MINISTRY OF EDUCATION, CULTURE AND RESEARCH OF THE REPUBLIC OF MOLDOVA

Technical University of Moldova Faculty of Computers, Informatics and Microelectronics Department of Software and Automation Engineering

Miricinschi Gabriel FAF-233

Report

Laboratory work №2

of Cryptography

Checked by:
Maia Zaica, *university assistant*
FCIM, UTM

Chișinău – 2025

Purpose of Laboratory Work

The purpose of this work is to study the frequency analysis method, applying it to decode an intercepted text.

Conditions of the Problem

1. An encrypted message has been intercepted, which is known to have been obtained using a monoalphabetic cipher. Apply the frequency analysis attack to find the original message, assuming that it is a text written in English. Keep in mind that only letters have been encrypted, while other characters remain unencrypted. The report will contain a description of the cracking process, exactly as presented in section 2.3 in Example of attack through frequency analysis. Each student will take the variant according to their order number in the group list.

Technical Implementation

Letter	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
Count	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
Percentage (%)	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

Table 1: Letter frequency for intercepted message.

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

Table 2: English letter frequency.

V→E, W→T, T→A, as they are the most common:

Xt RaP CIaGHe, QNReKeI, tQat UDASXPQeO NGe NC HIFUtNSNJF'P JIeateP-tANNLP. Sa HIFUtNJIaUQXH ZXSXtaXIe CXIPt aUUeaIeO aP tRN XGPtaSSZeGtP XGtQe ENDIGaS OeP PHXeGHeP ZXSXtaXIeP XG EaGDaIF ***aGO*** CeAIDaIF NC 1883,AeXGJ IeXPPDeO SateI tQat FeaI aP a UaUeIAaHL ANNL AF tQe ENDI-GaS'PUDASXPQeI. Xt XP ***tQe*** ZNPt HNGHXPe ANNL NG HIFUtNSNJF eKeI RIXtteG. XtPaDtQNI QaO tQe XGPtXGHt CNI t***Qe*** HIFUtNJIaUQXH EDJDSaI, aGO Qe HNZUIePPeOXGtN 64 UaJeP KXItDaSSF tQe eGtXIe LGNRG CXeSO

NC HIFUtNSNJF, XGHSDOXGJUNSFaSUQaAetXHP RXtQ ZXYeO aSUQaAetP, eGHXUQeIeO HNOe, ***aGO*** HXUQeIOeKXHeP. tQe ANNL XP aSPN NGe NC tQe ZNPt PHQNSaISF NG HIFUtNSNJF. XtPCNNtGNteP HXte ZNPt HSaPPXHaS aGO ZaGF ZNOeIG PNDIHeP; HNZZeGtP PDHQaP "tQXP XP GNt tQe NGSF QXPtNIXHaS NI AXASXNJIaUQXH eIINI CNI RQXHQ tQe aDPtIXaG RIXteI ZDPt Ae IeUINaHQeO"PQNR QNR HaIeCDSSF tQe aDtQNI QaP PtDOXeO tQNPe PNDIHeP.XtP aDtQNI RaP ANIG EeaG-JDXSSaDZe-QDAeItKXHtNICIaGJNXP-aSeYaGOIe-aDJDPte LeIHLQNCCP KNG GXeDReGQNC NG EaGDaIF 19, 1835, atGDtQ, QNSSaGO. aCteI JettXGJ OeJIeeP XG SetteIP aGO XG PHXeGHe CINZ tQeDGXKeIPXtF NC SXeJe, Qe RaP QXIeO XG 1863 aP aG XGPtIDHtNI XG ZNOeIGSaGJDaJeP at tQe QXJQ PHQNNS at ZeSDG, a SaIJe tNRG 25 ZXSeP PNDtQeaPtNC UaIXP. tQe GeYt FeaI Qe ZaIIXeO a JXIS CINZ tQe aIea aGO XG 1865, RQeGQe RaP 30, tQeF QaO tQeXI NGSF HQXSO, a OaDJQteI, UaDSXGe. Qe PtaFeO atZeSDG CNI 10 FeaIP, teaHQXGJ eGJSXPQ aGO JeIZaG.AF tQat tXZe Qe QaO PQNIteGeO QXP GaZe tN aDJDPte LeIHLQNCCP.AeaIOeO, OXJGXCXeO, PSNR NC PUeeHQ, LeIHLQNCCP, OePUXte aG XGaAXSXtF tNZaXGtaXG OXPHXUSXGe XG QXP HSaPPeP aGO PNZe eHHeGtIXHXtXeP NC HQaIaHteI,RaP a "SeaIGeO, MeaSNDP, HaUaASe" teaHQeI RQN aRNLe QXP PtDOeGtP'XGteIePt XG tQeXI RNIL; QXP PDUeIXNIP PaXO "QXP PtDOeGtP SXLe QXZ aGO RNILRXtQ PDHHePP." aCteIRaIO, Qe RNILeO aP a UIXKate XGPtIDHtNI XG UaIXP.QXP ADPXePt FeaIP CNSSNReO tQe UDASXHatXNG NC Sa HIFUtNJIaUQXHZXSXtaXIe. a GeR XGteIGatXNGaS SaGJDaJe HaSSeO KNSa-UXXL ("RNISOPUeaL")QaO AeeG XGKeGteO AF a JeIZaG UIXePt. aANDt 1885, Xt HaDJQt NG XGCIaGHe aGO CSaPQeO RXtQ eYUIePP-tIaXG PUeeO aSS NKeI tQe HNDGtIF, GNtNGSF aZNGJ XGteSSeHtDaSP ADt aZNGJ aSS HSaPPeP; Xt RaP eKeG QeaIO XG tQePtIeetP. CINZ CIaGHe Xt IaOXateO tQINDJQNDt tQe RNISO. tQe ZNPt aHtXKeUINUaJaGOXPt NC KNSaUXXL RaP aDJDPte LeIHLQNCCP, RQN, at tQe PeHNGOKNSaUXXL HNGJIePP XG ZDGXHQ XG 1887, RaP aHHSaXZeO OXIeHtNI ("OXSeLeS,"XG KNSaUXXL) NC tQe XGteIGatXNGaS aHaOeZF NC KNSaUXXL. ADt at tQe tQXIOHNGJIePP, QeSO at UaIXP XG ZaF NC 1889, RXtQ LeIHLQNCCP UIePXOXGJ, HIXtXHaSteGPXNGP RXtQXG tQe ZNKeZeGt ZNDGteO aGO CXGaSSF AINLe Xt aUaIt.LeIHLQNCCP RaP HIDPQeO AF tQe HNSSaUPe NC aG XGteIGatXNGaS OIeaZ tQatQaO PeeZeO PN GeeOCDS aGO PN HeItaXG. Qe HIeateO GNtQXGJ eSPe aGO, NGaDJDPt 9, 1903, OXeO RQXSe NG KaHatXNG XG PRXtMeISaGO.ADt QXP HIFUtNSNJXH XOeaP PtXSS GNDIXPQ. CNI LeIHLQNCCP PNDJQt aGPReIPtN tQe UINASeZP tQIDPt DUNG HIFUtNSNJF AF GeR HNGOXtXNGP. "Xt XPGeHePPaIF tN OXPtXGJDXPQ HaIeCDSSF AetReeG a PF-

