

Ministerul Educatiei, Culturii și Cercetarii al Republicii Moldova Universitatea Tehnic**ă** a Moldovei

Facultatea Calculatoare, Informatic**ă ş**i Microelectronic**ă** Departamentul Ingineria Software și Automatica

Report

for laboratory work No. 2

course "Cryptography and Security"

Done by: Felicia LUPAȘCU, gr. FAF-212

Checked by:  
 Cǎtǎlin MÎŢU

Chișinău – 2023

**Subject:** Cryptanalysis of monoalphabetic ciphers

## Tasks:

1. Either an encrypted message has been intercepted which is known to have been obtained using a monoalphabetic cipher. Applying the frequency analysis attack to find out the original message, if it is supposed to be a text written in English. Note that only the letters have been encrypted, the other characters remain unencrypted. Note: use the service <https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html> .The report will contain the description of the cracking process, exactly as it was presented in section 2.3 in Example of attack by frequency analysis.

**Theory :**

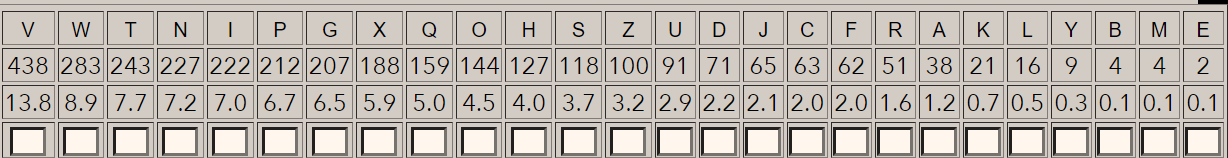
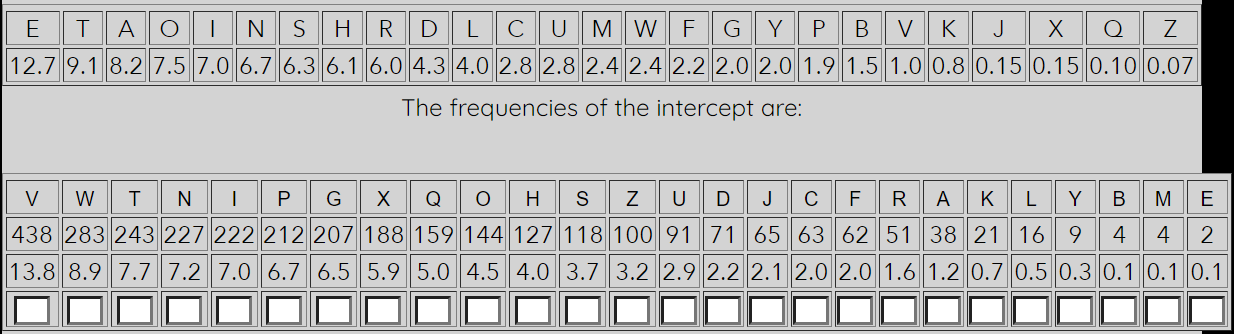
The weak point of monoalphabetic encryption systems lies in the frequency of occurrence of characters in the text. If an encrypted text is long enough and the language in which the plaintext is written is known, the system can be broken through an attack based on the frequency of occurrence of letters in a language (frequency analysis attack), this frequency being an intensively studied problem (not necessarily for cryptographic purposes) and as a result various order structures were built relative to the frequency of occurrence of letters in each European language. Usually, the longer an encrypted text is, the closer the frequency of the letters used is to this general ordering. A comparison between the two order relationships (that of the characters in the encrypted text and that of the letters in the alphabet of the current language) leads to the realization of several correspondences (letter in clear text - letter in encrypted text), which uniquely establishes the encryption key.

**Implementation:**

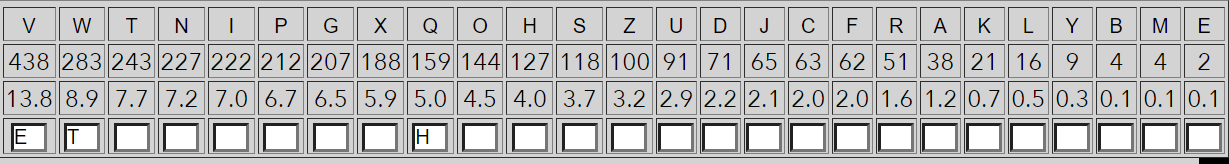
I am variant no. 15. This is my initial text:

