

Ministerul Educației și Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică



Laboratory work 2
Subject: Monoalphabetic script encryption

Done by:

Gitlan Gabriel
st. gr. FAF-213

Verified by:

Mîțu Cătălin
asist. univ.

Chișinău - 2023

Goal:

A message has been intercepted that is known to have been obtained through the use of a monoalphabetic cipher. By applying frequency analysis attack to discover the original message, assuming it is a text written in English, taking into account that only the letters have been encrypted, leaving the other characters unchanged.

Please use the following service:

<https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html>

The report will include a description of the breaking process, exactly as presented in section 2.3 in the Example of Frequency Analysis Attack.

Variant 18

Xw rtp Citghv, qnrkvi, wqtw udasxpqvo ngv nc hifuwnsnjfp jivtwvpwannlp. St Hifuwnjituqxhzxswtxiv cxipw tuuvtivo tp wrn xgpwtsszvgrp xgwqv Endigts ovp Phxvghvp zxsxwtxiv xg Etgdiftgo Cvaiftif nc 1883,avxgj ivxppdvo stwvi wqtw fvti tp t utuviathl annl af wqv endigts'pudasxpqvi. Xw xp wqv znpw hngxhpv annl ng hifuwnsnjf vkvi rixwwvg. Xwptdwqni qto wqv xgpwxghw cni wqv hifuwnjituqxh edjdsti, tgo qv hnzuivppvoxgwn 64 utjvp kxiwdtssf wqv vgwxiv lgnrg cxvso nc hifuwnsnjf, xghsdoxgjunsftsugtawwxhp rxwq zxyvo tsugtawvp, vghxuqvivo hnov, tgo hxuqviovkxhvp. Wqv annl xp tspn ngv nc wqv znpw phqnstisf ng hifuwnsnjf. Xwpcnnwgnwvp hxwv znpw hstppxhts tgo ztgf znovig pndihvp; hnzzvgrp pdhqtq "Wqxp xp gnw wqv ngsf qxpwnixhts ni axasxnjituqxh viini cni rqxhq wqv Tdpwixtg rixwvi zdpw av ivuinthqvo"pqnr qnr htivcdssf wqv tdwqni qtp pwdoxvo wqnpv pndihvp.Xwp tdwqni rtp anig Evtg-Jdxsstdzv-Qdaviw-Kxhwni-Citgjnpx-Tsvytgoiv-djdpwv Lvihlqncpp kng Gxvdrvgqnc ng Etgdift 19, 1835, twGdwq, Qnsstgo. Tcwvi jvwvxgj ovjivvp xg svwwwip tgo xg phxvghv cinz wqvDgxkvipxwf nc Sxvjv, qv rtp qxivo xg 1863 tp tg xgpwidhwni xg znovigstgjdjvvp tw wqv qxjq phqnns tw Zvsdg, t stjiv wnrg 25 zxsvp pndwqvtpwnc Utixp. Wqv gvyw fvti qv ztiixvo t jxis cinz wqv tivt tgo xg 1865, rqvgqv rtp 30, wqvf qto wqvx ngsf hqxso, t otdjqwvi, Utdsngxv. Qv pwtfvo twZvsdg cni 10 fvtip, wvthqxgj Vgjsxpq tgo Jvitzg.Af wqtw wxzv qv qto pqniwvgvo qxp gtzv wn Tdjdpwv Lvihlqncpp.Avtiovo, oxjgxcxvo, psnr nc puuvhq, Lvihlqncpp, ovpuvvp tg xgtaxsxf wnztxgwtg oxphxusxgv xg qxp hstppvp tgo pnzv vhhvgwixhxwvp nc hqtithwvi, rtp t "svtigvo, mvtsndp, htutasv" wvthqvi rqn trnlv qxp pwdovgwp'xgwwivpw xg wqvx rnil; qxp pduvixnip ptxo "qxp pwdovgwp sxlx qxz tgo nrlrxwq pdhhvvp." Tcwvirtio, qv rnilvo tp t uixktwv xgpwidhwni xg Utixp.Qxp adpxvpv fvtip cnssnrvo wqv udasxhtwxng nc St Hifuwnjituqxhzxswtxiv. T gvr xgwwigtwxngts stgjdjv htssvo Knstuxxl ("Rniso-Puvtl")qto avvg xgkvvgwo af t Jvitzg uixvpw. Tandw 1885, xw htdjqw ng xgCitghv tgo cstpqvo rxwq vyuiivpp-witxg puuvvo tss nkvi wqv hndgwif, gnwngsf tzngj xgwwssvhwtdsp adw tzngj tss hstppvp; xw rtp vkvg qvtio xg wqvpwivwvp. Cinz Citghv xw itoxtwvo wqindjqndw wqv rniso. Wqv znpw thwxkvuinutjgoxpw nc Knstuxxl rtp Tdjdpwv Lvihlqncpp, rqn, tw wqv pvhngoKnstuxxl hngjivvp xg Zdgxhq xg 1887, rtp thstxzo oxivhwni ("Oxsvlvs,"xg Knstuxxl) nc wqv Xgwwigtwxngts Thtovzf nc Knstuxxl. Adw tw wqv wqxiohngjivvp, qvso tw Utixp xg Ztf nc 1889, rxwq Lvihlqncpp uivpxoxgj, hixwxhtswvgpxngp rxwq xg wqv znkvzvgw zndgwo tgo cxgtssf ainlv xw tutiw.Lvihlqncpp rtp hidpqvo af wqv hnsstupv nc tg xgwwigtwxngts oivtz wqtwqto pvvzvo pn gvvocds tgo pn hviwtg. Qv hviwtvo gnwqxgj vspv tgo, ngTdjdpw 9, 1903, oxvo rqxsv ng kthtwxng xg Prxwmvistgo.Adw qxp hifuwnsnjx xovtp pwxss gndixpq. Cni Lvihlqncpp pndjqw tgrvipwn wqv uinasvzp wqidpw dung hifuwnsnjf af gvr hngoxwxngp. "Xw xpgvhvptif wn oxpwxgjdpxq htivcdssf avwrvvg t pfpwvz nc vghxuqvizvgwvgkxpxngvo cni t znzvgwtif vyhqtgfv nc svwwwip avwrvvg pvkvits xpnstwwouvnuvsg tgo t zvwqno nc hifuwnjituqf xgwwgovo wn jnkvig wqv hniivpungovghvavwrvvg oxccvivgw tizf hqxvcp cni tg dgsxzxwvo wxzv," qv rinwv. Xg wqtwngv pvgwvghv, Lvihlqncpp oxccvivgwxtwvp uiv-wvsvjituqf zxsxwtifhzzdgxhtwxngp cinz unpw-. Wqv pvgwvghv xp uivjgtw rxwq znpw nc wqvivbdxivzvgwp wqtw qtkv hnzv wn av ovztgovo nc pfpwvzp nc zxsxwtifhifuwnjituqf, ivbdxivzvgwp pdhq tp pxzusxhxf, ivsxtaxsxf, ituxoxwf, tgopn ng. Wqxp hsvti ivhnjgxwxng nc wqv gvr niovi hngpwxwdwvp Lvihlqncpp' cxipwjivtv hngwixadwxng wn hifuwnsnjf.Wqv pvhngo rtp wn ivtccxiz xg t znovig hngwvyw wqv uixghxusv wqtw ngsfhifuwtgtsfpwp htg lgnr wqv pvhdixwf nc t hxuqvi pfpwvz. Xw xp wqv cniz ncedojzvgw rqxhq xp pwxss dpvo.

V	W	T	X	N	P	G	I	Q	S	H	O	D	C	U	Z	F	J	R	A	L	K	E	Y	B	M
344	268	238	238	217	210	208	203	154	124	123	106	81	78	73	68	65	59	50	39	38	23	7	6	2	2
11.4	8.9	7.9	7.9	7.2	6.9	6.9	6.7	5.1	4.1	4.1	3.5	2.7	2.6	2.4	2.2	2.1	2.0	1.7	1.3	1.3	0.8	0.2	0.2	0.1	0.1