PteZ NC eGHXUQeIZeGteGKXPXNGeO CNI a ZNZeGtaIF eYHQaGJe NC SetteIP AetReeG PeKeIaS XPNSateOUeNUSe aGO a ZetQNO NC HIFUtNJIaUQF XGteGOeO tN JNKeIG tQe HNIIePUNGOeGHeAetReeG OXCCeIeGt aIZF HQXeCP CNI aG DGSXZXteO tXZe," Qe RINte. XG tQatNGe PeGteGHe, LeIHLQNCCP OXCCeIeGtXateP UIe-teSeJIaUQF ZXSXtaIFHNZZDGXHatXNGP CINZ UNPt-. tQe PeGteGHe XP UIeJGaGt RXtQ ZNPt NC tQeIeBDXIeZeGtP tQat QaKe HNZe tN Ae OeZaGOeO NC PFPteZP NC ZXSXtaIFHIFUtNJIaUQF, IeBDXIeZeGtP PDHQ aP PXZUSXHXtF, IeSXaAXSXtF, IaUXOXtF, aGOPN NG. tQXP HSeaI IeHNJGXtXNG NC tQe GeR NIOeI HNGPtXtDteP LeIHLQNCCP' CXIPtJIeat HNGtIXADtXNG tN HIFUtNSNJF.tQe PeHNGO RaP tN IeaCCXIZ XG a ZNOeIG HNGteYt tQe UIXGHXUSe tQat NGSFHIFUtaGaSFPtP HaG LGNR tQe PeHDIXtF NC a HXUQeI PFPteZ. Xt XP tQe CNIZ NCEDOJZeGt RQXHQ XP PtXSS DPeO.