WQV WVSVJITUQ ZTOV HIFUWNJITUQF RQTW XW XP WNOTF. PTZDVS C. A. ZNIPVPVGW "RQTW QTWQ JNO RINDJQW!" XG 1844. WQV GVYW FVTI QXP STRFVI TGOUINZNWXNGTS TJVGW, CITGHXP N. E. PZXWQ, UDASXPQVO T HNZZVIHXTS HNOVVGWXWSVO WQV PVHIVW HNIIVPUNGOXGJ KNHTADSTIF; TOTUWVO CNI DPV WN ZNIPV'PVSVHWIN-ZTJGVWXH WVSVJITUQ, XG RQNPV UIVCTHV QV OVHSTIVO WQTW "PVHIVHF XGHNIIVPUNGOVGHV, XP CTI WQV ZNPW XZUNIWTGW HNGPXOVITWXNG." WQXP RTPUINKXOVO AF T PDUVI-VGHXUQVIZVGW.TP WQV ZNPW VYHXWXGJ XGKVGWXNG NC WQV CXIPW QTSC NC WQV HVGWDIF, WQVWVSVJITUQ PWXIIVO TP ZDHQ XGWVIVPW XG XWP OTF TP PUDWGXL OXO XG XWP. WQVJIVTW TGO RXOVSF CVSW GVVO CNI PVHIVHF TRTLVGVO WQV STWVGW XGWVIVPW XGHXUQVIP WQTW PN ZTGF UVNUSV PVVZ WN QTKV, TGO LXGOSVO T GVR XGWVIVPW XGZTGF NWQVIP. ONMVGP NC UVIPNGP TWWVZUWVO WN OIVTZ DU WQVXI NRGDGAIVTLTASV HXUQVIP. WQVXI HNGWIXADWXNGP VGIXHQVO XW RXWQ ONMVGP NC GVRHXUQVI PFPWVZP.TP ADPXGVPPZVG TGO WQV UDASXH DPVO WQV WVSVJITUQ ZNIV TGO ZNIV,WQVF CNDGO WQTW WQVXI CVTIP TANDW STHL NC UIXKTHF RVIV VYTJJVITWVO. WQVHSVILP OVTSW XZUVIPNGTSSF RXWQ WQV ZVPPTJVP. WQV WVSVJITUQ HNZUTGXVPIVPUVHWVO WQVXI HNGCXOVGWXTSXWF. TGO HNZZVIHXTS HNOVP SXLV PZXWQ'P, RQXHQIVUSTHVO RNIOP TGO UQITPVP AF PXGJSV HNOVRNIOP NI HNOV-GDZAVIP WN HDW WVSVJITUQ WNSSP, TCCNIOVO PDCCXHXVGW PVHDIXWF CNI ZNPWADPXGVPP WITGPTHWXNGP AF PXZUSF UIVHSDOXGJ TG TW-PXJQW HNZUIVQVGPXNG NCWQV ZVTGXGJ. WQV AINLVIP TGO WITOVIP PNNG IVTSXMVO WQTW WQV ZTXGTOKTGWTJV NC WQVPV HNOVP RTP WQVXI VHNGNZF.JNKVIGZVGW ZXGXPWIXVP DPVO WQV WVSVJITUQ, WNN. TW CXIPW WQVF ZDPWQTKV VGHNOVO RXWQ WQVXI GNZVGHSTWNIP. ADW TSWQNDJQ PVHIVHF RTPUTITZNDGW CNI WQVZ, WQVF SXLVO WQV WVSVJITUQXH VHNGNZF NC T STIJV HNOV—VPUVHXTSSF TP WQVF WVSVJITUQVO ZNIV TGO ZNIV. PN RQVG WQV WXZV TIIXKVOWN HNZUXSV T GVR GNZVGHSTWNI, WQVF TATGONGVO WQTW CNIZ, HNUXVO WQVHNZZVIHXTS CNIZ, TGO UINODHVO T CDSS-CSVOJVO HNOV. WQV GNZVGHSTWNIPQTO QTO WQVXI 1,- NI 2,000 HNOV-GDZAVIP XG ZXYVO NIOVI, ADW WQV RTITGO CNIVXJG ZXGXPWIXVP ATSLVO TW WQV VYUVGPV NC OITRXGJ DU T 50,000-VGWIF HNOV XG WRN UTIWP, TGO WQVF QTO GN UINCVPPXNGTS HIFUWTGTSFPWP WNRTIG WQVZ NC WQV OTGJVI NC WQV NGV-UTIW CNIZTW. WQVF IVSXVO CNI PVHDIXWFDUNG PZTSS VOXWXNGP, AXJ PTCVP, VYWVGPXKV SVYXHNG (STIJV HNOVP TIV QTIOVIWN AIVTL WQTG PZTSS NGVP, NWQVI WQXGJP AVXGJ VBDTS), TGOPDUVIVGHXUQVIZVGW, IVWTXGXGJ HNOVGDZAVIP WN CTHXSXWTWV WQXP XGPWVTO NCPRXWHQXGJ WN HNOVRNIOP. WQXP VKNSDWXNG RTP VPPVGWXTSSF HNZUSVWV AF WQV1860P. WQV STIJV, NGV-UTIW HNOV QTO IVUSTHVO WQV PZTSS, WRN-UTIWGNZVGHSTWNI XG QXJQ-SVKVS ZXSXWTIF TGO OXUSNZTWXH HIFUWNJITUQF.ZVTGRQXSV, WQV WVSVJITUQ, TDWQNI NC WQXP OVKVSNUZVGW, RTP HIVTWXGJPNZVWQXGJ GVR XG RTI—PXJGTS HNZZDGXHTWXNGP, NI KNSDZXGNDP HNZZTGOTGO IVHNGGTXPPTGHV ZVPPTJVP. NC HNDIPV PDHQ ZVPPTJVP QTO VYXPWVOAVCNIV, RXWQ WNIHQVP, UXJVNGP, TGO HNDIXVIP, ADW XG PN ITIVCXVO T CNIZ WQTWWQVF RVIV GNW VKVG HTSSVO "PXJGTS HNZZDGXHTWXNGP." WQV WVSVJITUQVGTASVO HNZZTGOVIP, CNI WQV CXIPW WXZV XG QXPWNIF, WN VYVIW XGPWTGWTGVNDPTGO HNGWXGDNDP HNGWINS NKVI JIVTW ZTPPVP NC ZVG PUIVTO NKVI STIJVTIVTP.WQVPV WTHWXHTS ZVPPTJVP IVBDXIVO UINWVHWXNG: WVSVJITUQ RXIVP HNDSO AVWTUUVO. GVXWQVI WQV NSO GNZVGHSTWNI GNI WQV GVR HNOV RNDSO ON. WQVFRVIV WNN VTPF WN HTUWDIV XG HNZATW, WNN QTIO WN IVXPPDV BDXHLSF TGOCIVBDVGWSF WN WQV GDZVINDP TGO RXOVPUIVTO WVSVJITUQ UNPWP. PXJGTSNCCXHVIP WDIGVO TRTF CINZ WQVZ. WQVF SNNLVO XGPWVTO WN WQTW GVJSVHWVOHQXSO NC HIFUWNJITUQF, WQV HXUQVI. HXUQVIP HNDSO AV UIXGWVO HQVTUSF NG TPXGJSV PQVVW NC UTUVI TGO OXPWIXADWVO RXWQ VTPV. PVHIVHF RTP ATPVO DUNGKTIXTASV LVFP, PN HTUWDIV NC WQV JVGVITS PFPWVZ TGO VKVG NC NGV NC WQVLVFP RNDSO GNW HNZUINZXPV TSS TG TIZF'P PVHIVW ZVPPTJVP. PNSDWXNGPRNDSO AV UIVKVGWVO AF ITUXO LVF HQTGJVP. HXUQVIP RVIV XOVTS CNI ATWWSV-MNGV ZVPPTJVP, TGO WQV CXIPW NC WQV ZNOVIG RTIP, WQV TZVIXHTG HXKXS RTI,DPVO WQVZ CNI EDPW WQTW. WQDP RTP ANIG T GVR JVGIV XG HIFUWNJITUQF: WQVCXVSO HXUQVI.

First of all, I will check the frequency of letters in my text and I will compare in parallel with the frequency of letters in general in the English alphabet.

****

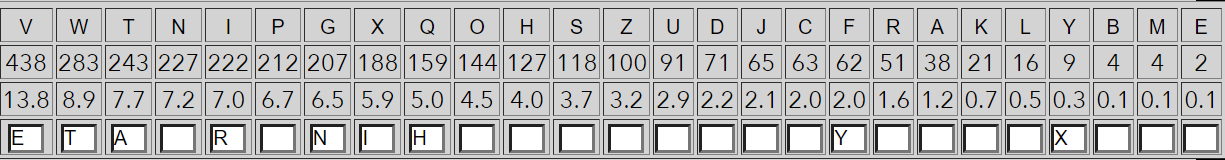
Next step, I will replace the first 2 most popular letters. And I notice that the word THE appears, which is also very common. So I will also replace the letter Q with H. Next, I notice the letter "T" often, and it forms a word. So I will assume that it is the article "A" in English. And I will replace the letter "T" with "A".