Figure 0: Tabel of frequency of th characters

XW RaP CIaGHe, QNReKeI, WQaW UDASXPQeO NGe NC HIFUWNSNJF'P JIeaWePWANNLP.
 Sa HIFUWNJiaUQXH ZXSXWaXie CXIPW aUUEaIeO aP WRN XGPWaSSZeGWP XGWQe ENDIGaS OeP PHXeGHeP
 ZXSXWaXieP XG EaGDaIF aGO CeAIdaIF NC 1883, AeXGJ IeXPPDeO SaWeI WQaW FeaI aP a UaUeIAaHL
 ANNl AF WQe ENDIGaS'PUDASXPQeI. XW XP WQe ZNPW HNGHXPe ANNl NG HIFUWNSNJF eKeI RIXWWeG.
 XWPaDWQNI QaO WQe XGPWXGHW CNI WQe HIFUWNJiaUQXH EDJDsaI, aGO Qe HNZUIePPeOXGWN 64 UaJeP
 KXIWDaSSf WQe eGWXie LGNRG CXeSO NC HIFUWNSNJF, XGHSDOXGJUNSFaSUQaAeWXHP RXWQ ZXYeO aSUQaAeWP,
 eGHXUQeIeO HNOe, aGO HXUQeIOeKXHeP. WQe ANNl XP aSPN NGe NC WQe ZNPW PHQNSaISf NG HIFUWNSNJF.
 XWPCNNWGNWeP HXWe ZNPW HSaPPXHaS aGO ZaGF ZNOeIG PNDIHeP; HNZZeGWP PDHQaP "WQXP XP GNW WQe NGSF
 QXPWNIXHaS NI AXASXNJiaUQXH eIINI CNI RQXHQ WQe aDPWIXaG RIXWeI ZDPW Ae IeUINaHQeO" PQNR QNR
 HaIeCDSSf WQe aDWQNI QaP PWDOXeO WQNPe PNDIHeP. XWP aDWQNI RaP ANIG
 EeaG-JDXSSaDZe-QDAeIW-KXHWNI-CIaGJNXp-aSeYaGOIe-aDJDPWe LeIHLQNCCP KNG GXeDReGQNC NG EaGDaIF 19,
 1835, aWGDWQ, QNSSaGO. aCWeI JeWwXGJ OeJieeP XG SeWWeIP aGO XG PHXeGHe CINZ WQeDGXKeIPXWF NC
 SXeJe, Qe RaP QXieO XG 1863 aP aG XGPWIDHWNI XG ZNOeIGSaGJDJeP aW WQe QXJQ PHQNNS aW ZeSDG, a
 SaIJe WNRG 25 ZXSeP PNDWQeaPWNC UaIXP. WQe GeYW FeaI Qe ZaIIXeO a JXIS CINZ WQe aIea aGO XG
 1865, RQeGQe RaP 30, WQeF QaO WQeXI NGSF HQXSO, a OaDJQWeI, UaDSXGe. Qe PWaFeO aWZeSDG CNI 10
 FeaIP, WeaHQXGJ eGSXPQ aGO JeIZaG.AF WQaW WXZe Qe QaO PQNIWeGeO QXP GaZe WN aDJDPWe LeIHLQNCCP.
 AeaIOeO, OXJGXCXeO, PSNR NC PUeeHQ, LeIHLQNCCP, OePUXWe aG XGaAXSXWF WNZaXGwaXG OXPHXUSXGe XG QXP
 HSaPPeP aGO PNZe eHHeGWIXHXWeP NC HQaIaHWeI, RaP a "SeaIGeO, MeaSNdp, HaUaASe" WeaHQeI RQN aRNLe
 QXP PWDOeGWP'XGWeIePW XG WQeXI RNIL; QXP PDUeIXNIP PaXO "QXP PWDOeGWP SXLe QXZ aGO RNILRXWQ
 PDHHePP." aCWeIRaIO, Qe RNILeO aP a UIXKaWe XGPWIDHWNI XG UaIXP.QXP ADPXePW FeaIP CNSSNReO WQe
 UDASXHaWXNG NC Sa HIFUWNJiaUQXH ZXSXWaXie. a GeR XGWeIGaWXNGaS SaGJDJe HaSSeO KNSa-UXXL
 ("RNISO-PUeaL") QaO Aeeg XGKeGWeO AF a JeIZaG UIXePW. aANDW 1885, XW HaDJQW NG XGCIaGHe aGO
 CSaPQeO RXWQ eYUIePP-WIaXG PUeeO aSS NKeI WQe HNDGWIF, GNWNGSF aZNGJ XGWeSSeHWDaSP ADW aZNGJ aSS
 HSaPPeP; XW RaP eKeG QeaIO XG WQePWIEeWP. CINZ CIaGHe XW IaOXaWeO WQINDJQNDW WQe RNISO. WQe ZNPW
 aHWXKeUINUaJaGOXPW NC KNSaUXXL RaP aDJDPWe LeIHLQNCCP, RQN, aW WQe PeHNGOKNSaUXXL HNGJiePP XG ZDGXHQ
 XG 1887, RaP aHHSaXZeO OXieHwNI ("OXSeLeS," XG KNSaUXXL) NC WQe XGWeIGaWXNGaS aHaOeZF NC KNSaUXXL.
 ADW aW WQe WQXIOHNGJiePP, QeSO aW UaIXP XG ZaF NC 1889, RXWQ LeIHLQNCCP UIePXOXGJ, HIXWXHaSWeGPXNGP
 RXWQXG WQe ZNKeZeGW ZNDGWeO aGO CXGaSSf AINLe XW aUaIW.LeIHLQNCCP RaP HIDPQeO AF WQe HNSSaUPe NC aG
 XGWeIGaWXNGaS OIeaZ WQaWQaO PeeZeO PN GeeOCDS aGO PN HeIWaXG. Qe HIeaWeO GNWQXGJ eSPe aGO, NGaDJDPW
 9, 1903, OXeO RQXSe NG KaHaWXNG XG PRXWMeISaGO.ADW QXP HIFUWNSNJXH XOeaP PWXSS GNDIXPQ. CNI
 LeIHLQNCCP PNDJQW aGPREIPWN WQe UINaSeZP WQIDPW DUNG HIFUWNSNJF AF GeR HNGOXWXNGP. "XW XPGeHePPaIF
 WN OXPWXGJDXPQ HaIeCDSSf AeWReeG a PFPWeZ NC eGHXUQeIZeGWeGKXPXNGeO CNI a ZNZeGwaIF eYHQaGJe NC
 SeWWeIP AeWReeG PeKeIaS XPNSaWeOUeNUSe aGO a ZeWQNO NC HIFUWNJiaUQF XGWeGOeO WN JNKeIG WQe
 HNIIPUNGoeGHeAeWReeG OXCCeIeGW aIZF HQXeCP CNI aG DGSXZXWeO WXZe," Qe RINWe. XG WQaWNGe PeGWeGHe,
 LeIHLQNCCP OXCCeIeGWXaWeP UIe-WeSeJiaUQF ZXSXWaIFHNZZDGXHaWXNGP CINZ UNPW-. WQe PeGWeGHe XP UIeJGaGW
 RXWQ ZNPW NC WQeIeBDXieZeGWP WQaW QaKe HNZe WN Ae OeZaGOeO NC PFPWeZP NC ZXSXWaIFHIFUWNJiaUQF,
 IeBDXieZeGWP PDHQ aP PXZUSHXWF, IeSXaAXSXWF, IaUXOXWF, aGOPN NG. WQXP HSeaI IeHNJGXWXNG NC WQe GeR
 NIOeI HNGPWWDWeP LeIHLQNCCP' CXIPWJieaW HNGWIXADWXNG WN HIFUWNSNJF.WQe PeHNGO RaP WN IeaCCXIZ XG a
 ZNOeIG HNGWeYW WQe UIXGHXUse WQaW NGSFHIFUWaGaSFPWP HaG LGNR WQe PeHDIXWF NC a HXUQeI PFPWeZ. XW XP
 WQe CNIZ NCEDOJZeGW RQXHQ XP PWXSS DPeO.

Figure 1: Replace V→e and T→a

‘e’ is the most frequent letter in English dictionary, so the replacements must be started with it