0.0.1 Found trigraphs tQe and aGO, matching to THE and AND, so Q→H, G→N, O→D:

Xt RaP CIanHe, hNReKeI, that UDASXPhed Nne NC HIFUtNSNJF'P JIeatePtANNLP. Sa HIFUtNJIaUhXH ZXSXtaXIe CXIPt aUUeaIed aP tRN XnPtaSSZentP Xnthe ENDInaS deP PHXenHeP ZXSXtaXIeP Xn EanDaIF and CeAIDaIF NC 1883,AeXnJ IeXPPDed SateI that FeaI aP a UaUeIAaHL ANNL AF the ENDInaS'PUDASXPheI. Xt XP the ZNPt HNnHXPe ANNL Nn HIFUtNSNJF eKeI RIXtten. XtPaDthNI had the XnPtXnHt CNI the HIFUtNJIaUhXH EDJDSaI, and he HNZUIePPedXntN 64 UaJeP KXItDaSSF the entXIe LnNRn CXeSd NC HIFUtNSNJF, XnHSDdXnJUNSFaSUhaAetXHP RXth ZXYed aSUhaAetP, enHXUheIed HNde, and HXUheIdeKXHeP. the ANNL XP aSPN Nne NC the ZNPt PHhNSaISF Nn HIFUtNSNJF. XtPCNNtnNteP HXte ZNPt HSaPPXHaS and ZanF ZNdeIn PNDIHeP; HNZZentP PDHhaP "thXP XP nNt the NnSF hXPtNIXHaS NI AXASXNJIaUhXH eIINI CNI RhXHh the aDPtIXan RIXteI ZDPt Ae IeUINaHhed"PhNR hNR HaIeCDSSF the aDthNI haP PtDdXed thNPe PNDIHeP.XtP aDthNI ***RaP*** ANIn Eean-JDXSSaDZe-hDAeIt-KXHtNICIanJNXP-aSeYandIe-aDJDPte LeIHLhNCCP KNn nXeDRenhNC Nn EanDaIF 19, 1835, atnDth, hNSSand. aCteI JettXnJ deJIeeP Xn SetteIP and Xn PHXenHe CINZ theDnXKeIPXtF NC SXeJe, ***he RaP*** hXIed Xn 1863 aP an XnPtIDHtNI Xn ZNdeInSanJDaJeP at the hXJh PHhNNS at ZeSDn, a SaIJe tNRn 25 ZXSeP PNDtheaPtNC UaIXP. the neYt FeaI he ZaIIXed a JXIS CINZ the aIea and Xn 1865, Rhenhe RaP 30, theF had theXI NnSF HhXSd, a daDJhteI, UaDSXne. he PtaFed atZeSDn CNI 10 FeaIP, teaHhXnJ enJSXPh and JeIZan.AF that tXZe he had PhNItened hXP naZe tN aDJDPte

LeIHLhNCCP.AeaIded, dXJnXCXed, PSNR NC PUeeHh, LeIHLhNCCP, dePUXte an XnaAXSXtF tNZaXntaXn dXPHXUSXne Xn hXP HSaPPeP and PNZe eHHentIXHXtXeP NC HhaIaHteI,RaP a "SeaIned, MeaSNDP, HaUaASe" teaHheI RhN aRNLe hXP PtDdentP'XnteIePt Xn theXI RNIL; hXP PDUeIXNIP PaXd "hXP PtDdentP SXLe hXZ and RNILRXth PDHHePP." aCteIRaId, he RNILed aP a UIXKate XnPtIDHtNI Xn UaIXP.hXP ADPXePt FeaIP CNSSNRed the UDASXHatXNn NC Sa HIFUtNJIaUhXHZXSXtaXIe. a neR XnteInatXNnaS SanJDaJe HaSSed KNSa-UXXL ("RNISdPUeaL")had Aeen XnKented AF a JeIZan UIXePt. aANDt 1885, Xt HaDJht Nn XnCIanHe and CSaPhed RXth eYUIePP-tIaXn PUeed aSS NKeI the HNDntIF, nNtNnSF aZNnJ XnteSSeHtDaSP ADt aZNnJ aSS HSaPPeP; ***Xt RaP*** eKen heaId Xn thePtIeetP. CINZ CIanHe Xt IadXated thINDJhNDt the RNISd. the ZNPt aHtXKeUINUaJandXPt NC KNSaUXXL RaP aDJDPte LeIHLhNCCP, RhN, at the PeHNndKNSaUXXL HNnJIePP Xn ZDnXHh Xn 1887, RaP aHHSaXZed dXIeHtNI ("dXSeLeS,"Xn KNSaUXXL) NC the XnteInatXNnaS aHadeZF NC KNSaUXXL. ADt at the thXIdHNnJIePP, heSd at UaIXP Xn ZaF NC 1889, RXth LeIHLhNCCP UIePXdXnJ, HIXtXHaStenPXNnP RXthXn the ZNKeZent ZNDnted and CXnaSSF AINLe Xt aUaIt.LeIHLhNCCP RaP HIDPhed AF the HNSSaUPe NC an XnteInatXNnaS dIeaZ thathad PeeZed PN needCDS and PN HeItaXn. he HIeated nNthXnJ eSPe and, NnaDJDPt 9, 1903, dXed RhXSe Nn KaHatXNn Xn PRXtMeISand.ADt hXP HIFUtNSNJXH XdeaP PtXSS nNDIXPh. CNI LeIHLhNCCP PNDJht anPReIPtN the UINASeZP thIDPt DUNn HIFUtNSNJF AF neR HNndXtXNnP. "Xt XPneHePPaIF tN dXPtXnJDXPh HaIeCDSSF AetReen a PFPteZ NC enHXUheIZentenKXPXNned CNI a ZNZentaIF eYHhanJe NC SetteIP AetReen PeKeIaS XPNSatedUeNUSe and a ZethNd NC HIFUtNJIaUhF Xntended tN JNKeIn the HNIIePUNndenHeAetReen dXCCeIent aIZF HhXeCP CNI an DnSXZXted tXZe," he RINte. Xn thatNne PentenHe, LeIHLhNCCP dXCCeIentXateP UIe-teSeJIaUhF ZXSXtaIFHNZZDnXHatXNnP CINZ UNPt-. the PentenHe XP UIeJnant RXth ZNPt NC theIeBDXIeZentP that haKe HNZe tN Ae deZanded NC PFPteZP NC ZXSXtaIFHIFUtNJIaUhF, IeBDXIeZentP PDHh aP PXZUSXHXtF, IeSXaAXSXtF, IaUXdXtF, andPN Nn. thXP HSeaI IeHNJnXtXNn NC the neR NIdeI HNnPtXtDteP LeIHLhNCCP' CXIPtJIeat HNntIXADtXNn tN HIFUtNSNJF.the PeHNnd RaP tN IeaCCXIZ Xn a ZNdeIn HNnteYt the UIXnHXUSe that NnSFHIFUtanaSFPtP Han LnNR the PeHDIXtF NC a HXUheI PFPteZ. Xt XP the CNIZ NCEDdJZent RhXHh XP PtXSS DPed.