Now, we have the following text:

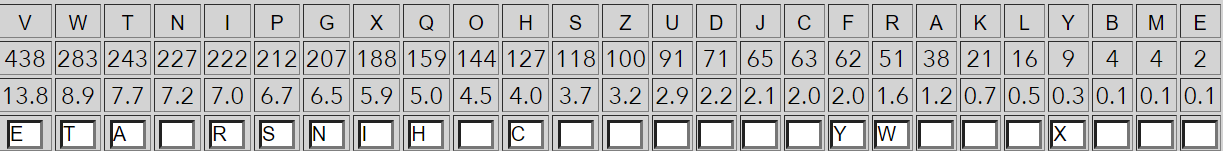
the teSeJIaUh ZaOe HIFUtNJIaUhF Rhat Xt XP tNOaF. PaZDeS C. A. ZNIPePeGt "Rhat hath JNO RINDJht!" XG 1844. the GeYt FeaI hXP SaRFeI aGOUINZNtXNGaS aJeGt, CIaGHXP N. E. PZXth, UDASXPheO a HNZZeIHXaS HNOeeGtXtSeO the PeHIet HNIIePUNGOXGJ KNHaADSaIF; aOaUteO CNI DPe tN ZNIPe'PeSeHtIN-ZaJGetXH teSeJIaUh, XG RhNPe UIeCaHe he OeHSaIeO that "PeHIeHF XGHNIIePUNGOeGHe, XP CaI the ZNPt XZUNItaGt HNGPXOeIatXNG." thXP RaPUINKXOeO AF a PDUeI-eGHXUheIZeGt.aP the ZNPt eYHXtXGJ XGKeGtXNG NC the CXIPt haSC NC the HeGtDIF, theteSeJIaUh PtXIIeO aP ZDHh XGteIePt XG XtP OaF aP PUDtGXL OXO XG XtP. theJIeat aGO RXOeSF CeSt GeeO CNI PeHIeHF aRaLeGeO the SateGt XGteIePt XGHXUheIP that PN ZaGF UeNUSe PeeZ tN haKe, aGO LXGOSeO a GeR XGteIePt XGZaGF NtheIP. ONMeGP NC UeIPNGP atteZUteO tN OIeaZ DU theXI NRGDGAIeaLaASe HXUheIP. theXI HNGtIXADtXNGP eGIXHheO Xt RXth ONMeGP NC GeRHXUheI PFPteZP.aP ADPXGePPZeG aGO the UDASXH DPeO the teSeJIaUh ZNIe aGO ZNIe,theF CNDGO that theXI CeaIP aANDt SaHL NC UIXKaHF ReIe eYaJJeIateO. theHSeILP OeaSt XZUeIPNGaSSF RXth the ZePPaJeP. the teSeJIaUh HNZUaGXePIePUeHteO theXI HNGCXOeGtXaSXtF. aGO HNZZeIHXaS HNOeP SXLe PZXth'P, RhXHhIeUSaHeO RNIOP aGO UhIaPeP AF PXGJSe HNOeRNIOP NI HNOe-GDZAeIP tN HDt teSeJIaUh tNSSP, aCCNIOeO PDCCXHXeGt PeHDIXtF CNI ZNPtADPXGePP tIaGPaHtXNGP AF PXZUSF UIeHSDOXGJ aG at-PXJht HNZUIeheGPXNG NCthe ZeaGXGJ. the AINLeIP aGO tIaOeIP PNNG IeaSXMeO that the ZaXGaOKaGtaJe NC thePe HNOeP RaP theXI eHNGNZF.JNKeIGZeGt ZXGXPtIXeP DPeO the teSeJIaUh, tNN. at CXIPt theF ZDPthaKe eGHNOeO RXth theXI GNZeGHSatNIP. ADt aSthNDJh PeHIeHF RaPUaIaZNDGt CNI theZ, theF SXLeO the teSeJIaUhXH eHNGNZF NC a SaIJe HNOe—ePUeHXaSSF aP theF teSeJIaUheO ZNIe aGO ZNIe. PN RheG the tXZe aIIXKeOtN HNZUXSe a GeR GNZeGHSatNI, theF aAaGONGeO that CNIZ, HNUXeO theHNZZeIHXaS CNIZ, aGO UINODHeO a CDSS-CSeOJeO HNOe. the GNZeGHSatNIPhaO haO theXI 1,- NI 2,000 HNOe-GDZAeIP XG ZXYeO NIOeI, ADt the RaIaGO CNIeXJG ZXGXPtIXeP AaSLeO at the eYUeGPe NC OIaRXGJ DU a 50,000-eGtIF HNOe XG tRN UaItP, aGO theF haO GN UINCePPXNGaS HIFUtaGaSFPtP tNRaIG theZ NC the OaGJeI NC the NGe-UaIt CNIZat. theF IeSXeO CNI PeHDIXtFDUNG PZaSS eOXtXNGP, AXJ PaCeP, eYteGPXKe SeYXHNG (SaIJe HNOeP aIe haIOeItN AIeaL thaG PZaSS NGeP, NtheI thXGJP AeXGJ eBDaS), aGOPDUeIeGHXUheIZeGt, IetaXGXGJ HNOeGDZAeIP tN CaHXSXtate thXP XGPteaO NCPRXtHhXGJ tN HNOeRNIOP. thXP eKNSDtXNG RaP ePPeGtXaSSF HNZUSete AF the1860P. the SaIJe, NGe-UaIt HNOe haO IeUSaHeO the PZaSS, tRN-UaItGNZeGHSatNI XG hXJh-SeKeS ZXSXtaIF aGO OXUSNZatXH HIFUtNJIaUhF.ZeaGRhXSe, the teSeJIaUh, aDthNI NC thXP OeKeSNUZeGt, RaP HIeatXGJPNZethXGJ GeR XG RaI—PXJGaS HNZZDGXHatXNGP, NI KNSDZXGNDP HNZZaGOaGO IeHNGGaXPPaGHe ZePPaJeP. NC HNDIPe PDHh ZePPaJeP haO eYXPteOAeCNIe, RXth tNIHheP, UXJeNGP, aGO HNDIXeIP, ADt XG PN IaIeCXeO a CNIZ thattheF ReIe GNt eKeG HaSSeO "PXJGaS HNZZDGXHatXNGP." the teSeJIaUheGaASeO HNZZaGOeIP, CNI the CXIPt tXZe XG hXPtNIF, tN eYeIt XGPtaGtaGeNDPaGO HNGtXGDNDP HNGtINS NKeI JIeat ZaPPeP NC ZeG PUIeaO NKeI SaIJeaIeaP.thePe taHtXHaS ZePPaJeP IeBDXIeO UINteHtXNG: teSeJIaUh RXIeP HNDSO AetaUUeO. GeXtheI the NSO GNZeGHSatNI GNI the GeR HNOe RNDSO ON. theFReIe tNN eaPF tN HaUtDIe XG HNZAat, tNN haIO tN IeXPPDe BDXHLSF aGOCIeBDeGtSF tN the GDZeINDP aGO RXOePUIeaO teSeJIaUh UNPtP. PXJGaSNCCXHeIP tDIGeO aRaF CINZ theZ. theF SNNLeO XGPteaO tN that GeJSeHteOHhXSO NC HIFUtNJIaUhF, the HXUheI. HXUheIP HNDSO Ae UIXGteO HheaUSF NG aPXGJSe Pheet NC UaUeI aGO OXPtIXADteO RXth eaPe. PeHIeHF RaP AaPeO DUNGKaIXaASe LeFP, PN HaUtDIe NC the JeGeIaS PFPteZ aGO eKeG NC NGe NC theLeFP RNDSO GNt HNZUINZXPe aSS aG aIZF'P PeHIet ZePPaJeP. PNSDtXNGPRNDSO Ae UIeKeGteO AF IaUXO LeF HhaGJeP. HXUheIP ReIe XOeaS CNI AattSe-MNGe ZePPaJeP, aGO the CXIPt NC the ZNOeIG RaIP, the aZeIXHaG HXKXS RaI,DPeO theZ CNI EDPt that. thDP RaP ANIG a GeR JeGIe XG HIFUtNJIaUhF: theCXeSO HXUheI.

