselor of the parliament, or court of Justice, of tours and a privy counselor to henry. Viète had for years amused himself with mathematics as a hobby-"never was a man more born for mathematics," said telemen des reauz. as the man who first used letters for quantities in algebra, giving that study its characteristic look, Viète is today remembered as the father of algebra. a year before, he had solved a Spanish dispatch addressed to Alessandro Farnese, the duke of Parma, who headed the Spanish forces of the league. Henry turned the new intercepts over to him to see if Viète could repeat his success.