The phrase 'Xt RaP' appears multiple times and 'RaP' appears next to he(already decoded), so we assume that X→I, R→W, P→S

it was CIanHe, hNweKeI, that UDASished ***Nne NC*** HIFUtNSNJF's JIeatestANNLs. Sa HIFUtNJIaUhiH ZiSitaiIe CiIst aUUeaIed as twN instaSSZents inthe ENDInaS des sHienHes ZiSitaiIes in EanDaIF and CeAIDaIF ***NC*** 1883,AeinJ IeissDed SateI that FeaI as a UaUeIAaHL ANNL AF the ENDInaS'sUDASisheI. it is the ZNst HNnHise ANNL Nn HIFUtNSNJF eKeI wIitten. itsaDthNI had the instinHt CNI the HIFUtNJIaUhiH EDJDSaI, and he HNZUIessedintN 64 UaJes KiItDaSSF the entiIe LnNwn CieSd ***NC*** HIFUtNSNJF, inHSDdinJUNSFaSUhaAetiHs with ZiYed aSUhaAets, enHiUheIed HNde, and HiUheIdeKiHes. the ANNL is aSsN ***Nne NC*** the ZNst sHhNSaISF Nn HIFUtNSNJF. itsCNNtnNtes Hite ZNst HSassiHaS and ZanF ZNdeIn sNDIHes; HNZZents sDHhas "this is ***nNt*** the NnSF histNIiHaS NI AiASiNJIaUhiH eIINI CNI whiHh the aDstIian wIiteI ZDst Ae IeUINaHhed"shNw hNw HaIeCDSSF the aDthNI has stDdied thNse sNDIHes.its aDthNI was ANIn Eean-JDiSSaDZe-hDAeIt-KiHtNICIanJNis-aSeYandIe-aDJDste LeIHLhNCCs KNn nieDwenhNC Nn EanDaIF 19, 1835, atnDth, hNSSand. aCteI JettinJ deJIees in SetteIs and in sHienHe CINZ theDniKeIsitF NC SieJe, he was hiIed in 1863 as an instIDHtNI in ZNdeInSanJDaJes at the hiJh sHhNNS at ZeSDn, a SaIJe tNwn 25 ZiSes sNDtheastNC UaIis. the neYt FeaI he ZaIIied a JiIS CINZ the aIea and in 1865, whenhe was 30, theF had theiI NnSF HhiSd, a daDJhteI, UaDSine. he staFed atZeSDn CNI 10 FeaIs, teaHhinJ enJSish and JeIZan.AF that tiZe he had shNItened his naZe tN aDJDste LeIHLhNCCs.AeaIded, diJniCied, sSNw NC sUeeHh, LeIHLhNCCs, desUite an inaAiSitF tNZaintain disHiUSine in his HSasses and sNZe eHHentIiHities NC HhaIaHteI,was a "SeaIned, MeaSNDs, HaUaASe" teaHheI whN awNLe his stDdents'inteIest in theiI wNIL; his sDUeIiNIs said "his stDdents SiLe hiZ and wNILwith sDHHess." aCteIwaId, he wNILed as a UIiKate instIDHtNI in UaIis.his ADsiest FeaIs CNSSNwed the UDASiHatiNn NC Sa HIFUtNJIaUhiHZiSitaiIe. a new inteInatiNnaS SanJDaJe HaSSed KNSa-UiiL ("wNISdsUeaL")had Aeen inKented AF a JeIZan UIiest. aANDt 1885, it HaDJht Nn inCIanHe and CSashed with eYUIess-tIain sUeed aSS NKeI the HNDntIF, nNtNnSF aZNnJ inteSSeHtDaSs ADt aZNnJ aSS HSasses; it was eKen heaId in thestIeets. CINZ CIanHe it Iadiated thINDJhNDt the wNISd. the ZNst aHtiKeUINUaJandist NC KNSaUiiL was aDJDste LeIHLhNCCs, whN, at the seHNndKNSaUiiL HNnJIess in ZDniHh in 1887, was aHHSaiZed diIeHtNI ("diSeLeS,"in KNSaUiiL) NC the inteInatiNnaS aHadeZF NC KNSaUiiL. ADt at the thiIdHNnJIess, heSd at UaIis in ZaF NC 1889, with LeIHLhNCCs UIesidinJ, HIitiHaStensiNns within