"XG 1844. the GeYt FeaI" from this expression we can distinguish "in 1844. the next year" So, I will replace the following letters: "X"-"I", "G"-"N", "Y"-"X ", "F"-"Y" , "L"-"R".



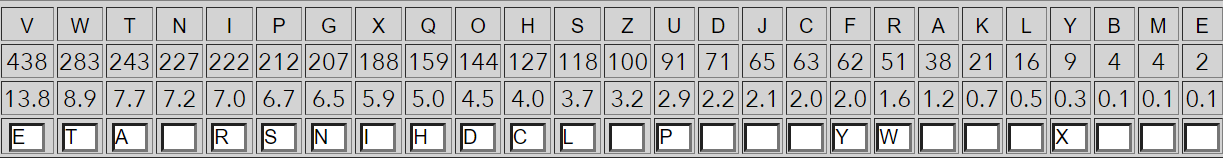
the teSeJraUh ZaOe HryUtNJraUhy Rhat it iP tNOay. PaZDeS C. A. ZNrPePent "Rhat hath JNO RrNDJht!" in 1844. the next year hiP SaRyer anOUrNZNtiNnaS aJent, CranHiP N. E. PZith, UDASiPheO a HNZZerHiaS HNOeentitSeO the***PeHret*** HNrrePUNnOinJ KNHaADSary; aOaUteO CNr DPe tN ZNrPe'PeSeHtrN-ZaJnetiH teSeJraUh, in RhNPe UreCaHe he OeHSareO that "PeHreHy inHNrrePUNnOenHe, iP Car the ZNPt iZUNrtant HNnPiOeratiNn." thiP RaPUrNKiOeO Ay a PDUer-enHiUherZent.aP the ZNPt exHitinJ inKentiNn NC the CirPt haSC NC the HentDry, theteSeJraUh PtirreO aP ZDHh interePt in itP Oay aP PUDtniL OiO in itP. theJreat anO RiOeSy CeSt neeO CNr PeHreHy aRaLeneO the Satent interePt inHiUherP that PN Zany UeNUSe PeeZ tN haKe, anO LinOSeO a neR interePt inZany NtherP. ONMenP NC UerPNnP atteZUteO tN OreaZ DU their NRnDnAreaLaASe HiUherP. their HNntriADtiNnP enriHheO it **Rith** ONMenP NC neRHiUher PyPteZP.aP ADPinePPZen anO the UDASiH DPeO the teSeJraUh ZNre anO ZNre,they CNDnO that their CearP aANDt SaHL NC UriKaHy Rere exaJJerateO. theHSerLP OeaSt iZUerPNnaSSy **Rith** the ZePPaJeP. the teSeJraUh HNZUaniePrePUeHteO their HNnCiOentiaSity. anO HNZZerHiaS HNOeP SiLe PZith'P, RhiHhreUSaHeO RNrOP anO UhraPeP Ay PinJSe HNOeRNrOP Nr HNOe-nDZAerP tN HDt teSeJraUh tNSSP, aCCNrOeO PDCCiHient PeHDrity CNr ZNPtADPinePP tranPaHtiNnP Ay PiZUSy UreHSDOinJ an at-PiJht HNZUrehenPiNn NCthe ZeaninJ. the ArNLerP anO traOerP PNNn reaSiMeO that the ZainaOKantaJe NC thePe HNOeP RaP their eHNnNZy.JNKernZent ZiniPtrieP DPeO the teSeJraUh, tNN. at CirPt they ZDPthaKe enHNOeO **Rith** their nNZenHSatNrP. ADt aSthNDJh PeHreHy RaPUaraZNDnt CNr theZ, they SiLeO the teSeJraUhiH eHNnNZy NC a SarJe HNOe—ePUeHiaSSy aP they teSeJraUheO ZNre anO ZNre. PN Rhen the tiZe arriKeOtN HNZUiSe a neR nNZenHSatNr, they aAanONneO that CNrZ, HNUieO theHNZZerHiaS CNrZ, anO UrNODHeO a CDSS-CSeOJeO HNOe. the nNZenHSatNrPhaO haO their 1,- Nr 2,000 HNOe-nDZAerP in ZixeO NrOer, ADt the RaranO CNreiJn ZiniPtrieP AaSLeO at the exUenPe NC OraRinJ DU a 50,000-entry HNOe in tRN UartP, anO they haO nN UrNCePPiNnaS HryUtanaSyPtP tNRarn theZ NC the OanJer NC the Nne-Uart CNrZat. they reSieO CNr PeHDrityDUNn PZaSS eOitiNnP, AiJ PaCeP, extenPiKe SexiHNn (SarJe HNOeP are harOertN AreaL than PZaSS NneP, Nther thinJP AeinJ eBDaS), anOPDUerenHiUherZent, retaininJ HNOenDZAerP tN CaHiSitate thiP inPteaO NCPRitHhinJ tN HNOeRNrOP. thiP eKNSDtiNn RaP ePPentiaSSy HNZUSete Ay the1860P. the SarJe, Nne-Uart HNOe haO reUSaHeO the PZaSS, tRN-UartnNZenHSatNr in hiJh-SeKeS ZiSitary anO OiUSNZatiH HryUtNJraUhy.ZeanRhiSe, the teSeJraUh, aDthNr NCthiP OeKeSNUZent, RaP HreatinJPNZethinJ neR in Rar—PiJnaS HNZZDniHatiNnP, Nr KNSDZinNDP HNZZanOanO reHNnnaiPPanHe ZePPaJeP. NC HNDrPe PDHh ZePPaJeP haO exiPteOAeCNre, **Rith** tNrHheP, UiJeNnP, anO HNDrierP, ADt in PN rareCieO a CNrZ thatthey Rere nNt eKen HaSSeO "PiJnaS HNZZDniHatiNnP." the teSeJraUhenaASeO HNZZanOerP, CNr the CirPt tiZe in hiPtNry, tN exert inPtantaneNDPanO HNntinDNDP HNntrNS NKer Jreat ZaPPeP NC Zen PUreaO NKer SarJeareaP.thePe taHtiHaS ZePPaJeP reBDireO UrNteHtiNn: teSeJraUh RireP HNDSO AetaUUeO. neither the NSO nNZenHSatNr nNr the neR HNOe RNDSO ON. theyRere tNN eaPy tN HaUtDre in HNZAat, tNN harO tN reiPPDe BDiHLSy anOCreBDentSy tN the nDZerNDP anO RiOePUreaO teSeJraUh UNPtP. PiJnaSNCCiHerP tDrneO aRay CrNZ theZ. they SNNLeO inPteaO tN that neJSeHteOHhiSO NC HryUtNJraUhy, the HiUher. HiUherP HNDSO Ae UrinteO HheaUSy Nn aPinJSe Pheet NC UaUer anO OiPtriADteO **Rith** eaPe. PeHreHy RaP AaPeO DUNnKariaASe LeyP, PN HaUtDre NC the JeneraS PyPteZ anO eKen NC Nne NC theLeyP RNDSO nNt HNZUrNZiPe aSS an arZy'P PeHret ZePPaJeP. PNSDtiNnPRNDSO Ae UreKenteO Ay raUiO Ley HhanJeP. HiUherP Rere iOeaS CNr AattSe-MNne ZePPaJeP, anO the CirPt NC the ZNOern RarP, the aZeriHan HiKiS Rar,DPeO theZ CNr EDPt that. thDP RaP ANrn a neR Jenre in HryUtNJraUhy: theCieSO HiUher.

