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

Technical University of Moldova

Faculty of Computers, Informatics and Microelectronics

Department of Software Engineering and Automatics

Report

for Laboratory Work Nr. 2

for “Cryptographic Methods of Information Protection”

Done by:

Sirghi Tudor, gr. FAF-213

Verify by:

Aureliu ZGUREANU

Chișinău – 2023

**Topic**: Mono-alphabetic Cipher Cryptanalysis

**Tasks**:

1. Break a sequence of encoded text using the frequency analysis method. The text has been encoded using a 2-key version of the Caesar Cipher. The original text is assumed to be in English, and non-letter characters were not encoded.

**Frequency analysis attack method:**

Mono-alphabetic substitution ciphers have one glaring vulnerability: the letter frequency remains unchanged, simply, the letters matching those frequencies have been swapped. By analyzing the frequencies of characters in ciphertext and using the frequencies of letters of a given language as reference, the original message can be determined, with longer messages being easier to decrypt.

Simply substituting according to frequency alone is not enough, as the contents of a message can diverge from the language average letter frequency. A cryptanalyst must also use the frequencies of digraphs (such as AN, IN, ON, ER, RE, etc.) and trigraphs (such as THE, AND, ENT, ION, FOR, etc.) in order to facilitate breaking the message.

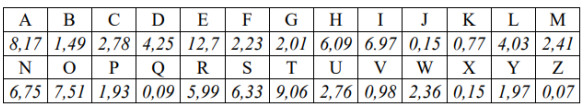
For the English language, the frequency of letters (expressed in percentages) is:  


Fig. 1: *Frequency of letters in English language*

**Ciphertext (Variant 3):**

UNSFAXDP TGO NWQVIP GVKVI PTXO RQVWQVI TGF NC WQV PDAPWXWDWXNGHXUQVIP WQVF OVPHIXAVO RVIV

THWDTSSF DPVO, TGO PN WQV CXIPW TWWVPWVO DPV NCWQTW JVGIV XG UNSXWXHTS TCCTXIP HNZV CINZ WQV

INZTGP — TGO CINZ WQV JIVTWVPW INZTG NC WQVZ TSS. EDSXDPHTVPTI WQDP XZUIVPPVO QXP GTZV

UVIZTGVGWSF XGWN HIFUWNSNJF.XW ZDPW AV WQTW TP PNNG TP T HDSWDIV QTP IVTHQVO T HVIWTXG

SVKVS,UINATASF ZVTPDIVO STIJVSF AF XWP SXWVITHF, HIFUWNJITUQF TUUVTIPPUNGWTGVNDPSF — TP XWP

UTIVGWP, STGJDTJV TGO RIXWXGJ, UINATASF TSPN OXO.WQV ZDSWXUSV QDZTG GVVOP TGO OVPXIVP WQTW OVZTGO

UIXKTHF TZNGJ WRNNI ZNIV UVNUSV XG WQV ZXOPW NC PNHXTS SXCV ZDPW XGVKXWTASF SVTO WNHIFUWNSNJF

RQVIVKVI ZVG WQIXKV TGO RQVIVKVI WQVF RIXWV. HDSWDITSOXCCDPXNG PVVZP T SVPP SXLVSF VYUSTGTWXNG

CNI XWP NHHDIIVGHV XG. PN ZTGFTIVTP, ZTGF NC WQVZ OXPWTGW TGO XPNSTWVO.WQV FVMXOXP, TG NAPHDIV

PVHW NC TANDW 25,000 UVNUSV XG, GNIWQVIG XITB,DPV T HIFUWXH PHIXUW XG WQVXI QNSF ANNLP AVHTDPV

WQVF CVTI UVIPVHDWXNG AFWQVXI ZNPSVZ GVXJQANIP. WXAVWTGP DPV T LXGO NC HXUQVI HTSSVO "IXGPUDGP"CNI NCCXHXTS HNIIVPUNGOVGHV; XW XP GTZVO CNI XWP XGKVGWNI IXG-H'(QQVG-)PUDGP(-UT), RQN