the ZNKeZent ZNDnted and CinaSSF AINLe it aUaIt.LeIHLhNCCs was HIDshed AF the HNSSaUse NC an inteInatiNnaS dIeaZ thathad seeZed sN needCDS and sN HeItain. he HIeated ***nNthinJ eSse*** and, NnaDJDst 9, 1903, died whiSe Nn KaHatiNn in switMeISand.ADt his HIFUtNSNJiH ideas stiSS nNDIish. CNI LeIHLhNCCs sNDJht answeIstN the UINASeZs thIDst DUNn HIFUtNSNJF AF new HNnditiNns. "it isneHessaIF tN distinJDish HaIeCDSSF Aetween a sFsteZ NC enHiUheIZentenKisiNned CNI a ZNZentaIF eYHhanJe NC SetteIs Aetween seKeIaS isNSatedUeNUSe and a ZethNd NC HIFUtNJIaUhF intended tN JNKeIn the HNIIesUNndenHeAetween diCCeIent aIZF HhieCs CNI an DnSiZited tiZe," he wINte. in thatNne sentenHe, LeIHLhNCCs diCCeIentiates UIe-teSeJIaUhF ZiSitaIFHNZZDniHatiNns CINZ UNst-. the sentenHe is UIeJnant with ZNst NC theIeBDiIeZents that haKe HNZe tN Ae deZanded NC sFsteZs NC ZiSitaIFHIFUtNJIaUhF, IeBDiIeZents sDHh as siZUSiHitF, IeSiaAiSitF, IaUiditF, andsN Nn. this HSeaI IeHNJnitiNn NC the new NIdeI HNnstitDtes LeIHLhNCCs' CiIstJIeat HNntIiADtiNn tN HIFUtNSNJF.the seHNnd was tN IeaCCiIZ in a ZNdeIn HNnteYt the UIinHiUSe that NnSFHIFUtanaSFsts Han LnNw the seHDItF NC a HiUheI sFsteZ. it is the CNIZ NCEDdJZent whiHh is stiSS Dsed.

'Nne' appears a few times and on its own sometimes next to 'NC', which appears a lot as a preposition, and there's also 'nNthinJ eSse', meaning that we can assume N→O, C→F, J→G, S→L:

it was fIanHe, ***howeKeI***, ***that UDAlished one of HIFUtologF's gIeatestAooLs***. la HIFUtogIaUhiH ZilitaiIe fiIst aUUeaIed as two installZents inthe EoDInal des sHienHes ZilitaiIes in EanDaIF and feAIDaIF of 1883,Aeing IeissDed lateI that FeaI as a UaUeIAaHL AooL AF the EoDInal'sUDAlisheI. it is the Zost HonHise AooL on HIFUtologF eKeI wIitten. itsaDthoI had the instinHt foI the HIFUtogIaUhiH EDgDlaI, and he HoZUIessedinto 64 Uages KiItDallF the entiIe Lnown field of HIFUtologF, inHlDdingUolFalUhaAetiHs with ZiYed alUhaAets, enHiUheIed Hode, and HiUheIdeKiHes. the AooL is also one of the Zost sHholaIlF on HIFUtologF. itsfootnotes Hite Zost HlassiHal and ZanF ZodeIn soDIHes; HoZZents sDHhas "this is not the onlF histoIiHal oI AiAliogIaUhiH eIIoI foI whiHh the aDstIian wIiteI ZDst Ae IeUIoaHhed"show how HaIefDllF the aDthoI has stDdied those soDIHes.its aDthoI was AoIn Eean-gDillaDZe-hDAeIt-KiHtoIfIangoisaleYandIe-aDgDste LeIHLhoffs Kon nieDwenhof on EanDaIF 19, 1835, atnDth, holland. afteI getting degIees in letteIs and in sHienHe fIoZ theDniKeIsitF of liege, he was hiIed in 1863 as an instIDHtoI in ZodeInlangDages at the high sHhool at ZelDn, a laIge town 25 Ziles soDtheastof UaIis. the neYt FeaI he ZaIIied a giIl