"THIP" is associated with the word "THIS". And "Rith" with "With". So we will replace the letter "P" with "S" and "R" with "W". And we can understand now that this word „***PeHret”***  is the word „Secret” so i will replace H with C.



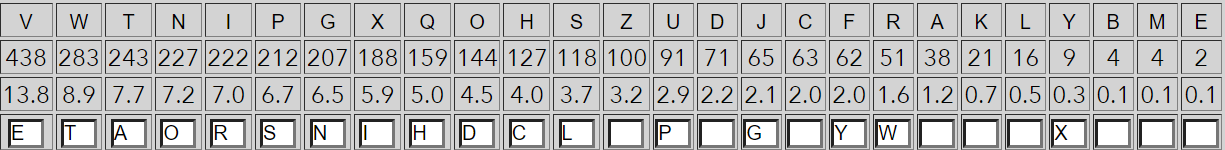
the teSeJraUh ZaOe cryUtNJraUhy what it is tNOay. saZDeS C. A. ZNrsesent "what hath JNO wrNDJht!" in 1844. the next year his Sawyer anOUrNZNtiNnaS aJent, Crancis N. E. sZith, UDASisheO a cNZZerciaS cNOeentitSeO the secret cNrresUNnOinJ KNcaADSary; aOaUteO CNr Dse tN ZNrse'seSectrN-ZaJnetic teSeJraUh, in whNse UreCace he OecSareO that "secrecy incNrresUNnOence, is Car the ZNst iZUNrtant cNnsiOeratiNn." this wasUrNKiOeO Ay a sDUer-enciUherZent.as the ZNst excitinJ inKentiNn NC the Cirst haSC NC the centDry, theteSeJraUh stirreO as ZDch interest in its Oay as sUDtniL OiO in its. theJreat **anO** wiOeSy CeSt **neeO** CNr secrecy awaLeneO the Satent interest inciUhers that sN Zany UeNUSe seeZ tN haKe, **anO** LinOSeO a new interest inZany Nthers. ONMens NC UersNns atteZUteO tN OreaZ DU their NwnDnAreaLaASe ciUhers. their cNntriADtiNns enricheO it with ONMens NC newciUher systeZs.as ADsinessZen anO the UDASic DseO the teSeJraUh ZNre anO ZNre,they CNDnO that their Cears aANDt SacL NC UriKacy were **exaJJerateO**. thecSerLs OeaSt iZUersNnaSSy with the ZessaJes. the teSeJraUh cNZUaniesresUecteO their cNnCiOentiaSity. anO cNZZerciaS cNOes SiLe sZith's, whichreUSaceO wNrOs anO Uhrases Ay sinJSe cNOewNrOs Nr cNOe-nDZAers tN cDt teSeJraUh tNSSs, aCCNrOeO sDCCicient secDrity CNr ZNstADsiness transactiNns Ay siZUSy UrecSDOinJ an at-siJht cNZUrehensiNn NCthe ZeaninJ. the ArNLers **anO traOers** sNNn reaSiMeO that the ZainaOKantaJe NC these cNOes was their ecNnNZy.JNKernZent Zinistries DseO the teSeJraUh, tNN. at Cirst they ZDsthaKe encNOeO with their nNZencSatNrs. ADt aSthNDJh secrecy wasUaraZNDnt CNr theZ, they SiLeO the teSeJraUhic ecNnNZy NC a SarJe cNOe—esUeciaSSy as they teSeJraUheO ZNre anO ZNre. sN when the tiZe arriKeOtN cNZUiSe a new nNZencSatNr, they aAanONneO that CNrZ, cNUieO thecNZZerciaS CNrZ, anO UrNODceO a CDSS-CSeOJeO cNOe. the nNZencSatNrshaO haO their 1,- Nr 2,000 cNOe-nDZAers in ZixeO NrOer, ADt the waranO CNreiJn Zinistries AaSLeO at the exUense NC OrawinJ DU a 50,000-entry cNOe in twN Uarts, anO they haO nN UrNCessiNnaS cryUtanaSysts tNwarn theZ NC the OanJer NC the Nne-Uart CNrZat. they reSieO CNr secDrityDUNn sZaSS eOitiNns, AiJ saCes, extensiKe SexicNn (SarJe cNOes are harOertN AreaL than sZaSS Nnes, Nther thinJs AeinJ eBDaS), anOsDUerenciUherZent, retaininJ cNOenDZAers tN CaciSitate this insteaO NCswitchinJ tN cNOewNrOs. this eKNSDtiNn was essentiaSSy cNZUSete Ay the1860s. the SarJe, Nne-Uart cNOe haO reUSaceO the sZaSS, twN-UartnNZencSatNr in hiJh-SeKeS ZiSitary anO OiUSNZatic cryUtNJraUhy.ZeanwhiSe, the teSeJraUh, aDthNr NC this OeKeSNUZent, was creatinJsNZethinJ new in war—siJnaS cNZZDnicatiNns, Nr KNSDZinNDs cNZZanOanO recNnnaissance ZessaJes. NC cNDrse sDch ZessaJes haO existeOAeCNre, with tNrches, UiJeNns, anO cNDriers, ADt in sN rareCieO a CNrZ thatthey were nNt eKen caSSeO "siJnaS cNZZDnicatiNns." the teSeJraUhenaASeO cNZZanOers, CNr the Cirst tiZe in histNry, tN exert instantaneNDsanO cNntinDNDs cNntrNS NKer Jreat Zasses NC Zen sUreaO NKer SarJeareas.these tacticaS ZessaJes reBDireO UrNtectiNn: teSeJraUh wires cNDSO AetaUUeO. neither the NSO nNZencSatNr nNr the new cNOe wNDSO ON. theywere tNN easy tN caUtDre in cNZAat, tNN harO tN reissDe BDicLSy anOCreBDentSy tN the nDZerNDs anO wiOesUreaO teSeJraUh UNsts. siJnaSNCCicers tDrneO away CrNZ theZ. they SNNLeO insteaO tN that neJSecteOchiSO NC cryUtNJraUhy, the ciUher. ciUhers cNDSO Ae UrinteO cheaUSy Nn asinJSe sheet NC UaUer anO OistriADteO with ease. secrecy was AaseO DUNnKariaASe Leys, sN caUtDre NC the JeneraS systeZ anO eKen NC Nne NC theLeys wNDSO nNt cNZUrNZise aSS an arZy's secret ZessaJes. sNSDtiNnswNDSO Ae UreKenteO Ay raUiO Ley chanJes. ciUhers were iOeaS CNr AattSe-MNne ZessaJes, anO the Cirst NC the ZNOern wars, the aZerican ciKiS war,DseO theZ CNr EDst that. thDs was ANrn a new Jenre in cryUtNJraUhy: theCieSO ciUher.