Xt RaP CIaGHe, hNReKeI, that UDASXPheO NGe NC HIFUtNSNJF'P JIeatePtANLp.
 Sa HIFUtNJiaUhXH ZXSXtaXie CXIPt aUueaIeO aP tRN XGPTaSSZeGtP XGthe ENDIGaS OeP PHXeGHeP
 ZXSXtaXieP XG EaGDaiF aGO CeAIDaIF NC 1883, AeXGJ IeXPPDeO SateI that FeaI aP a UaUeIAaHL
 ANNL AF the ENDIGaS'PUDASXPheI. Xt XP the ZNPt HNGHXPe ANNL NG HIFUtNSNJF eKeI RIXtteG.
 XtPaDthNI haO the XGPTXGHT CNI the HIFUtNJiaUhXH EDJDSaI, aGO he HNzUIePPeOXGtN 64 UaJeP
 KXItDaSSF the eGtXie LGNRG CXeSO NC HIFUtNSNJF, XGHSDOXGJUNSFaSUhaAetXHP RXth ZXYeO aSUhaAetP,
 eGHXUheIeO HNOe, aGO HXUheIOeKXHeP. the ANNL XP aSPN NGe NC the ZNPt PHhNSaISF NG HIFUtNSNJF.
 XtPCNNtGNteP HXte ZNPt HSaPPXHaS aGO ZaGF ZNOeIG PNDIHeP; HNZZeGtP PDHhaP "thXP XP Gnt the NGSF
 hXPtNIXHaS NI AXASXNJiaUhXH eIINI CNI RhXHh the aDptIXaG RIXteI ZDpt Ae IeUINaHheO"PhNR hNR
 HaIeCDSSF the aDthNI haP PtDOXeO thNPe PNDIHeP.XtP aDthNI RaP ANIG
 EeaG-JDXSSaDZe-hDAeIt-KXhtNI-CIaGJNXp-aSeYaGOIe-aDJDPte LeIHLhNCCP KNG GXeDReGhNC NG EaGDaiF 19,
 1835, atGDth, hNSSaGO. aCteI JettXGJ OeJieeP XG SetteIP aGO XG PHXeGHe CINZ theDGXKeIPXtF NC
 SXeJe, he RaP hXieO XG 1863 aP aG XGPTIDhtNI XG ZNOeIGSaGJDaJeP at the hXJh PHhNNS at ZeSDG, a
 SaIJe tNRG 25 ZXSeP PNDtheaPtNC UaIXP. the GeYt FeaI he ZaIIXeO a JXIS CINZ the aIea aGO XG
 1865, RheGhe RaP 30, theF haO theXI NGSF HhXSO, a OaDJhteI, UaDSXGe. he PtaFeO atZeSDG CNI 10
 FeaIP, teaHhXGJ eGSXPh aGO JeIZaG.AF that tXZe he haO PhNiteGeO hXP GaZe tN aDJDPte LeIHLhNCCP.
 AeaIOeO, OXJGXCXeO, PSNR NC PUeeHh, LeIHLhNCCP, OePUXte aG XGaAXSXtF tNZaXGtaXG OXPHXUSXGe XG hXP
 HSaPPeP aGO PNZe eHHeGtIXHtXeP NC HhaIaHteI, RaP a "SeaIGeO, MeaSNdp, HaUaASe" teaHheI RhN aRNLe
 hXP PtDOeGtP'XGteIePt XG theXI RNIL; hXP PDUeIXNIP PaXO "hXP PtDOeGtP SXLe hXZ aGO RNILRXth
 PDHHePP." aCteIRAIO, he RNILEO aP a UIXKate XGPTIDhtNI XG UaIXP.hXP ADPXePt FeaIP CNSSNReO the
 UDASXHatXNG NC Sa HIFUtNJiaUhXHZXSXtaXie. a GeR XGteIGatXNGaS SaGJDaJe HaSSeO KNSa-UXXL
 ("RNISO-PUeal")haO Aeeg XGKeGteO AF a JeIZaG UIXePt. aANDt 1885, Xt HaDJht NG XGCIaGHe aGO
 CSaPheO RXth eYUIePP-tIaXG PUeeO aSS NKeI the HNDGtIF, GntNGSF aZNGJ XGteSSeHtDaSP Adt aZNGJ aSS
 HSaPPeP; Xt RaP eKeG heaIO XG thePtIeetP. CINZ CIaGHe Xt IaOXateO thINDJhNDt the RNISO. the ZNPt
 aHTXKeUINUaJaGOXPt NC KNSaUXXL RaP aDJDPte LeIHLhNCCP, RhN, at the PeHNGOKNSaUXXL HNGJiePP XG ZDGXhH
 XG 1887, RaP aHHSaXZeO OXieHtNI ("OXSeLeS,"XG KNSaUXXL) NC the XGteIGatXNGaS aHaOeZF NC KNSaUXXL.
 Adt at the thXIOHNGJiePP, heSO at UaIXP XG ZaF NC 1889, RXth LeIHLhNCCP UIePXOXGJ, HIXtXHaSteGPXNGP
 RXthXG the ZNKeZeGt ZNDGteO aGO CXGaSSF AINLe Xt aUaIt.LeIHLhNCCP RaP HIDPheO AF the HNSSaUPe NC aG
 XGteIGatXNGaS OIeaZ thathaO PeeZeO PN GeeOCDS aGO PN HeItaXG. he HIeateO GNthXGJ eSPe aGO, NGaDJDPt
 9, 1903, OXeO RhXSe NG KaHatXNG XG PRXtMeISaGO.Adt hXP HIFUtNSNJXH XOeaP PtXSS GNDIXPh. CNI
 LeIHLhNCCP PNDJht aGPreIPtN the UINaSeZP thIDpt DUNG HIFUtNSNJF AF GeR HNGOXtXNGP. "Xt XPGeHePPaIF
 tN OXPtXGJDxPh HaIeCDSSF AetReeG a PFPteZ NC eGHXUheIZeGteGKXPXNGeO CNI a ZNZeGtaIF eYHhaGJe NC
 SetteIP AetReeG PeKeIaS XPNSateOUeNUSe aGO a ZethNO NC HIFUtNJiaUhF XGteGOeO tN JNKeIG the
 HNIIEPUNGOeGHeAetReeG OXCCeIeGt aIZF HhXeCP CNI aG DGsxZXteO tXZe," he RINte. XG thatNGe PeGteGHe,
 LeIHLhNCCP OXCCeIeGtXateP UIe-teSeJiaUhF ZXSXtaIFHNZZDGXHatXNGP CINZ UNPt-. the PeGteGHe XP UIeJGaGt
 RXth ZNPt NC theIeBDXieZeGtP that haKe HNZe tN Ae OeZaGOeO NC PFPteZP NC ZXSXtaIFHIFUtNJiaUhF,
 IeBDXieZeGtP PDHh aP PXZUSXHtF, IeSXaAXSXtF, IaUXOXtF, aGOPN NG. thXP HSeaI IeHNJGtXNG NC the GeR
 NIOeI HNGPtXtDteP LeIHLhNCCP' CXIPtJieat HNGtIXADtXNG tN HIFUtNSNJF.the PeHNGO RaP tN IeaCCXIZ XG a
 ZNOeIG HNGteYt the UIXGHXUSE that NGSFHIFutaGaSFtP HaG LGNR the PeHDIXtF NC a HXUheI PFPteZ. Xt XP
 the CNIZ NCEDOJZeGt RhXHh XP PtXSS DPeO.