fIoZ the aIea and in 1865, whenhe was 30, theF had theiI onlF Hhild, a daDghteI, UaDline. he staFed atZelDn foI 10 FeaIs, teaHhing english and geIZan.AF that tiZe he had shoItened his naZe to aDgDste LeIHLhoffs.AeaIded, dignified, slow of sUeeHh, LeIHLhoffs, desUite an inaAilitF toZaintain disHiUline in his Hlasses and soZe eHHentIiHities of HhaIaHteI,was a "leaIned, MealoDs, HaUaAle" teaHheI who awoLe his stDdents'inteIest in theiI woIL; his sDUeIioIs said "his stDdents liLe hiZ and woILwith sDHHess." afteIwaId, he woILed as a UIiKate instIDHtoI in UaIis.his ADsiest FeaIs followed the UDAliHation of la HIFUtogIaUhiHZilitaiIe. a new inteInational langDage Halled Kola-UiiL ("woIldsUeaL")had Aeen inKented AF a geIZan UIiest. aAoDt 1885, it HaDght on infIanHe and flashed with eYUIess-tIain sUeed all oKeI the HoDntIF, notonlF aZong intelleHtDals ADt aZong all Hlasses; it was eKen heaId in thestIeets. fIoZ fIanHe it Iadiated thIoDghoDt the woIld. the Zost aHtiKeUIoUagandist of KolaUiiL was aDgDste LeIHLhoffs, who, at the seHondKolaUiiL HongIess in ZDniHh in 1887, was aHHlaiZed diIeHtoI ("dileLel,"in KolaUiiL) of the inteInational aHadeZF of KolaUiiL. ADt at the thiIdHongIess, held at UaIis in ZaF of 1889, with LeIHLhoffs UIesiding, HItitiHaltensions within the ZoKeZent ZoDnted and finallF AIoLe it aUaIt.LeIHLhoffs was HIDshed AF the HollaUse of an inteInational dIeaZ thathad seeZed so needfDl and so HeItain. he HIeated nothing else and, onaDgDst 9, 1903, died while on KaHation in switMeIland.ADt his HIFUtologiH ideas still noDIish. foI LeIHLhoffs soDght answeIsto the UIoAleZs thIDst DUon HIFUtologF AF new Honditions. "it isneHessaIF to distingDish HaIefDllF Aetween a sFsteZ of enHiUheIZentenKisioned foI a ZoZentaIF eYHhange of letteIs Aetween seKeIal isolatedUeoUle and a Zethod of HIFUtogIaUhF intended to goKeIn the HoIIesUondenHeAetween diffeIent aIZF Hhiefs foI an DnliZited tiZe," he wIote. in thatone sentenHe, LeIHLhoffs diffeIentiates UIe-telegIaUhF ZilitaIFHoZZDniHations fIoZ Uost-. the sentenHe is UIegnant with Zost of theIeBDiIeZents that haKe HoZe to Ae deZanded of sFsteZs of ZilitaIFHIFUtogIaUhF, IeBDiIeZents sDHh as siZUliHitF, IeliaAilitF, IaUiditF, andso on. this HleaI IeHognition of the new oIdeI HonstitDtes LeIHLhoffs' fiIstgIeat HontIiADtion to HIFUtologF.the seHond was to IeaffiIZ in a ZodeIn HonteYt the UIinHiUle that onlFHIFUtanalFsts Han Lnow the seHDIitF of a HiUheI sFsteZ. it is the foIZ ofEDdgZent whiHh is still Dsed.

'howeKeI' is clearly 'however' and 'that UDAlished one of HIFUtologF's gIeatestAooLs' shows that 'UDAlished' can be 'published', so K→V, I→R, U→P, D→U, A→B:

it was ***franHe***, however, that published one of ***HrFptologF's*** greatestbooLs. la HrFptographiH Zilitaire first appeared as two ***installZents*** inthe ***Eournal des***