SXKVO XG WQV 1300P. WQV GPXAXOX PVHIVW PNHXVWF NC GXJVIXTLVVUP XWP UXHWNJITUQXH PHIXUW

CINZ VDINUVTGP TP ZDHQ TP UNPPXASVAVHTDPV XW XP DPVO HQXVCSF WN VYUIVPP SNKV XG ITWQVI OXIVHW

XZTJVIF, TGOPTZUSVP TUUVTI WN AV TW SVTPW TP UNIGNJITUQXH TP WQVF TIV HIFUWNJITUQXH.WQV HIFUWNJITUQF

NC WQTXSTGO OVKVSNUVO DGOVI XGOXTG XGCSDVGHV. TGVZAIFNGXH PWDOF NC WQV PDAEVHW VKVG TUUVTIP

XG T JITZZTWXHTS RNILVGWXWSVO UNITGTKTLFT AF QSDTGJ UITPNW TLPTITGXWX (UQV). NGV PFPWVZ,HTSSVO

"WQV VIIXGJ PXTZVPV," PDAPWXWDWVP NGV OVSXHTWV PXTZVPV SVWWVI CNITGNWQVI. XG TGNWQVI

PFPWVZ, HNGPNGTGWP TIV OXKXOVO XGWN PVKVG JINDUP NC CXKV SVWWVIP;T SVWWVI XP XGOXHTWVO AF

RIXWXGJ WQV PXTZVPV GDZAVI NC XWP JINDU TGOUSTHXGJ KVIWXHTS ONWP DGOVI XW VBDTS XG GDZAVI WN

WQV SVWWVI'P USTHV XG XWPJINDU. T PFPWVZ HTSSVO "WQV QVIZXW ZVWTZNIUQNPXGJ SVWWVIP" RIXWVP

WQVWVYW ATHLRTIOP.XG WQV VDINUV NC WQV STWXG TSUQTAVW—CINZ RQXHQ ZNOVIG HIFUWNSNJFRNDSO

PUIXGJ—HIFUWNJITUQF CSXHLVIVO RVTLSF. RXWQ WQV HNSSTUPV NC WQVINZTG VZUXIV, VDINUV QTO USDGJVO

XGWN WQV NAPHDIXWF NC WQV OTIL TJVP.SXWVITHF QTO TSS ADW OXPTUUVTIVO. TIWP TGO PHXVGHVP RVIV

CNIJNWWVG, TGOHIFUWNJITUQF RTP GNW VYHVUWVO. NGSF ODIXGJ WQV ZXOOSV TJVP

NHHTPXNGTSZTGDPHIXUWP, RXWQ TG XGCIVBDVGW PXJGTWDIV NI JSNPP NI "OVN JITWXTP" WQTW TANIVO ZNGL

UDW XGWN HXUQVI WN TZDPV QXZPVSC, CXWCDSSF XSSDZXGTWV WQVHIFUWNSNJXH OTILGVPP, TGO, SXLV T

PXGJSV HTGOSV JDWWVIXGJ XG T JIVTWZVOXVKTS QTSS, WQVXI CVVASV CSTIXGJP NGSF VZUQTPXMV WQV

JSNNZ.WQV PFPWVZP DPVO RVIV PXZUSV XG WQV VYWIVZV. UQITPVP RVIV RIXWWVGKVIWXHTSSF NI ATHLRTIOP;

ONWP RVIV PDAPWXWDWVO CNI KNRVSP;CNIVXJG TSUQTAVWP, TP JIVVL, QVAIVR, TGO TIZVGXTG, RVIV DPVO;

VTHQSVWWVI NC WQV USTXGWVYW RTP IVUSTHVO AF WQV NGV WQTW CNSSNRP XW; XG WQV ZNPWTOKTGHVO

PFPWVZ, PUVHXTS PXJGP PDAPWXWDWVO CNI SVWWVIP. CNI TSZNPW TWQNDPTGO FVTIP, CINZ AVCNIV 500

WN 1400, WQV HIFUWNSNJF NC RVPWVIGHXKXSXMTWXNG PWTJGTWVO.

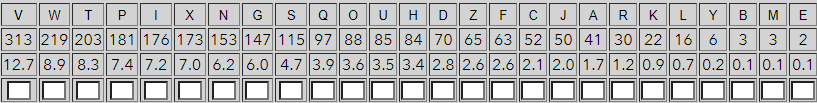
**Implementation:** For first, we need to find the frequency of each letter in crypted text. For my variant it is: (Fig.2)  


Fig. 2: *Frequency of letters in text*

The most common characters used in the text were V, W and T, while the most common digraphs were WQ and QV, coinciding with English’s most common digraphs: TH and HE. The most common trigraph was WQV, corresponding with “THE”. We can assume that W stands for “T”, Q stands for “H” and V stands for “E”, respectively. Following these substitutions, the ciphertext now looks as such:

UNSFAXDP TGO NtheIP GeKeI PTXO RhetheI TGF NC the PDAPtXtDtXNGHXUheIP theF OePHIXAeO ReIe

THtDTSSF DPeO, TGO PN the CXIPt TttePteO DPe NCthTt JeGIe XG UNSXtXHTS TCCTXIP HNZe CINZ the