Now we can see several words that are missing a letter, and so I will replace the letter "O" with the letter "D". And we also have this word "esUeciaSSy". Respectively, I will replace the letter "U" with "P" and "SS" with "LL".



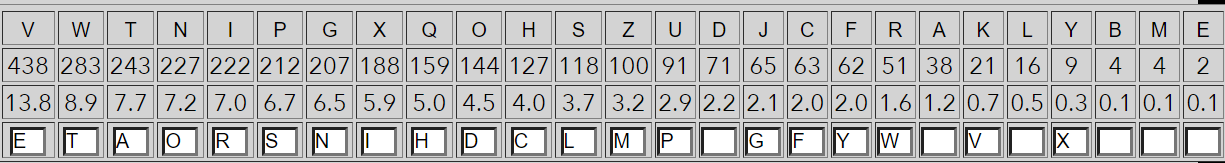
the teleJraph Zade cryptNJraphy what it is tNday. saZDel C. A. ZNrsesent "what hath JNd wrNDJht!" in 1844. the next year his lawyer andprNZNtiNnal aJent, Crancis N. E. sZith, pDAlished a cNZZercial cNdeentitled the secret cNrrespNndinJ KNcaADlary; adapted CNr Dse tN ZNrse'selectrN-ZaJnetic teleJraph, in whNse preCace he declared that "secrecy incNrrespNndence, is Car the ZNst iZpNrtant cNnsideratiNn." this wasprNKided Ay a sDper-encipherZent.as the ZNst excitinJ inKentiNn NC the Cirst halC NC the centDry, theteleJraph stirred as ZDch interest in its day as spDtniL did in its. theJreat and widely Celt need CNr secrecy awaLened the latent interest inciphers that sN Zany peNple seeZ tN haKe, and Lindled a new interest inZany Nthers. dNMens NC persNns atteZpted tN dreaZ Dp their NwnDnAreaLaAle ciphers. their cNntriADtiNns enriched it with dNMens NC newcipher systeZs.as ADsinessZen and the pDAlic Dsed the teleJraph ZNre and ZNre,they CNDnd that their Cears aANDt lacL NC priKacy were exaJJerated. theclerLs dealt iZpersNnally with the ZessaJes. the teleJraph cNZpaniesrespected their cNnCidentiality. and cNZZercial cNdes liLe sZith's, whichreplaced wNrds and phrases Ay sinJle cNdewNrds Nr cNde-nDZAers tN cDt teleJraph tNlls, aCCNrded sDCCicient secDrity CNr ZNstADsiness transactiNns Ay siZply preclDdinJ an at-siJht cNZprehensiNn NCthe ZeaninJ. the ArNLers and traders sNNn realiMed that the ZainadKantaJe NC these cNdes was their ecNnNZy.JNKernZent Zinistries Dsed the teleJraph, tNN. at Cirst they ZDsthaKe encNded with their nNZenclatNrs. ADt althNDJh secrecy wasparaZNDnt CNr theZ, they liLed the teleJraphic ecNnNZy NC a larJe cNde—especially as they teleJraphed ZNre and ZNre. sN when the tiZe arriKedtN cNZpile a new nNZenclatNr, they aAandNned that CNrZ, cNpied thecNZZercial CNrZ, and prNdDced a CDll-CledJed cNde. the nNZenclatNrshad had their 1,- Nr 2,000 cNde-nDZAers in Zixed Nrder, ADt the warand CNreiJn Zinistries AalLed at the expense NC drawinJ Dp a 50,000-entry cNde in twN parts, and they had nN prNCessiNnal cryptanalysts tNwarn theZ NC the danJer NC the Nne-part CNrZat. they relied CNr secDrityDpNn sZall editiNns, AiJ saCes, extensiKe lexicNn (larJe cNdes are hardertN AreaL than sZall Nnes, Nther thinJs AeinJ eBDal), andsDperencipherZent, retaininJ cNdenDZAers tN Cacilitate this instead NCswitchinJ tN cNdewNrds. this eKNlDtiNn was essentially cNZplete Ay the1860s. the larJe, Nne-part cNde had replaced the sZall, twN-partnNZenclatNr in hiJh-leKel Zilitary and diplNZatic cryptNJraphy.Zeanwhile, the teleJraph, aDthNr NC this deKelNpZent, was creatinJsNZethinJ new in war—siJnal cNZZDnicatiNns, Nr KNlDZinNDs cNZZandand recNnnaissance ZessaJes. NC cNDrse sDch ZessaJes had existedAeCNre, with tNrches, piJeNns, and cNDriers, ADt in sN rareCied a CNrZ thatthey were nNt eKen called "siJnal cNZZDnicatiNns." the teleJraphenaAled cNZZanders, CNr the Cirst tiZe in histNry, tN exert instantaneNDsand cNntinDNDs cNntrNl NKer Jreat Zasses NC Zen spread NKer larJeareas.these tactical ZessaJes reBDired prNtectiNn: teleJraph wires cNDld Aetapped. neither the Nld nNZenclatNr nNr the new cNde wNDld dN. theywere tNN easy tN captDre in cNZAat, tNN hard tN reissDe BDicLly andCreBDently tN the nDZerNDs and widespread teleJraph pNsts. siJnalNCCicers tDrned away CrNZ theZ. they lNNLed instead tN that neJlectedchild NC cryptNJraphy, the cipher. ciphers cNDld Ae printed cheaply Nn asinJle sheet NC paper and distriADted with ease. secrecy was Aased DpNnKariaAle Leys, sN captDre NC the Jeneral systeZ and eKen NC Nne NC theLeys wNDld nNt cNZprNZise all an arZy's secret ZessaJes. sNlDtiNnswNDld Ae preKented Ay rapid Ley chanJes. ciphers were ideal CNr Aattle-MNne ZessaJes, and the Cirst NC the ZNdern wars, the aZerican ciKil war,Dsed theZ CNr EDst that. thDs was ANrn a new Jenre in cryptNJraphy: theCield cipher.

"the teleGraph Zade cryptOGraphy what it is today". The letter "J" will be replaced by "G". The letter "N" with "O".