Figure 2: Replace Q→h and W→t

Evident places where the word “the” can be, continuing replacement.


```

it RaP CIGHe, hoReKeI, that UDASiPheO oGe oC HIFutoSoJF'P JIeatePtAooLP.
Sa HIFutoJiaUhiH ZiSitaiIe CiIPt aUueaIeO aP tRo iGPTaSSZeGtP iGthe EoDIGaS OeP PHieGHeP
ZiSitaiIeP iG EaGDaiF aGO CeAIDaIF oC 1883,AeiGJ IeiPPDeO SateI that FeaI aP a UaUeIAaHL
AooL AF the EoDIGaS'PUDasIPheI. it iP the ZoPt HoGHiPe AooL oG HIFutoSoJF eKeI RIitteG.
itPaDthoI haO the iGPTiGht CoI the HIFutoJiaUhiH EDJDSaI, aGO he HoZUIePPEoiGto 64 UaJeP
KiItDaSSF the eGtiIe LGoRG CieSO oC HIFutoSoJF, iGHSDoiGJUoSFaSUhaAetiHP Rith ZiYeO aSUhaAetP,
eGHiUheIeO HoOe, aGO HiUheIOeKiHeP. the AooL iP aSPo oGe oC the ZoPt PHhoSaISF oG HIFutoSoJF.
itPCootGoteP Hite ZoPt HSApPiHaS aGO ZaGF ZoOeIG PoDIHeP; HoZZeGtP PDHhaP "thiP iP Got the oGSF
hiPtoIiHaS oI AiASioJiaUhiH eIIoI CoI RhiHh the aDPTiiaG RIiteI ZDPt Ae IeUIoaHheO"PhoR hoR
HaIeCDSSF the aDthoI haP PtDOieO thoPe PoDIHeP.itP aDthoI RaP AoIG
EeaG-JDiSSaDZe-hDAeIt-KiHtoI-CIaGJoiP-aSeYaGOIe-aDJDPte LeIHLhoCCP KoG GieDReGhoC oG EaGDaiF 19,
1835, atGDth, hoSSaGO. aCteI JettiGJ OeJieeP iG SetteIP aGO iG PHieGHe CIOZ theDGiKeIPitF oC
SieJe, he RaP hiIeO iG 1863 aP aG iGPTIDHtoI iG ZoOeIGSaGJDaJeP at the hiJh PHhooS at ZeSDG, a
SaIJe toRG 25 ZiSeP PoDtheaPtoC UaiiP. the GeYt FeaI he ZaIIieO a JiIS CIOZ the aIea aGO iG
1865, RheGhe RaP 30, theF haO theiI oGSF HhiSO, a OaDJhteI, UaDSiGe. he PtaFeO atZeSDG CoI 10
FeaIP, teaHhiGJ eGJSiPh aGO JeIZaG.AF that tiZe he haO PhoIteGeO hiP GaZe to aDJDPte LeIHLhoCCP.
AeaIOeO, OijGiCieO, PSOR oC PUeeHh, LeIHLhoCCP, OePUite aG iGaAiSitF toZaiGtaig OiPHiUSiGe iG hiP
HSAppeP aGO PoZe eHHeGtiIHitieP oC HhaIaHteI,RaP a "SeaIGeO, MeaSoDP, HaUaASe" teaHheI Rho aRole
hiP PtDOeGtP'igTeIePt iG theiI RoIL; hiP PDUeIioIP PaiO "hiP PtDOeGtP SiLe hiZ aGO RoILRith
PDHHePP." aCteIRAIO, he RoILEO aP a UIiKate iGPTIDHtoI iG UaiiP.hiP ADPiePt FeaIP CoSSoReO the
UDASiHatioG oC Sa HIFutoJiaUhiHziSitaiIe. a GeR iGteIGatioGaS SaGJDaJe HaSSeO KoSa-Uiil
("RoISO-PUeaL")haO Aeeg iGKeGteO AF a JeIZaG UIiePt. aAoDt 1885, it HaDJht oG iGCIaGHe aGO
CSaPheO Rith eYUIePP-tIaiG PUeeO aSS oKeI the HoDGtIF, GotoGSF aZoGJ iGteSSeHtDaSP Adt aZoGJ aSS
HSAppeP; it RaP eKeG heaIO iG thePtIeetP. CIOZ CIGHe it IaOiateO thIoDJhoDt the RoISO. the ZoPt
aHtiKeUIoUaJaGOiPt oC KoSaUiil RaP aDJDPte LeIHLhoCCP, Rho, at the PeHoGOKoSaUiil HoGJIePP iG ZDGihH
iG 1887, RaP aHHSaiZeO OiIeHtoI ("OiSeLeS,"iG KoSaUiil) oC the iGteIGatioGaS aHaOeZF oC KoSaUiil.
Adt at the thiIOHoGJIePP, heSO at UaiiP iG ZaF oC 1889, Rith LeIHLhoCCP UIePiOiGJ, HIitiHaSteGPioGP
RithiG the ZoKeZeGt ZoDGteO aGO CiGaSSF AIole it aUaIt.LeIHLhoCCP RaP HIDPheO AF the HoSSaUpe oC aG
iGteIGatioGaS OIeaZ thathaO PeeZeO Po GeeOCDS aGO Po HeItaiG. he HIeateO GothiGJ eSPe aGO, oGaDJDPt
9, 1903, OieO RhiSe oG KaHatioG iG PritMeISaGO.Adt hiP HIFutoSoJih ioeaP PtiSS GoDIiPh. CoI
LeIHLhoCCP PoDJht aGPreIPto the UIoASeZP thIDPt DUoG HIFutoSoJF AF GeR HoGOitioGP. "it iPGeHePPaIF
to OiPtIGJDIPh HaIeCDSSF AetReeG a PFPteZ oC eGHiUheIZeGteGKiPioGeO CoI a ZoZeGtaIF eYHhaGJe oC
SetteIP AetReeG PeKeIaS iPoSateOUeoUse aGO a ZethoO oC HIFutoJiaUhf iGteGOeO to JoKeIG the
HoIiePUoGOeGHeAetReeG OiCCeIeGt aIZF HhieCP CoI aG DGSiZiteO tiZe," he RIote. iG thatoGe PeGteGHe,
LeIHLhoCCP OiCCeIeGtiatP UIe-teSeJiaUhf ZiSitaIFHoZZDGiHatioGP CIOZ UoPt-. the PeGteGHe iP UIeJGaGt
Rith ZoPt oC theIeBDiIeZeGtP that haKe HoZe to Ae OeZaGOeO oC PFPteZP oC ZiSitaIFHIFutoJiaUhf,
IeBDiIeZeGtP PDHh aP PiZUSiHitF, IeSiaAiSitF, IaUiOitF, aGOPo oG. thiP HSeaI IeHoJGitioG oC the GeR
oIOeI HoGPtitDteP LeIHLhoCCP' CiIPtJieat HoGtiADtioG to HIFutoSoJF.the PeHoGO RaP to IeaCCiIZ iG a
ZoOeIG HoGteYt the UIiGHiUSE that oGSFHIFutaGaSFtpT HaG LGoR the PeHDIitF oC a HiUheI PFPteZ. it iP
the CoIZ oCEDOJZeGt RhiHh iP PtiSS DPeO.

```

Figure 3: Replace X→i and N→o

it Ras CIanHe, hoReKeI, that UDASisheO one oC HIFutoSoJF's JIeatestAooLs.
 Sa HIFutoJIAUhiH ZiSitaiIe CiIst aUueaIeO as tRo instaSSZents inthe EoDinaS Oes sHienHes
 ZiSitaiIes in EanDaIF anO CeAIDaIF oC 1883,AeinJ IeissDeO SateI that FeaI as a UaUeIAaHL
 AooL AF the EoDinaS'sUDASisheI. it is the Zost HonHise AooL on HIFutoSoJF eKeI RIitten.
 itsaDthoI haO the instinHt CoI the HIFutoJIAUhiH EDJDSaI, anO he HoZUIesseOinto 64 UaJes
 KiItDaSSF the entiIe LnoRn CieSO oC HIFutoSoJF, inHSDoinJUoSFaSUhaAetiHs Rith ZiYeO aSUhaAets,
 enHiUheIeO HoOe, anO HiUheIOeKiHes. the AooL is aSso one oC the Zost sHhoSaISF on HIFutoSoJF.
 itsCootnotes Hite Zost HSassiHaS anO ZanF ZoOeIn soDIHes; HoZZents sDHhas "this is not the onSF
 histoIiHaS oI AiASioJIAUhiH eIIoI CoI RhiHh the aDstIian RIiteI ZDst Ae IeUIoAHheO"shoR hoR
 HaIeCDSSF the aDthoI has stDOieO those soDIHes.its aDthoI Ras AoIn
 Eean-JDiSSaDZe-hDAeIt-KiHtoI-CIanJois-aSeYanOIe-aDJDste LeIHLhoCCs Kon nieDRenhoC on EanDaIF 19,
 1835, atnDth, hoSSanO. aCteI JettinJ OeJiees in SetteIs anO in sHienHe CIOZ theDniKeIsitF oC
 SieJe, he Ras hiIeO in 1863 as an instIDHtoI in ZoOeInSanJDaJes at the hiJh sHhooS at ZeSDn, a
 SaIJe toRn 25 ZiSes soDtheastoC UaIis. the neYt FeaI he ZaIIieO a JiIS CIOZ the aIea anO in
 1865, Rhenhe Ras 30, theF haO theiI onSF HhiSO, a OaDJhteI, UaDSine. he staFeO atZeSDn CoI 10
 FeaIs, teaHhinJ enJSish anO JeIZan.AF that tiZe he haO shoIteneO his naZe to aDJDste LeIHLhoCCs.
 AeaIOeO, OijniCieO, sSor oC sUeeHh, LeIHLhoCCs, OesUite an inaAiSitF toZaintain OisHiUSine in his
 HSasses anO soZe eHhentIiHities oC HhaIaHteI,Ras a "SeaIneO, MeaSoDs, HaUaASe" teaHheI Rho aRoLe
 his stDOents'intest in thei RoIL; his sDUeIioIs saiO "his stDOents SiLe hiZ anO RoILRith
 sDHHess." aCteIRAIO, he RoILEO as a UIIkeat instIDHtoI in UaIis.his ADsiest FeaIs CoSSoReO the
 UDASiHation oC Sa HIFutoJIAUhiHziSitaiIe. a neR inteInationaS SanJDaJe HaSSeO KoSa-Uiil
 ("RoISO-sUeaL")haO Aeen inKenteO AF a JeIZan UIiest. aAoDt 1885, it HaDJht on inCIanHe anO
 CSasheO Rith eYUIess-tIain sUeeO aSS oKeI the HoDntIF, notonSF aZonJ inteSSeHtDaSs ADt aZonJ aSS
 HSasses; it Ras eKen heaIO in thestIeets. CIOZ CIanHe it IaOiateO thIoDJhoDt the RoISO. the Zost
 aHtiKeUIoUaJanOist oC KoSaUiil Ras aDJDste LeIHLhoCCs, Rho, at the seHonOKoSaUiil HonJIess in ZDniHh
 in 1887, Ras aHHSaiZeO OiIeHtoI ("OiSeLeS,"in KoSaUiil) oC the inteInationaS aHaOeZF oC KoSaUiil.
 ADt at the thiIOHonJIess, heSO at UaIis in ZaF oC 1889, Rith LeIHLhoCCs UIesiOinJ, HIitiHaStensions
 Rithin the ZoKeZent ZoDnteO anO CinaSSF AIole it aUaIt.LeIHLhoCCs Ras HIDsheO AF the HoSSaUse oC an
 inteInationaS OIeaZ thathaO seeZeO so neeOCDS anO so HeItain. he HIeateO nothinJ eSse anO, onaDJDst
 9, 1903, OieO RhiSe on KaHation in sRitMeISanO.ADt his HIFutoSoJiH ioeas stiSS noDIish. CoI
 LeIHLhoCCs soDJht ansReIsto the UIoASeZs thIDst DUon HIFutoSoJF AF neR HonOitions. "it isneHessaIF
 to OistinJDish HaIeCDSSF AetReen a sFsteZ oC enHiUheIZentenKisioneO CoI a ZoZentaIF eYHhanJe oC
 SetteIs AetReen seKeIaS isoSateOUeoUse anO a ZethoO oC HIFutoJIAUhF intenOeO to JoKeIn the
 HoIIesUonOenHeAetReen OiCCeient aIZF HhieCs CoI an DnSiZiteO tiZe," he RIote. in thatone sentenHe,
 LeIHLhoCCs OiCCeientiates UIe-teSeJIAUhF ZiSitaIFHoZZDniHations CIOZ Uost-. the sentenHe is UIeJnant
 Rith Zost oC theIeBDiIeZents that haKe HoZe to Ae OeZanOeO oC sFsteZs oC ZiSitaIFHIFutoJIAUhF,
 IeBDiIeZents sDHH as siZUSiHitF, IeSiaAiSitF, IaUiOitF, anOso on. this HSeaI IeHoJnition oC the neR
 oIOeI HonstitDtes LeIHLhoCCs' CiIstJJeat HontIiADtion to HIFutoSoJF.the seHonO Ras to IeaCCiIZ in a
 ZoOeIn HonteYt the UIinHiUSE that onSFHIFUtanaSFsts Han LnoR the seHDIitF oC a HiUheI sFsteZ. it is
 the CoIZ oCEDOJZent RhiHh is stiSS DseO.