INZTGP — TGO CINZ the JIeTtePt INZTG NC theZ TSS. EDSXDPHTePTI thDP XZUIePPeO hXP GTZe

UeIZTGeGtSF XGtN HIFUtNSNJF.Xt ZDPt Ae thTt TP PNNG TP T HDStDIe hTP IeTHheO T HeItTXG

SeKeS,UINATASF ZeTPDIeO STIJeSF AF XtP SXteITHF, HIFUtNJITUhF TUUeTIPPUNGtTGeNDPSF — TP XtP

UTIeGtP, STGJDTJe TGO RIXtXGJ, UINATASF TSPN OXO.the ZDStXUSe hDZTG GeeOP TGO OePXIeP thTt OeZTGO

UIXKTHF TZNGJ tRNNI ZNIe UeNUSe XG the ZXOPt NC PNHXTS SXCe ZDPt XGeKXtTASF SeTO tNHIFUtNSNJF

RheIeKeI ZeG thIXKe TGO RheIeKeI theF RIXte. HDStDITSOXCCDPXNG PeeZP T SePP SXLeSF eYUSTGTtXNG

CNI XtP NHHDIIeGHe XG. PN ZTGFTIeTP, ZTGF NC theZ OXPtTGt TGO XPNSTteO.the FeMXOXP, TG NAPHDIe

PeHt NC TANDt 25,000 UeNUSe XG, GNItheIG XITB,DPe T HIFUtXH PHIXUt XG theXI hNSF ANNLP AeHTDPe

theF CeTI UeIPeHDtXNG AFtheXI ZNPSeZ GeXJhANIP. tXAetTGP DPe T LXGO NC HXUheI HTSSeO "IXGPUDGP"CNI NCCXHXTS HNIIePUNGOeGHe; Xt XP GTZeO CNI XtP XGKeGtNI IXG-H'(hheG-)PUDGP(-UT), RhN

SXKeO XG the 1300P. the GPXAXOX PeHIet PNHXetF NC GXJeIXTLeeUP XtP UXHtNJITUhXH PHIXUt

CINZ eDINUeTGP TP ZDHh TP UNPPXASeAeHTDPe Xt XP DPeO HhXeCSF tN eYUIePP SNKe XG ITtheI OXIeHt

XZTJeIF, TGOPTZUSeP TUUeTI tN Ae Tt SeTPt TP UNIGNJITUhXH TP theF TIe HIFUtNJITUhXH.the HIFUtNJITUhF

NC thTXSTGO OeKeSNUeO DGOeI XGOXTG XGCSDeGHe. TGeZAIFNGXH PtDOF NC the PDAEeHt eKeG TUUeTIP

XG T JITZZTtXHTS RNILeGtXtSeO UNITGTKTLFT AF hSDTGJ UITPNt TLPTITGXtX (Uhe). NGe PFPteZ,HTSSeO

"the eIIXGJ PXTZePe," PDAPtXtDteP NGe OeSXHTte PXTZePe SetteI CNITGNtheI. XG TGNtheI

PFPteZ, HNGPNGTGtP TIe OXKXOeO XGtN PeKeG JINDUP NC CXKe SetteIP;T SetteI XP XGOXHTteO AF

RIXtXGJ the PXTZePe GDZAeI NC XtP JINDU TGOUSTHXGJ KeItXHTS ONtP DGOeI Xt eBDTS XG GDZAeI tN

the SetteI'P USTHe XG XtPJINDU. T PFPteZ HTSSeO "the heIZXt ZetTZNIUhNPXGJ SetteIP" RIXteP

theteYt ATHLRTIOP.XG the eDINUe NC the STtXG TSUhTAet—CINZ RhXHh ZNOeIG HIFUtNSNJFRNDSO

PUIXGJ—HIFUtNJITUhF CSXHLeIeO ReTLSF. RXth the HNSSTUPe NC theINZTG eZUXIe, eDINUe hTO USDGJeO

XGtN the NAPHDIXtF NC the OTIL TJeP.SXteITHF hTO TSS ADt OXPTUUeTIeO. TItP TGO PHXeGHeP ReIe

CNIJNtteG, TGOHIFUtNJITUhF RTP GNt eYHeUteO. NGSF ODIXGJ the ZXOOSe TJeP

NHHTPXNGTSZTGDPHIXUtP, RXth TG XGCIeBDeGt PXJGTtDIe NI JSNPP NI "OeN JITtXTP" thTt TANIeO ZNGL

UDt XGtN HXUheI tN TZDPe hXZPeSC, CXtCDSSF XSSDZXGTte theHIFUtNSNJXH OTILGePP, TGO, SXLe T