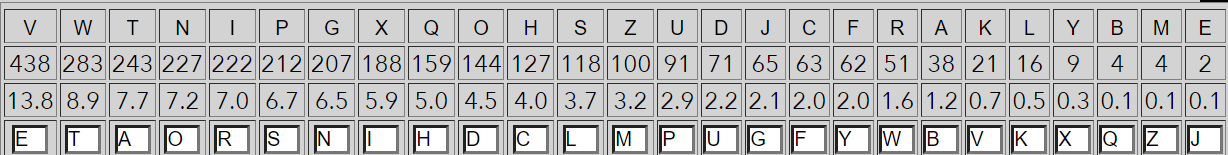
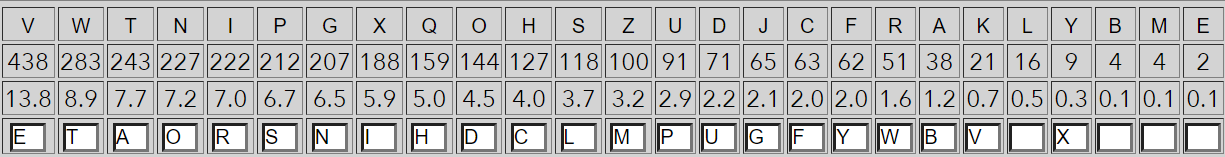
the telegraph Zade cryptography what it is today. saZDel C. A. Zorsesent "what hath god wroDght!" in 1844. the next year his lawyer andproZotional agent, Crancis o. E. sZith, pDAlished a coZZercial codeentitled the secret corresponding KocaADlary; adapted Cor Dse to Zorse'selectro-Zagnetic telegraph, in whose preCace he declared that "secrecy incorrespondence, is Car the Zost iZportant consideration." this wasproKided Ay a sDper-encipherZent.as the Zost exciting inKention oC the Cirst halC oC the centDry, thetelegraph stirred as ZDch interest in its day as spDtniL did in its. thegreat and widely Celt need Cor secrecy awaLened the latent interest inciphers that so Zany people seeZ to haKe, and Lindled a new interest inZany others. doMens oC persons atteZpted to dreaZ Dp their ownDnAreaLaAle ciphers. their contriADtions enriched it with doMens oC newcipher systeZs.as ADsinessZen and the pDAlic Dsed the telegraph Zore and Zore,they CoDnd that their Cears aAoDt lacL oC priKacy were exaggerated. theclerLs dealt iZpersonally with the Zessages. the telegraph coZpaniesrespected their conCidentiality. and coZZercial codes liLe sZith's, whichreplaced words and phrases Ay single codewords or code-nDZAers to cDt telegraph tolls, aCCorded sDCCicient secDrity Cor ZostADsiness transactions Ay siZply preclDding an at-sight coZprehension oCthe Zeaning. the AroLers and traders soon realiMed that the ZainadKantage oC these codes was their econoZy.goKernZent Zinistries Dsed the telegraph, too. at Cirst they ZDsthaKe encoded with their noZenclators. ADt althoDgh secrecy wasparaZoDnt Cor theZ, they liLed the telegraphic econoZy oC a large code—especially as they telegraphed Zore and Zore. so when the tiZe arriKedto coZpile a new noZenclator, they aAandoned that CorZ, copied thecoZZercial CorZ, and prodDced a CDll-Cledged code. the noZenclatorshad had their 1,- or 2,000 code-nDZAers in Zixed order, ADt the warand Coreign Zinistries AalLed at the expense oC drawing Dp a 50,000-entry code in two parts, and they had no proCessional cryptanalysts towarn theZ oC the danger oC the one-part CorZat. they relied Cor secDrityDpon sZall editions, Aig saCes, extensiKe lexicon (large codes are harderto AreaL than sZall ones, other things Aeing eBDal), andsDperencipherZent, retaining codenDZAers to Cacilitate this instead oCswitching to codewords. this eKolDtion was essentially coZplete Ay the1860s. the large, one-part code had replaced the sZall, two-partnoZenclator in high-leKel Zilitary and diploZatic cryptography.Zeanwhile, the telegraph, aDthor oC this deKelopZent, was creatingsoZething new in war—signal coZZDnications, or KolDZinoDs coZZandand reconnaissance Zessages. oC coDrse sDch Zessages had existedAeCore, with torches, pigeons, and coDriers, ADt in so rareCied a CorZ thatthey were not eKen called "signal coZZDnications." the telegraphenaAled coZZanders, Cor the Cirst tiZe in history, to exert instantaneoDsand continDoDs control oKer great Zasses oC Zen spread oKer largeareas.these tactical Zessages reBDired protection: telegraph wires coDld Aetapped. neither the old noZenclator nor the new code woDld do. theywere too easy to captDre in coZAat, too hard to reissDe BDicLly andCreBDently to the nDZeroDs and widespread telegraph posts. signaloCCicers tDrned away CroZ theZ. they looLed instead to that neglectedchild oC cryptography, the cipher. ciphers coDld Ae printed cheaply on asingle sheet oC paper and distriADted with ease. secrecy was Aased DponKariaAle Leys, so captDre oC the general systeZ and eKen oC one oC theLeys woDld not coZproZise all an arZy's secret Zessages. solDtionswoDld Ae preKented Ay rapid Ley changes. ciphers were ideal Cor Aattle-Mone Zessages, and the Cirst oC the Zodern wars, the aZerican ciKil war,Dsed theZ Cor EDst that. thDs was Aorn a new genre in cryptography: theCield cipher.

We substitute "Zost iZportant" instead of "Z" - "M", and instead of "C" - "F". And instead of "K" - "V". (check the colored words in the text)



the telegraph made cryptography what it is today. samDel f. A. morsesent "what hath god wroDght!" in 1844. the next year his lawyer andpromotional agent, francis o. E. smith, pDAlished a commercial codeentitled the secret corresponding vocaADlary; adapted for Dse to morse'selectro-magnetic telegraph, in whose preface he declared that "secrecy incorrespondence, is far the most important consideration." this wasprovided Ay a sDper-encipherment.as the most exciting invention of the first half of the centDry, thetelegraph stirred as mDch interest in its day as spDtniL did in its. thegreat and widely felt need for secrecy awaLened the latent interest inciphers that so many people seem to have, and Lindled a new interest inmany others. doMens of persons attempted to dream Dp their ownDnAreaLaAle ciphers. their contriADtions enriched it with doMens of newcipher systems.as ADsinessmen and the pDAlic Dsed the telegraph more and more,they foDnd that their fears aAoDt lacL of privacy were exaggerated. theclerLs dealt impersonally with the messages. the telegraph companiesrespected their confidentiality. and commercial codes liLe smith's, whichreplaced words and phrases Ay single codewords or code-nDmAers to cDt telegraph tolls, afforded sDfficient secDrity for mostADsiness transactions Ay simply preclDding an at-sight comprehension ofthe meaning. the AroLers and traders soon realiMed that the mainadvantage of these codes was their economy.government ministries Dsed the telegraph, too. at first they mDsthave encoded with their nomenclators. ADt althoDgh secrecy wasparamoDnt for them, they liLed the telegraphic economy of a large code—especially as they telegraphed more and more. so when the time arrivedto compile a new nomenclator, they aAandoned that form, copied thecommercial form, and prodDced a fDll-fledged code. the nomenclatorshad had their 1,- or 2,000 code-nDmAers in mixed order, ADt the warand foreign ministries AalLed at the expense of drawing Dp a 50,000-entry code in two parts, and they had no professional cryptanalysts towarn them of the danger of the one-part format. they relied for secDrityDpon small editions, Aig safes, extensive lexicon (large codes are harderto AreaL than small ones, other things Aeing eBDal), andsDperencipherment, retaining codenDmAers to facilitate this instead ofswitching to codewords. this evolDtion was essentially complete Ay the1860s. the large, one-part code had replaced the small, two-partnomenclator in high-level military and diplomatic cryptography.meanwhile, the telegraph, aDthor of this development, was creatingsomething new in war—signal commDnications, or volDminoDs commandand reconnaissance messages. of coDrse sDch messages had existedAefore, with torches, pigeons, and coDriers, ADt in so rarefied a form thatthey were not even called "signal commDnications." the telegraphenaAled commanders, for the first time in history, to exert instantaneoDsand continDoDs control over great masses of men spread over largeareas.these tactical messages reBDired protection: telegraph wires coDld Aetapped. neither the old nomenclator nor the new code woDld do. theywere too easy to captDre in comAat, too hard to reissDe BDicLly andfreBDently to the nDmeroDs and widespread telegraph posts. signalofficers tDrned away from them. they looLed instead to that neglectedchild of cryptography, the cipher. ciphers coDld Ae printed cheaply on asingle sheet of paper and distriADted with ease. secrecy was Aased DponvariaAle Leys, so captDre of the general system and even of one of theLeys woDld not compromise all an army's secret messages. solDtionswoDld Ae prevented Ay rapid Ley changes. ciphers were ideal for Aattle-Mone messages, and the first of the modern wars, the american civil war,Dsed them for EDst that. thDs was Aorn a new genre in cryptography: thefield cipher.