sHienHes Zilitaires in EanuarF and februarF of 1883,being reissued later that Fear as a paperbaHL booL bF the Eournal'spublisher. it is the Zost HonHise booL on HrFptologF ever written. itsauthor had the instinHt for the HrFptographiH Eugular, and he HoZpressedinto 64 pages virtuallF the entire Lnown field of HrFptologF, inHludingpolFalphabetiHs with ZiYed alphabets, enHiphered Hode, and HipherdeviHes. the booL is also one of the Zost sHholarlF on HrFptologF. itsfootnotes Hite Zost HlassiHal and ZanF Zodern sourHes; HoZZents suHhas "this is not the onlF historiHal or bibliographiH error for whiHh the austrian writer Zust be reproaHhed"show how HarefullF the author has studied those sourHes.its author was born Eean-guillauZe-hubert-viHtorfrangois-aleYandre-auguste LerHLhoffs von nieuwenhof on EanuarF 19, 1835, atnuth, holland. after getting degrees in letters and in sHienHe froZ theuniversitF of liege, he was hired in 1863 as an instruHtor in Zodernlanguages at the high sHhool at Zelun, a large town 25 Ziles southeastof paris. the neYt Fear he Zarried a girl froZ the area and in 1865, whenhe was 30, theF had their onlF Hhild, a daughter, pauline. he staFed atZelun for 10 Fears, teaHhing english and gerZan.bF that tiZe he had shortened his naZe to auguste LerHLhoffs.bearded, dignified, slow of speeHh, LerHLhoffs, despite an inabilitF toZaintain disHipline in his Hlasses and soZe eHHentriHities of HharaHter,was a "learned, Mealous, Hapable" teaHher who awoLe his students'interest in their worL; his superiors said "his students liLe hiZ and worLwith suHHess." afterward, he worLed as a private instruHtor in paris.his busiest Fears followed the publiHation of la HrFptographiHZilitaire. a new international language Halled vola-piiL ("worldspeaL")had been invented bF a gerZan priest. about 1885, it Haught on infranHe and flashed with eYpress-train speed all over the HountrF, notonlF aZong intelleHtuals but aZong all Hlasses; it was even heard in thestreets. froZ franHe it radiated throughout the world. the Zost aHtivepropagandist of volapiiL was auguste LerHLhoffs, who, at the seHondvolapiiL Hongress in ZuniHh in 1887, was aHHlaiZed direHtor ("dileLel,"in volapiiL) of the international aHadeZF of volapiiL. but at the thirdHongress, held at paris in ZaF of 1889, with LerHLhoffs presiding, HritiHaltensions within the ZoveZent Zounted and finallF broLe it apart.LerHLhoffs was Hrushed bF the Hollapse of an international dreaZ thathad seeZed so needful and so Hertain. he Hreated nothing else and, onaugust 9, 1903, died while on vaHation in switMerland.but his HrFptologiH ideas still nourish. for LerHLhoffs sought answersto the probleZs thrust upon HrFptologF bF new Honditions. "it isneHessarF to distinguish HarefullF between a sFsteZ of enHipherZentenvisioned for a ZoZentarF eYHhange of letters between several isolatedpeople and a Zethod of HrFptographF intended to govern the HorrespondenHebetween different arZF Hhiefs for an unliZited tiZe," he wrote. in thatone sentenHe, LerHLhoffs differen-

tiates pre-telegraphF ZilitarFHoZZuniHations froZ post-. the sentenHe is pregnant with Zost of thereBuireZents that have HoZe to be deZanded of sFsteZs of ZilitarFHrFptographF, reBuireZents suHh as siZpliHitF, reliabilitF, rapiditF, andso on. this Hlear reHognition of the new order Honstitutes LerHLhoffs' firstgreat Hontribution to HrFptologF.the seHond was to reaffirZ in a Zodern HonteYt the prinHiple that onlFHrFptanalFsts Han Lnow the seHuritF of a Hipher sFsteZ. it is the forZ ofEudgZent whiHh is still used.

'HrFptologF's', is clearly cryptology, meaning that 'franHe' is France and 'Eournal des sHienHes Zilitaires' is 'Journal des Sciences Militaires', being proven by 'installZents', so H→C, F→Y, E→J, Z→M:

it was france, however, that published one of cryptology's greatest***booLs***. la cryptographic militaire first appeared as two installments inthe journal des sciences militaires in january and february of 1883,being reissued later that year as a ***paperbacL*** booL by the journal'spublisher. it is the most concise booL on cryptology ever written. itsauthor had the instinct for the cryptographic jugular, and he compressedinto 64 pages virtually the entire Lnown field of cryptology, includingpolyalphabetics with ***miYed*** alphabets, enciphered code, and cipherdevices. the booL is also one of the most scholarly on cryptology. itsfootnotes cite most classical and many modern sources; comments suchas "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-victorfrangois-aleYandre-auguste LercLhoffs von nieuwenhof on january 19, 1835, atnuth, holland. after getting degrees in letters and in science from theuniversity of liege, he was hired in 1863 as an instructor in modernlanguages at the high school at melun, a large town 25 miles southeastof paris. the neYt year he married a girl from the area and in 1865, whenhe was 30, they had their only child, a daughter, pauline. he stayed atmelun for 10 years, teaching english and german.by that time he had shortened his name to auguste LercLhoffs.bearded, dignified, slow of speech, LercLhoffs, despite an inability tomaintain discipline in his classes and some eccentricities of character,was a "learned, Mealous, capable" teacher who awoLe his students'interest in their worL; his superiors said "his students liLe him and worLwith success." afterward, he worLed as a private instructor in paris.his busiest years followed the publication of la cryptographicmilitaire. a new international language called volapiiL ("worldspeaL")had been invented by a german priest. about 1885, it caught on infrance and flashed with eYpress-train speed all over the country, notonly among intellectuals but among all classes; it was even heard in thestreets. from france it