PXGJSe HTGOSe JDtteIXGJ XG T JIeTtZeOXeKTS hTSS, theXI CeeASe CSTIXGJP NGSF eZUhTPXMe the

JSNNZ.the PFPteZP DPeO ReIe PXZUSe XG the eYtIeZe. UhITPeP ReIe RIXtteGKeItXHTSSF NI ATHLRTIOP;

ONtP ReIe PDAPtXtDteO CNI KNReSP;CNIeXJG TSUhTAetP, TP JIeeL, heAIeR, TGO TIZeGXTG, ReIe DPeO;

eTHhSetteI NC the USTXGteYt RTP IeUSTHeO AF the NGe thTt CNSSNRP Xt; XG the ZNPtTOKTGHeO

PFPteZ, PUeHXTS PXJGP PDAPtXtDteO CNI SetteIP. CNI TSZNPt TthNDPTGO FeTIP, CINZ AeCNIe 500

tN 1400, the HIFUtNSNJF NC RePteIGHXKXSXMTtXNG PtTJGTteO.

It is clear that T and "A" are related because of the repeating of solitary Ts and patterns like "thTt". In that situation, independent digraphs like "Xt" and "XP" could be equivalent to "IT" and "IS". We can safely assume that X represents "I". The following round of substitutions:

UNSFAiDP aGO NtheIP GeKeI PaiO RhetheI aGF NC the PDAPtitDtiNGHiUheIP theF OePHIiAeO ReIe

aHtDaSSF DPeO, aGO PN the CiIPt attePteO DPe NCthat JeGIe iG UNSitiHaS aCCaiIP HNZe CINZ the

INZaGP — aGO CINZ the JIeatePt INZaG NC theZ aSS. EDSiDPHaePaI thDP iZUIePPeO hiP GaZe

UeIZaGeGtSF iGtN HIFUtNSNJF.it ZDPt Ae that aP PNNG aP a HDStDIe haP IeaHheO a HeItaiG

SeKeS,UINAaASF ZeaPDIeO SaIJeSF AF itP SiteIaHF, HIFUtNJIaUhF aUUeaIPPUNGtaGeNDPSF — aP itP

UaIeGtP, SaGJDaJe aGO RIitiGJ, UINAaASF aSPN OiO.the ZDStiUSe hDZaG GeeOP aGO OePiIeP that OeZaGO

UIiKaHF aZNGJ tRNNI ZNIe UeNUSe iG the ZiOPt NC PNHiaS SiCe ZDPt iGeKitaASF SeaO tNHIFUtNSNJF

RheIeKeI ZeG thIiKe aGO RheIeKeI theF RIite. HDStDIaSOiCCDPiNG PeeZP a SePP SiLeSF eYUSaGatiNG

CNI itP NHHDIIeGHe iG. PN ZaGFaIeaP, ZaGF NC theZ OiPtaGt aGO iPNSateO.the FeMiOiP, aG NAPHDIe

PeHt NC aANDt 25,000 UeNUSe iG, GNItheIG iIaB,DPe a HIFUtiH PHIiUt iG theiI hNSF ANNLP AeHaDPe

theF CeaI UeIPeHDtiNG AFtheiI ZNPSeZ GeiJhANIP. tiAetaGP DPe a LiGO NC HiUheI HaSSeO "IiGPUDGP"CNI NCCiHiaS HNIIePUNGOeGHe; it iP GaZeO CNI itP iGKeGtNI IiG-H'(hheG-)PUDGP(-Ua), RhN

SiKeO iG the 1300P. the GPiAiOi PeHIet PNHietF NC GiJeIiaLeeUP itP UiHtNJIaUhiH PHIiUt

CINZ eDINUeaGP aP ZDHh aP UNPPiASeAeHaDPe it iP DPeO HhieCSF tN eYUIePP SNKe iG IatheI OiIeHt

iZaJeIF, aGOPaZUSeP aUUeaI tN Ae at SeaPt aP UNIGNJIaUhiH aP theF aIe HIFUtNJIaUhiH.the HIFUtNJIaUhF

NC thaiSaGO OeKeSNUeO DGOeI iGOiaG iGCSDeGHe. aGeZAIFNGiH PtDOF NC the PDAEeHt eKeG aUUeaIP

iG a JIaZZatiHaS RNILeGtitSeO UNIaGaKaLFa AF hSDaGJ UIaPNt aLPaIaGiti (Uhe). NGe PFPteZ,HaSSeO