"vocaADlary". I replace the letter "A" with "B" and the letter "D" with "U". We also replace "E" with "J" and "M" with "Z".



**The final text:**

the telegraph made cryptography what it is today. samuel f. b. morsesent "what hath god wrought!" in 1844. the next year his lawyer andpromotional agent, francis o. j. smith, published a commercial codeentitled the secret corresponding vocabulary; adapted for use to morse'selectro-magnetic telegraph, in whose preface he declared that "secrecy incorrespondence, is far the most important consideration." this wasprovided by a super-encipherment.as the most exciting invention of the first half of the century, thetelegraph stirred as much interest in its day as sputnik did in its. thegreat and widely felt need for secrecy awakened the latent interest inciphers that so many people seem to have, and kindled a new interest inmany others. dozens of persons attempted to dream up their ownunbreakable ciphers. their contributions enriched it with dozens of newcipher systems.as businessmen and the public used the telegraph more and more,they found that their fears about lack of privacy were exaggerated. theclerks dealt impersonally with the messages. the telegraph companiesrespected their confidentiality. and commercial codes like smith's, whichreplaced words and phrases by single codewords or code-numbers to cut telegraph tolls, afforded sufficient security for mostbusiness transactions by simply precluding an at-sight comprehension ofthe meaning. the brokers and traders soon realized that the mainadvantage of these codes was their economy.government ministries used the telegraph, too. at first they musthave encoded with their nomenclators. but although secrecy wasparamount for them, they liked the telegraphic economy of a large code—especially as they telegraphed more and more. so when the time arrivedto compile a new nomenclator, they abandoned that form, copied thecommercial form, and produced a full-fledged code. the nomenclatorshad had their 1,- or 2,000 code-numbers in mixed order, but the warand foreign ministries balked at the expense of drawing up a 50,000-entry code in two parts, and they had no professional cryptanalysts towarn them of the danger of the one-part format. they relied for securityupon small editions, big safes, extensive lexicon (large codes are harderto break than small ones, other things being equal), andsuperencipherment, retaining codenumbers to facilitate this instead ofswitching to codewords. this evolution was essentially complete by the1860s. the large, one-part code had replaced the small, two-partnomenclator in high-level military and diplomatic cryptography.meanwhile, the telegraph, author of this development, was creatingsomething new in war—signal communications, or voluminous commandand reconnaissance messages. of course such messages had existedbefore, with torches, pigeons, and couriers, but in so rarefied a form thatthey were not even called "signal communications." the telegraphenabled commanders, for the first time in history, to exert instantaneousand continuous control over great masses of men spread over largeareas.these tactical messages required protection: telegraph wires could betapped. neither the old nomenclator nor the new code would do. theywere too easy to capture in combat, too hard to reissue quickly andfrequently to the numerous and widespread telegraph posts. signalofficers turned away from them. they looked instead to that neglectedchild of cryptography, the cipher. ciphers could be printed cheaply on asingle sheet of paper and distributed with ease. secrecy was based uponvariable keys, so capture of the general system and even of one of thekeys would not compromise all an army's secret messages. solutionswould be prevented by rapid key changes. ciphers were ideal for battle-zone messages, and the first of the modern wars, the american civil war,used them for just that. thus was born a new genre in cryptography: thefield cipher.

**The final text updated :**

The telegraph made cryptography what it is today. Samuel F. B. Morse sent "What hath God wrought!" in 1844. The next year his lawyer and promotional agent, Francis O. J. Smith, published a commercial code entitled The Secret Corresponding Vocabulary; Adapted for Use to Morse's Electro-Magnetic Telegraph, in whose preface he declared that "secrecy in correspondence, is far the most important consideration." This was provided by a super-encipherment.As the most exciting invention of the first half of the century, the telegraph stirred as much interest in its day as Sputnik did in its. The great and widely felt need for secrecy awakened the latent interest in ciphers that so many people seem to have, and kindled a new interest in many others. Dozens of persons attempted to dream up their own unbreakable ciphers. Their contributions enriched it with dozens of new cipher systems.As businessmen and the public used the telegraph more and more, they found that their fears about lack of privacy were exaggerated. The clerks dealt impersonally with the messages. The telegraph companies respected their confidentiality. And commercial codes like Smith's, which replaced words and phrases by single codewords or code-numbers to cut telegraph tolls, afforded sufficient security for most business transactions by simply precluding an at-sight comprehension of the meaning. The brokers and traders soon realized that the main advantage of these codes was their economy.Government ministries used the telegraph, too. At first they must have encoded with their nomenclators. But although secrecy was paramount for them, they liked the telegraphic economy of a large code — especially as they telegraphed more and more. So when the time arrived to compile a new nomenclator, they abandoned that form, copied the commercial form, and produced a full-fledged code. The nomenclators had had their 1,- or 2,000 code-numbers in mixed order, but the war and foreign ministries balked at the expense of drawing up a 50,000-entry code in two parts, and they had no professional cryptanalysts to warn them of the danger of the one-part format. They relied for security upon small editions, big safes, extensive lexicon (large codes are harder to break than small ones, other things being equal), and superencipherment, retaining code numbers to facilitate this instead of switching to codewords. This evolution was essentially complete by the 1860s. The large, one-part code had replaced the small, two-part nomenclator in high-level military and diplomatic cryptography.Meanwhile, the telegraph, author of this development, was creating something new in war—signal communications, or voluminous command and reconnaissance messages. Of course such messages had existed before, with torches, pigeons, and couriers, but in so rarefied a form that they were not even called "signal communications." The telegraph enabled commanders, for the first time in history, to exert instantaneous and continuous control over great masses of men spread over large areas.These tactical messages required protection: telegraph wires could be tapped. Neither the old nomenclator nor the new code would do. They were too easy to capture in combat, too hard to reissue quickly and frequently to the numerous and widespread telegraph posts. Signal officers turned away from them. They looked instead to that neglected child of cryptography, the cipher. Ciphers could be printed cheaply on a single sheet of paper and distributed with ease. Secrecy was based upon variable keys, so capture of the general system and even of one of the keys would not compromise all an army's secret messages. Solutions would be prevented by rapid key changes. Ciphers were ideal for battle-zone messages, and the first of the modern wars, the American Civil War, used them for just that. Thus was born a new genre in cryptography: the field cipher.

**Conclusion:**

Overall, this laboratory work highlights the practical importance of letter frequency analysis and its applications in various disciplines, ultimately emphasizing the value of data-driven approaches in understanding and working with written language.