Figure 4: Replace P→s and G→n

it Ras CranHe, hoReKer, that UDAlisheO one oC HrFutoloJF's JreatestAooLs.
 la HrFutoJraUhiH Zilitaire Cirst aUueareO as tRo installZents inthe EoDrnal Oes sHienHes
 Zilitaires in EanDarF anO CeArDarF oC 1883,AeinJ reissDeO later that Fear as a UaUerAaHL
 AooL AF the EoDrnal'sUDAlisher. it is the Zost HonHise AooL on HrFutoloJF eKer Rritten.
 itsaDthor haO the instinHt Cor the HrFutoJraUhiH EDJDlar, anO he HoZUresseOinto 64 UaJes
 KirtDallF the entire LnoRn CieLO oC HrFutoloJF, inHLDoinJUolFalUhaAetiHs Rith ZiYeO alUhaAets,
 enHiUhereO HoOe, anO HiUherOeKiHes. the AooL is also one oC the Zost sHholarlF on HrFutoloJF.
 itsCootnotes Hite Zost HlassiHal anO ZanF ZoOern soDrHes; HoZZents sDHhas "this is not the onlF
 historiHal or AiAlioJraUhiH error Cor RhiHh the aDstriar Rriter ZDst Ae reUroaHheO"shoR hoR
 HareCDllF the aDthor has stDOieO those soDrHes.its aDthor Ras Aorn
 Eean-JDillaDZe-hDAert-KiHtor-CranJois-aleYanOre-aDDJste LerHLhoCCs Kon nieDRenhoC on EanDarF 19,
 1835, atnDth, hollanO. aCter JettinJ OeJrees in letters anO in sHienHe CroZ theDniKersitF oC
 lieJe, he Ras hireO in 1863 as an instrDHtor in ZoOernlanJDaJes at the hiJh sHhool at ZelDn, a
 larJe toRn 25 Ziles soDtheastoC Uaris. the neYt Fear he ZarrieO a Jirl CroZ the area anO in
 1865, Rhenhe Ras 30, theF haO their onlF Hhilo, a OaDJhter, UaDline. he staFeO atZelDn Cor 10
 Fears, teaHhinJ enJlish anO JerZan.AF that tiZe he haO shorteneO his naZe to aDDJste LerHLhoCCs.
 AearOeO, OiJniCieO, sloR oC sUeeHh, LerHLhoCCs, OesUite an inaAilitF toZaintain OisHiUline in his
 Hlasses anO soZe eHHentriHities oC HharaHter,Ras a "learneO, MealoDs, HaUaAle" teaHher Rho aRole
 his stDOents'interest in their RorL; his sDUeriors saiO "his stDOents liLe hiZ anO RorLRith
 sDHHess." aCterRarO, he RorLeO as a UriKate instrDHtor in Uaris.his ADSiest Fears ColloReO the
 UDAliaHation oC la HrFutoJraUhiHZilitaire. a neR international lanJDaJe HalleO Kola-Uiil
 ("RorLO-sUeaL")haO Aeen inKenteO AF a JerZan Uriest. aAoDt 1885, it HaDJht on inCranHe anO
 ClasheO Rith eYUress-train sUeeO all oKer the HoDntrF, notonlF aZonJ intelleHtDals ADt aZonJ all
 Hlasses; it Ras eKen hearO in thestreets. CroZ CranHe it raOiateO throDJhoDt the RorLO. the Zost
 aHTiKeUroUaJanOist oC KolaUiil Ras aDDJste LerHLhoCCs, Rho, at the seHonOKolaUiil HonJress in ZDniHh
 in 1887, Ras aHHLaiZeO OireHtor ("OileLel,"in KolaUiil) oC the international aHaOeZF oC KolaUiil.
 ADt at the thiroHonJress, helO at Uaris in ZaF oC 1889, Rith LerHLhoCCs UresiOinJ, HritiHaltensions
 Rithin the ZoKeZent ZoDnteO anO CinallF Arole it aUart.LerHLhoCCs Ras HrDsheO AF the HollaUse oC an
 international OreaZ thathaO seeZeO so neeOCDL anO so Hertain. he HreateO nothinJ else anO, onaDDJst
 9, 1903, OieO Rhile on KaHation in sRitMerlanO.ADt his HrFutoloJiH ioeas still noDrish. Cor
 LerHLhoCCs soDJht ansRersto the UroAleZs thrDst DUon HrFutoloJF AF neR HonOitions. "it isneHessarF
 to OistinJDish HareCDllF AetReen a sFsteZ oC enHiUherZentenKisioneO Cor a ZoZentarF eYHhanJe oC
 letters AetReen seKeral isolateOUeoUle anO a ZethoO oC HrFutoJraUhf intenOeO to JoKern the
 HorresUonOenHeAetReen OiCCerent arZF HhieCs Cor an DnliZiteO tiZe," he Rrote. in thatone sentenHe,
 LerHLhoCCs OiCCerentiates Ure-teleJraUhf ZilitarFHozZDniHations CroZ Uost-. the sentenHe is UreJnant
 Rith Zost oC thereBDireZents that haKe HoZe to Ae OeZanOeO oC sFsteZs oC ZilitarFHrFutoJraUhf,
 reBDireZents sDHH as siZULiHitF, reliaAilitF, raUiOitF, anOso on. this Hlear reHoJnition oC the neR
 orOer HonstitDtes LerHLhoCCs' CirstJreat HontriADtion to HrFutoloJF.the seHonO Ras to reaCCirZ in a
 ZoOern HonteYt the UrinHiUle that onlFHrFUTanalFsts Han LnoR the seHDritF oC a HiUher sFsteZ. it is
 the CorZ oCEDOJZent RhiHh is still DseO.