radiated throughout the world. the most activepropagandist of volapiiL was auguste LercLhoffs, who, at the secondvolapiiL congress in munich in 1887, was acclaimed director ("dileLel,"in volapiiL) of the international academy of volapiiL. but at the thirdcongress, held at paris in may of 1889, with LercLhoffs presiding, criticaltensions within the movement mounted and finally broLe it apart.LercLhoffs was crushed by the collapse of an international dream thathad seemed so needful and so certain. he created nothing else and, onaugust 9, 1903, died while on vacation in ***switMerland***.but his cryptologic ideas still nourish. for LercLhoffs sought answersto the problems thrust upon cryptology by new conditions. "it isnecessary to distinguish carefully between a system of enciphermentenvisioned for a momentary eYchange of letters between several isolatedpeople and a method of cryptography intended to govern the correspondencebetween different army chiefs for an unlimited time," he wrote. in thatone sentence, LercLhoffs differentiates pre-telegraphy militarycommunications from post-. the sentence is pregnant with most of thereBuirements that have come to be demanded of systems of militarycryptography, ***reBuirements*** such as simplicity, reliability, rapidity, andso on. this clear recognition of the new order constitutes LercLhoffs' firstgreat contribution to cryptology.the second was to reaffirm in a modern ***conteYt*** the principle that onlycryptanalysts can Lnow the security of a cipher system. it is the form ofjudgment which is still used.

The remaining words show that L→K, Y→X, B→Q, M→Z:

it was france, however, that published one of cryptology's greatestbooks. la cryptographic militaire first appeared as two installments inthe journal des sciences militaires in january and february of 1883,being reissued later that year as a paperback book by the journal'spublisher. it is the most concise book on cryptology ever written. itsauthor had the instinct for the cryptographic jugular, and he compressedinto 64 pages virtually the entire known field of cryptology, includingpolyalphabetics with mixed alphabets, enciphered code, and cipherdevices. the book is also one of the most scholarly on cryptology. itsfootnotes cite most classical and many modern sources; comments suchas "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-victorfrangois-alexandre-auguste kerckhoffs von nieuwenhof on january 19, 1835, atnuth, holland. after getting degrees in letters and in science from theuniversity of liege, he was hired in 1863 as an instructor in modernlanguages at the high school at melun, a large town 25 miles southeastof paris. the next year he married a girl from the area and in 1865, whenhe was 30, they had their only child, a daughter, pauline. he stayed atmelun 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 tomaintain 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 workwith success." afterward, he worked as a private instructor in paris.his busiest years followed the publication of la cryptographicmilitaire. a new international language called vola-piik ("worldspeak")had been invented by a german priest. about 1885, it caught on infrance and flashed with express-train speed all over the country, notonly among intellectuals but among all classes; it was even heard in thestreets. from france it radiated throughout the world. the most activepropagandist of volapiik was auguste kerckhoffs, who, at the secondvolapiik congress in munich in 1887, was acclaimed director ("dilekel,"in volapiik) of the international academy of volapiik. but at the thirdcongress, held at paris in may of 1889, with kerckhoffs presiding, criticaltensions within the movement mounted and finally broke it apart.kerckhoffs was crushed by the collapse of an international dream thathad seemed so needful and so certain. he created nothing else and, onaugust 9, 1903, died while on vacation in switzerland.but his cryptologic ideas still nourish. for kerckhoffs sought answersto the problems thrust upon cryptology by new conditions. "it isnecessary to distinguish carefully between a system of enciphermentenvisioned for a momentary exchange of letters between several isolatedpeople and a method of cryptography intended to govern the correspondencebetween different army chiefs for an unlimited time," he wrote. in thatone sentence, kerckhoffs differentiates pretelegraphy militarycommunications from post-. the sentence is pregnant with most of therequirements that have come to be demanded of systems of militarycryptography, requirements such as simplicity, reliability, rapidity, andso on. this clear recognition of the new order constitutes kerckhoffs' firstgreat contribution to cryptology.the second was to reaffirm in a modern context the principle that onlycryptanalysts can know the security of a cipher system. it is the form ofjudgment which is still used.

Conclusions

In this lab, I decrypted an intercepted message using the frequency analysis method and found its meaning - A paragraph about french authors that published and worked in cryptology.