Figure 5: Replace I→r and S→l

it Ras Crance, hoReKer, that UDAlished one oC crFutoloJF's JreatestAooLs.
 la crFutoJraUhic Zilitaire Cirst aUueared as tRo installZents inthe EoDrnal des sciences
 Zilitaires in EanDarF and CeArDarF oC 1883,AeinJ reissDed later that Fear as a UaUerAacL
 AooL AF the EoDrnal'sUDAlisher. it is the Zost concise AooL on crFutoloJF eKer Rritten.
 itsaDthor had the instinct Cor the crFutoJraUhic EDJDlar, and he coZUressedinto 64 UaJes
 KirtDallF the entire LnoRn Cield oC crFutoloJF, inclDdinJUoIFaUhaAetics Rith ZiYed alUhaAets,
 enciUhered code, and ciUherdeKices. the AooL is also one oC the Zost scholarlF on crFutoloJF.
 itsCootnotes cite Zost classical and ZanF Zodern soDrces; coZZents sDchas "this is not the onlF
 historical or AiAlioJraUhic error Cor Rhich the aDstrian Rriter ZDst Ae reUroached"shoR hoR
 careCDllF the aDthor has stDdied those soDrces.its aDthor Ras Aorn
 Eean-JDillaDZe-hDAert-Kictor-CranJois-aleYandre-aDJDste LercLhoCCs Kon niedRenhoC on EanDarF 19,
 1835, atnDth, holland. aCter JettinJ deJrees in letters and in science CroZ theDniKersitF oC
 lieJe, he Ras hired in 1863 as an instrDctor in ZodernlanJDaJes at the hiJh school at ZelDn, a
 larJe toRn 25 Ziles soDtheastoC Uaris. the neYt Fear he Zarried a Jirl CroZ the area and in
 1865, Rhenhe Ras 30, theF had their onlF child, a daDJhter, UaDline. he stafed atZelDn Cor 10
 Fears, teachinJ enJlish and JerZan.AF that tiZe he had shortened his naZe to aDJDste LercLhoCCs.
 Aearded, diJniCied, sloR oC sUeech, LercLhoCCs, desUite an inaAilitF toZaintain disciUline in his
 classes and soZe eccentricities oC character,Ras a "learned, MealoDs, caUaAle" teacher Rho aRole
 his stDdents'interest in their RorL; his sDUeriors said "his stDdents lile hiZ and RorLRith
 sDccess." aCterRard, he RorLed as a UriKate instrDctor in Uaris.his ADsiest Fears ColloRed the
 UDAlication oC la crFutoJraUhicZilitaire. a neR international lanJDaJe called Kola-Uiil
 ("RorlD-sUeaL")had Aeen inKented AF a JerZan Uriest. aAoDt 1885, it caDJht on inCrance and
 Clashed Rith eYUress-train sUeed all oKer the coDntrF, notonlF aZonJ intellectDals ADt aZonJ all
 classes; it Ras eKen heard in thestreets. CroZ Crance it radiated throDJhoDt the RorlD. the Zost
 actiKeUroUaJandist oC KolaUiil Ras aDJDste LercLhoCCs, Rho, at the secondKolaUiil conJress in ZDnich
 in 1887, Ras acclaiZed director ("dileLel,"in KolaUiil) oC the international acadeZF oC KolaUiil.
 ADt at the thirdconJress, held at Uaris in ZaF oC 1889, Rith LercLhoCCs UresidinJ, criticaltensions
 Rithin the ZoKeZent ZoDnted and CinallF Arole it aUart.LercLhoCCs Ras crDshed AF the collaUse oC an
 international dreaZ thathad seeZed so needCDL and so certain. he created nothinJ else and, onaDJDst
 9, 1903, died Rhile on Kacation in sRitMerland.ADt his crFutoloJic ideas still noDrish. Cor
 LercLhoCCs soDJht ansRersto the UroAleZs thrDst DUon crFutoloJF AF neR conditions. "it isnecessarF
 to distinJDish careCDllF AetReen a sFsteZ oC enciUherZentenKisioned Cor a ZoZentarF eYchanJe oC
 letters AetReen seKeral isolatedUeoUle and a Zethod oC crFutoJraUhF intended to JoKern the
 corresUondenceAetReen diCCerent arZF chieCs Cor an DnliZited tiZe," he Rrote. in thatone sentence,
 LercLhoCCs diCCerentiates Ure-teleJraUhF ZilitarFcoZZDnications CroZ Uost-. the sentence is UreJnant
 Rith Zost oC thereBDireZents that haKe coZe to Ae deZanded oC sFsteZs oC ZilitarFcrFutoJraUhF,
 reBDireZents sDch as siZulicitF, reliaAilitF, raUiditF, andso on. this clear recoJnition oC the neR
 order constitDtes LercLhoCCs' CirstJreat contriADtion to crFutoloJF.the second Ras to reaCCirZ in a
 Zodern conteYt the UrinciUle that onlFcrFUTanalFsts can LnoR the secDritF oC a ciUher sFsteZ. it is
 the CorZ oCEDdJZent Rhich is still Dsed.

Figure 6: Replace H→c and O→d

it Ras France, hoReKer, that UuAlished one of crFUtoloJF's JreatestAooLs.
 la crFutoJraUhic Zilitaire first aUueared as tRo installZents inthe Eournal des sciences
 Zilitaires in EanuarF and feAruarF of 1883, AeinJ reissued later that Fear as a UaUerAacL
 AooL AF the Eournal'sUuAlisher. it is the Zost concise AooL on crFUtoloJF eKer Rritten.
 itsauthor had the instinct for the crFutoJraUhic EuJular, and he coZUressedinto 64 UaJes
 KirtuallF the entire LnoRn field of crFUtoloJF, includinJUoLFaLUhaAetics Rith ZiYed alUhaAets,
 enciUhered code, and ciUherdeKices. the AooL is also one of the Zost scholarlF on crFUtoloJF.
 itsfootnotes cite Zost classical and ZanF Zodern sources; coZZents suchas "this is not the onlF
 historical or AiAlioJraUhic error for Rhich the austrian Rriter Zust Ae reUroached" shoR hoR
 carefullF the author has studied those sources.its author Ras Aorn
 Eean-JuillauZe-huAert-Kictor-franJois-aleYandre-auJuste LerclHoffs Kon nieuRenhof on EanuarF 19,
 1835, atnuth, holland. after JettinJ deJrees in letters and in science froZ theunikersitF of
 lieJe, he Ras hired in 1863 as an instructor in ZodernlanJuaJes at the hiJh school at Zelun, a
 larJe toRn 25 Ziles southeastof Uaris. the neYt Fear he Zarried a Jirl froZ the area and in
 1865, Rhenhe Ras 30, theF had their onlF child, a dauJhter, Uauline. he stafed atZelun for 10
 Fears, teachinJ enJlish and JerZan.AF that tiZe he had shortened his naZe to auJuste LerclHoffs.
 Aearded, diJnified, sloR of sUeech, LerclHoffs, desUite an inaAilitF toZaintain disciUline in his
 classes and soZe eccentricities of character, Ras a "learned, Mealous, caUaAle" teacher Rho aRoLe
 his students' interest in their RorL; his suUeriors said "his students liLe hiZ and RorLRith
 success." afterRard, he RorLed as a UriKate instructor in Uaris. his Ausiest Fears folloRed the
 UuAlication of la crFutoJraUhicZilitaire. a neR international lanJuaJe called Kola-Uiil
 ("Rorld-sUeaL") had Aeen inKented AF a JerZan Uriest. aAout 1885, it cauJht on infrance and
 flashed Rith eYUress-train sUeed all oKer the countrF, notonlF aZonJ intellectuals Aut aZonJ all
 classes; it Ras eKen heard in thestreets. froZ France it radiated throuJhout the Rorld. the Zost
 actiKeUroUaJandist of KolaUiil Ras auJuste LerclHoffs, Rho, at the secondKolaUiil conJress in Zunich
 in 1887, Ras acclaiZed director ("dileLeL," in KolaUiil) of the international acadeZF of KolaUiil.
 Aut at the thirdconJress, held at Uaris in ZaF of 1889, Rith LerclHoffs UresidinJ, criticaltensions
 Rithin the ZoKeZent Zounted and finallF AroLe it aUart. LerclHoffs Ras crushed AF the collaUse of an
 international dreaZ that had seeZed so needful and so certain. he created nothinJ else and, onauJust
 9, 1903, died Rhile on Kacation in sRitMerland. Aut his crFUtoloJic ideas still nourish. for
 LerclHoffs souJht ansRersto the UroAleZs thrust uVon crFUtoloJF AF neR conditions. "it is necessarF
 to distinJuish carefullF AetReen a sFsteZ of enciUherZentenKisioned for a ZoZentarF eYchanJe of
 letters AetReen seKeral isolatedUeoUle and a Zethod of crFutoJraUhf intended to JoKern the
 corresUondenceAetReen different arZF chiefs for an unliZited tiZe," he Rrote. in thatone sentence,
 LerclHoffs differentiates Ure-teleJraUhf ZilitarFcoZZunications froZ Uost-. the sentence is UreJnant
 Rith Zost of thereBuireZents that haKe coZe to Ae deZanded of sFsteZs of ZilitarFcrFutoJraUhf,
 reBuireZents such as siZUlicitF, reliaAilitF, raUiditF, andso on. this clear recoJnition of the neR
 order constitutes LerclHoffs' firstJreat contriAution to crFUtoloJF. the second Ras to reaffirZ in a
 Zodern conteYt the UrinciUle that onlFcrFUtanalFsts can LnoR the securitF of a ciUher sFsteZ. it is
 the forZ of EudJJent Rhich is still used.

Figure 7: Replace D→u and C→f

it was France, however, that published one of CrFptoloJF's GreatestAools.
 la crFptoJraphic militaire first appeared as two installments in the Journal des sciences
 militaires in January and February of 1883, and was reissued later that year as a paperAool
 Aool AF the Journal's publisher. it is the most concise Aool on crFptoloJF ever written.
 its author had the instinct for the crFptoJraphic EuJular, and he compressed into 64 pages
 virtually the entire known field of crFptoloJF, including polyalphabetic cipher alphabets,
 enciphered code, and cipher tricks. the Aool is also one of the most scholarly on crFptoloJF.
 its footnotes cite most classical and many modern sources; comments such as "this is not the only
 historical or alphabetical error for which the Austrian writer must be reproached" show how
 carefully the author has studied those sources. its author was Jean
 Eean-Juillaume-henri-Kector-françois-alexandre-auguste Lerchhoffs von neuRenhof on January 19,
 1835, in Utrecht, Holland. after getting degrees in letters and in science from the University of
 Leiden, he was hired in 1863 as an instructor in modern languages at the high school at Melun, a
 large town 25 miles southeast of Paris. there he married a girl from the area and in
 1865, when he was 30, they had their only child, a daughter, Pauline. he stayed at Melun for 10
 years, teaching English and German. AF that time he had shortened his name to Auguste Lerchhoffs.
 As a result, diminished, slow of speech, Lerchhoffs, despite an inability to maintain discipline in his
 classes and some eccentricities of character, was a "learned, jealous, capable" teacher who aroused
 his students' interest in their work; his superiors said "his students like him and work with
 success." afterward, he worked as a private instructor in Paris. his Ausiest years followed the
 publication of la crFptoJraphic militaire. a new international language called Kola-piil
 ("World-speak") had been invented by a German priest. about 1885, it caught on in France and
 spread with express-train speed all over the country, not only among intellectuals but among all
 classes; it was even heard in the streets. from France it radiated throughout the world. the most
 active propagandist of Kola-piil was Auguste Lerchhoffs, who, at the second Kola-piil congress in Munich
 in 1887, was acclaimed director ("director," in Kola-piil) of the international academy of Kola-piil.
 But at the third congress, held at Paris in May of 1889, with Lerchhoffs presiding, critical tensions
 within the movement mounted and finally broke it apart. Lerchhoffs was crushed by the collapse of an
 international dream that had seemed so needful and so certain. he created nothing else and, on August
 9, 1903, died while on vacation in Switzerland. But his crFptoloJic ideas still flourish. for
 Lerchhoffs sought answers to the problems thrust upon crFptoloJF by new conditions. "it is necessary
 to distinguish carefully between a system of encipherment intended for a momentary exchange of
 letters between isolated people and a method of crFptoJraphy intended to govern the
 correspondence between different army chiefs for an unlimited time," he wrote. in that one sentence,
 Lerchhoffs differentiates pre-teleJraphy military communications from post-. the sentence is pregnant
 with most of the requirements that have come to be demanded of systems of military crFptoJraphy,
 requirements such as simplicity, reliability, rapidity, and so on. this clear recognition of the new
 order constitutes Lerchhoffs' first great contribution to crFptoloJF. the second was to reaffirm in a
 modern context the principle that only crFptanalytists can know the security of a cipher system. it is
 the form of judgment which is still used.

Figure 8: Replace U→p and Z→m

it was France, however, that published one of cryptology's greatest works.
 The cryptographic *militaire* first appeared as two installments in the *Journal des sciences militaires* in January and February of 1883, being reissued later that year as a paperback by the Journal's publisher. It is the most concise work on cryptology ever written. Its author had the instinct for the cryptographic equivalent, and he compressed into 64 pages virtually the entire known field of cryptology, including polyalphabetic cipher, enciphered code, and cipher machines. The work is also one of the most scholarly on cryptology. Its footnotes cite most classical and many modern sources; comments such as "this is not the only historical or bibliographic error for which the Austrian writer must be reproached" show how carefully the author has studied those sources. Its author was Auguste Kerckhoffs.
 Jean-Guillaume-Henri-Klément-François-Alexandre-Auguste Kerckhoffs was born on January 19, 1835, in Brussels, Belgium. After getting degrees in letters and in science from the University of Liège, he was hired in 1863 as an instructor in modern languages at the high school at Melun, a large town 25 miles southeast of Paris. The next year he married a girl from the area and in 1865, when he was 30, they had their only child, a daughter, Pauline. He stayed at Melun for 10 years, teaching English and German. At that time he had shortened his name to Auguste Kerckhoffs. A reserved, dignified, slow of speech, Kerckhoffs, despite an inability to maintain discipline in his classes and some eccentricities of character, was a "learned, jealous, capable" teacher who aroused his students' interest in their work; his superiors said "his students like him and work with success." Afterward, he worked as a private instructor in Paris. His busiest years followed the publication of *La cryptographie militaire*, a new international language called *Kolapil* ("World-speak") had been invented by a German priest. About 1885, it caught on in France and flashed with express-train speed all over the country, not only among intellectuals but among all classes; it was even heard in the streets. From France it radiated throughout the world. The most active propagandist of *Kolapil* was Auguste Kerckhoffs, who, at the second *Kolapil* congress in Munich in 1887, was acclaimed director ("director," in *Kolapil*) of the international academy of *Kolapil*. But at the third congress, held at Paris in May of 1889, with Kerckhoffs presiding, critical tensions within the movement mounted and finally broke it apart. Kerckhoffs was crushed by the collapse of an international dream that had seemed so needful and so certain. He created nothing else and, on August 9, 1903, died while on vacation in Switzerland. But his cryptologic ideas still flourish. For Kerckhoffs sought answer to the problems thrust upon cryptology by new conditions. "It is necessary to distinguish carefully between a system of encipherment intended for a momentary exchange of letters between isolated people and a method of cryptography intended to govern the correspondence between different army chiefs for an unlimited time," he wrote. In that one sentence, Kerckhoffs differentiates pre-telegraphy military communications from post-. The sentence is pregnant with most of the requirements that have come to be demanded of systems of military cryptography, requirements such as simplicity, reliability, rapidity, and so on. This clear recognition of the new order constitutes Kerckhoffs' first great contribution to cryptology. The second was to reaffirm in a modern context the principle that only cryptanalysts can know the security of a cipher system. It is the form of judgment which is still used.

Figure 9: Replace F→y and J→g

it was France, however, that published one of cryptology's greatest books. The cryptographic *militaire* first appeared as two installments in the *Journal des sciences militaires* in January and February of 1883, being reissued later that year as a paperback book by the Journal's publisher. It is the most concise book on cryptology ever written. Its author had the instinct for the cryptographic *jugular*, and he compressed into 64 pages virtually the entire known field of cryptology, including polyalphabetic systems, enciphered code, and cipher devices. The book is also one of the most scholarly on cryptology. Its footnotes cite most classical and many modern sources; comments such as "this is not the only historical or bibliographic error for which the Austrian writer must be reproached" show how carefully the author has studied those sources. Its author was born Jean-guillaume-hubert-ictor-françois-alexandre-auguste Lerchhoffs Konnewenhuysen on January 19, 1835, in Antwerp, Belgium. After getting degrees in letters and in science from the University of Liege, he was hired in 1863 as an instructor in modern languages at the high school in Melun, a large town 25 miles southeast of Paris. The next year he married a girl from the area and in 1865, when he was 30, they had their only child, a daughter, Pauline. He stayed in Melun for 10 years, teaching English and German. By that time he had shortened his name to Auguste Lerchhoffs. Bearded, dignified, slow of speech, Lerchhoffs, despite an inability to maintain discipline in his classes and some eccentricities of character, was a "learned, jealous, capable" teacher who aroused his students' interest in their work; his superiors said "his students like him and work with success." Afterward, he worked as a private instructor in Paris. His busiest years followed the publication of *la cryptographie militaire*. A new international language called *Kolapil* ("world-speak") had been invented by a German priest. About 1885, it caught on in France and flashed with express-train speed all over the country, not only among intellectuals but among all classes; it was even heard in the streets. From France it radiated throughout the world. The most active propagandist of *Kolapil* was Auguste Lerchhoffs, who, at the second *Kolapil* congress in Munich in 1887, was acclaimed director ("directeur," in *Kolapil*) of the international academy of *Kolapil*. But at the third congress, held in Paris in May of 1889, with Lerchhoffs presiding, critical tensions within the movement mounted and finally broke it apart. Lerchhoffs was crushed by the collapse of an international dream that had seemed so needful and so certain. He created nothing else and, on August 9, 1903, died while on vacation in Switzerland. But his cryptologic ideas still flourish. For Lerchhoffs sought answers to the problems thrust upon cryptology by new conditions. "It is necessary to distinguish carefully between a system of encipherment intended for a momentary exchange of letters between isolated people and a method of cryptography intended to govern the correspondence between different army chiefs for an unlimited time," he wrote. In that one sentence, Lerchhoffs differentiates pre-telegraphy military communications from post-. The sentence is pregnant with most of the requirements that have come to be demanded of systems of military cryptography, requirements such as simplicity, reliability, rapidity, and so on. This clear recognition of the new order constitutes Lerchhoffs' first great contribution to cryptology. The second was to reaffirm in a modern context the principle that only cryptanalysts can know the security of a cipher system. It is the form of judgment which is still used.

Figure 10: Replace R→w and A→b

it was France, however, that published one of cryptology's greatest books. *La cryptographie militaire* first appeared as two installments in the *Journal des sciences militaires* in January and February of 1883, being reissued later that year as a paperback book by the Journal's publisher. It is the most concise book on cryptology ever written. Its author had the instinct for the cryptographic Euler, and he compressed into 64 pages virtually the entire known field of cryptology, including polyalphabetic with mixed alphabets, enciphered code, and cipher devices. The book is also one of the most scholarly on cryptology. Its footnotes cite most classical and many modern sources; comments such as "this is not the only historical or bibliographic error for which the Austrian writer must be reproached" show how carefully the author has studied those sources. Its author was born Jean-guillaume-hubert-victor-françois-alexandre-auguste Kerckhoffs von Nieuwenhof on January 19, 1835, at Nuth, Holland. After getting degrees in letters and in science from the University of Liège, he was hired in 1863 as an instructor in modern languages at the high school at Melun, a large town 25 miles southeast of Paris. The next year he married a girl from the area and in 1865, when he was 30, they had their only child, a daughter, Pauline. He stayed at Melun for 10 years, teaching English and German. By that time he had shortened his name to Auguste Kerckhoffs. Bearded, dignified, slow of speech, Kerckhoffs, despite an inability to maintain discipline in his classes and some eccentricities of character, was a "learned, jealous, capable" teacher who awoke his students' interest in their work; his superiors said "his students like him and work with success." Afterward, he worked as a private instructor in Paris. His busiest years followed the publication of *La cryptographie militaire*. A new international language called *Volapük* ("world-speak") had been invented by a German priest. About 1885, it caught on in France and flashed with express-train speed all over the country, not only among intellectuals but among all classes; it was even heard in the streets. From France it radiated throughout the world. The most active propagandist of *Volapük* was Auguste Kerckhoffs, who, at the second *Volapük* congress in Munich in 1887, was acclaimed director ("dilekel," in *Volapük*) of the International Academy of *Volapük*. But at the third congress, held at Paris in May of 1889, with Kerckhoffs presiding, critical tensions within the movement mounted and finally broke it apart. Kerckhoffs was crushed by the collapse of an international dream that had seemed so needful and so certain. He created nothing else and, on August 9, 1903, died while on vacation in Switzerland. But his cryptologic ideas still flourish. For Kerckhoffs sought answers to the problems thrust upon cryptology by new conditions. "It is necessary to distinguish carefully between a system of encipherment envisioned for a momentary exchange of letters between several isolated people and a method of cryptography intended to govern the correspondence between different army chiefs for an unlimited time," he wrote. In that one sentence, Kerckhoffs differentiates pre-telegraphy military communications from post-. The sentence is pregnant with most of the requirements that have come to be demanded of systems of military cryptography, requirements such as simplicity, reliability, rapidity, and so on. This clear recognition of the new order constitutes Kerckhoffs' first great contribution to cryptology. The second was to reaffirm in a modern context the principle that only cryptanalysts can know the security of a cipher system. It is the form of judgment which is still used.

Figure 11: Replace L→k and K→v

it was france, however, that published one of cryptology's greatest books. la cryptographic militaire first appeared as two installments in the journal des sciences militaires in january and february of 1883, being reissued later that year as a paperback book by the journal's publisher. it is the most concise book on cryptology ever written. its author had the instinct for the cryptographic jugular, and he compressed into 64 pages virtually the entire known field of cryptology, including polyalphabetic with mixed alphabets, enciphered code, and cipher devices. the book is also one of the most scholarly on cryptology. its footnotes cite most classical and many modern sources; comments such as "this is not the only historical or bibliographic error for which the austrian writer must be reproached" show how carefully the author has studied those sources. its author was born

jean-guillaume-hubert-victor-françois-alexandre-auguste kerckhoffs von nieuwenhof on january 19, 1835, at nuth, holland. after getting degrees in letters and in science from the university of liege, he was hired in 1863 as an instructor in modern languages at the high school at melun, a large town 25 miles southeast of paris. the next year he married a girl from the area and in 1865, when he was 30, they had their only child, a daughter, pauline. he stayed at melun for 10 years, teaching english and german. by that time he had shortened his name to auguste kerckhoffs. bearded, dignified, slow of speech, kerckhoffs, despite an inability to maintain discipline in his classes and some eccentricities of character, was a "learned, jealous, capable" teacher who awoke his students' interest in their work; his superiors said "his students like him and work with success." afterward, he worked as a private instructor in paris. his busiest years followed the publication of la cryptographic militaire. a new international language called volapik ("world-speak") had been invented by a german priest. about 1885, it caught on in france and flashed with express-train speed all over the country, not only among intellectuals but among all classes; it was even heard in the streets. from france it radiated throughout the world. the most active propagandist of volapik was auguste kerckhoffs, who, at the second volapik congress in munich in 1887, was acclaimed director ("dilekel," in volapik) of the international academy of volapik. but at the third congress, held at paris in may of 1889, with kerckhoffs presiding, critical tensions within the movement mounted and finally broke it apart. kerckhoffs was crushed by the collapse of an international dream that had seemed so needful and so certain. he created nothing else and, on august 9, 1903, died while on vacation in switzerland. but his cryptologic ideas still nourish. for kerckhoffs sought answers to the problems thrust upon cryptology by new conditions. "it is necessary to distinguish carefully between a system of encipherment envisioned for a momentary exchange of letters between several isolated people and a method of cryptography intended to govern the correspondence between different army chiefs for an unlimited time," he wrote. in that one sentence, kerckhoffs differentiates pre-telegraphy military communications from post-. the sentence is pregnant with most of the requirements that have come to be demanded of systems of military cryptography, requirements such as simplicity, reliability, rapidity, and so on. this clear recognition of the new order constitutes kerckhoffs' first great contribution to cryptology. the second was to reaffirm in a modern context the principle that only cryptanalysts can know the security of a cipher system. it is the form of judgment which is still used.

Figure 12: Replace E→j and X→y

it was france, however, that published one of cryptology's greatest books. la cryptographic militaire first appeared as two installments in the journal des sciences militaires in january and february of 1883, being reissued later that year as a paperback book by the journal's publisher. it is the most concise book on cryptology ever written. its author had the instinct for the cryptographic jugular, and he compressed into 64 pages virtually the entire known field of cryptology, including polyalphabetic with mixed alphabets, enciphered code, and cipher devices. the book is also one of the most scholarly on cryptology. its footnotes cite most classical and many modern sources; comments such as "this is not the only historical or bibliographic error for which the austrian writer must be reproached" show how carefully the author has studied those sources. its author was born jean-guillaume-hubert-victor-françois-alexandre-auguste kerckhoffs von nieuwenhof on january 19, 1835, at nuth, holland. after getting degrees in letters and in science from the university of liege, he was hired in 1863 as an instructor in modern languages at the high school at melun, a large town 25 miles southeast of paris. the next year he married a girl from the area and in 1865, when he was 30, they had their only child, a daughter, pauline. he stayed at melun for 10 years, teaching english and german. by that time he had shortened his name to auguste kerckhoffs. bearded, dignified, slow of speech, kerckhoffs, despite an inability to maintain discipline in his classes and some eccentricities of character, was a "learned, zealous, capable" teacher who awoke his students' interest in their work; his superiors said "his students like him and work with success." afterward, he worked as a private instructor in paris. his busiest years followed the publication of la cryptographic militaire. a new international language called volapik ("world-speak") had been invented by a german priest. about 1885, it caught on in france and flashed with express-train speed all over the country, not only among intellectuals but among all classes; it was even heard in the streets. from france it radiated throughout the world. the most active propagandist of volapik was auguste kerckhoffs, who, at the second volapik congress in munich in 1887, was acclaimed director ("dilekel," in volapik) of the international academy of volapik. but at the third congress, held at paris in may of 1889, with kerckhoffs presiding, critical tensions within the movement mounted and finally broke it apart. kerckhoffs was crushed by the collapse of an international dream that had seemed so needful and so certain. he created nothing else and, on august 9, 1903, died while on vacation in switzerland. but his cryptologic ideas still nourish. for kerckhoffs sought answers to the problems thrust upon cryptology by new conditions. "it is necessary to distinguish carefully between a system of encipherment envisioned for a momentary exchange of letters between several isolated people and a method of cryptography intended to govern the correspondence between different army chiefs for an unlimited time," he wrote. in that one sentence, kerckhoffs differentiates pre-telegraphy military communications from post-. the sentence is pregnant with most of the requirements that have come to be demanded of systems of military cryptography, requirements such as simplicity, reliability, rapidity, and so on. this clear recognition of the new order constitutes kerckhoffs' first great contribution to cryptology. the second was to reaffirm in a modern context the principle that only cryptanalysts can know the security of a cipher system. it is the form of judgment which is still used.

Figure 13: Replace B→q and M→z (final result)

V → e	C → f
T → a	U → p
Q → h	Z → m
W → t	F → y
X → i	J → g
N → o	R → w
P → s	A → b
G → n	L → k
I → r	K → v
S → l	E → j
H → c	y → x
O → d	B → q
D → u	M → z

Figure 14: Final decryption table

Conclusion:

At this laboratory work I studied how monoalphabetic decryption works and how to transform letter by letter the text to readable form. As I noticed, it was easier to find 'a', because it is the only letter that is single in the article. Then 'e', as it is the most common letter in the text and alphabet frequency. I also found the 't' and 'h'. After that, I had to pass every letter and see whether it fits in the text.