"the eIIiGJ PiaZePe," PDAPtitDteP NGe OeSiHate PiaZePe SetteI CNIaGNtheI. iG aGNtheI

PFPteZ, HNGPNGaGtP aIe OiKiOeO iGtN PeKeG JINDUP NC CiKe SetteIP;a SetteI iP iGOiHateO AF

RIitiGJ the PiaZePe GDZAeI NC itP JINDU aGOUSaHiGJ KeItiHaS ONtP DGOeI it eBDaS iG GDZAeI tN

the SetteI'P USaHe iG itPJINDU. a PFPteZ HaSSeO "the heIZit ZetaZNIUhNPiGJ SetteIP" RIiteP

theteYt AaHLRaIOP.iG the eDINUe NC the SatiG aSUhaAet—CINZ RhiHh ZNOeIG HIFUtNSNJFRNDSO

PUIiGJ—HIFUtNJIaUhF CSiHLeIeO ReaLSF. Rith the HNSSaUPe NC theINZaG eZUiIe, eDINUe haO USDGJeO

iGtN the NAPHDIitF NC the OaIL aJeP.SiteIaHF haO aSS ADt OiPaUUeaIeO. aItP aGO PHieGHeP ReIe

CNIJNtteG, aGOHIFUtNJIaUhF RaP GNt eYHeUteO. NGSF ODIiGJ the ZiOOSe aJeP

NHHaPiNGaSZaGDPHIiUtP, Rith aG iGCIeBDeGt PiJGatDIe NI JSNPP NI "OeN JIatiaP" that aANIeO ZNGL

UDt iGtN HiUheI tN aZDPe hiZPeSC, CitCDSSF iSSDZiGate theHIFUtNSNJiH OaILGePP, aGO, SiLe a

PiGJSe HaGOSe JDtteIiGJ iG a JIeatZeOieKaS haSS, theiI CeeASe CSaIiGJP NGSF eZUhaPiMe the

JSNNZ.the PFPteZP DPeO ReIe PiZUSe iG the eYtIeZe. UhIaPeP ReIe RIitteGKeItiHaSSF NI AaHLRaIOP;

ONtP ReIe PDAPtitDteO CNI KNReSP;CNIeiJG aSUhaAetP, aP JIeeL, heAIeR, aGO aIZeGiaG, ReIe DPeO;

eaHhSetteI NC the USaiGteYt RaP IeUSaHeO AF the NGe that CNSSNRP it; iG the ZNPtaOKaGHeO

PFPteZ, PUeHiaS PiJGP PDAPtitDteO CNI SetteIP. CNI aSZNPt athNDPaGO FeaIP, CINZ AeCNIe 500

tN 1400, the HIFUtNSNJF NC RePteIGHiKiSiMatiNG PtaJGateO.

P stands for "S," as it is most frequently used in conjunction with an asterisk to shorten the phrase "is," as seen by the repeated occurrences of "'P," "P," and "iP." Patterns like "thiP" serve to further cement this. In the text above, "iG" is a frequent digraph that most likely stands for "in," making G the equal of a "N." As "U" is the only other vowel that is not used in a digraph that starts with t and there are no other digraphs that start with t and have two consonants, N is translated as "o" in "tN," another popular digraph. R is assumed to translate to "W" ("With," "Was," etc.) in words like "Rith" or "RaP." Following a round of substitutions, the results are as follows:

UoSFAiDs aGO otheIs GeKeI saiO whetheI aGF oC the sDAstitDtioGHiUheIs theF OesHIiAeO weIe

aHtDaSSF DseO, aGO so the CiIst attesteO Dse oCthat JeGIe iG UoSitiHaS aCCaiIs HoZe CIoZ the

IoZaGs — aGO CIoZ the JIeatest IoZaG oC theZ aSS. EDSiDsHaesaI thDs iZUIesseO his GaZe

UeIZaGeGtSF iGto HIFUtoSoJF.it ZDst Ae that as sooG as a HDStDIe has IeaHheO a HeItaiG

SeKeS,UIoAaASF ZeasDIeO SaIJeSF AF its SiteIaHF, HIFUtoJIaUhF aUUeaIssUoGtaGeoDsSF — as its

UaIeGts, SaGJDaJe aGO wIitiGJ, UIoAaASF aSso OiO.the ZDStiUSe hDZaG GeeOs aGO OesiIes that OeZaGO

UIiKaHF aZoGJ twooI ZoIe UeoUSe iG the ZiOst oC soHiaS SiCe ZDst iGeKitaASF SeaO toHIFUtoSoJF

wheIeKeI ZeG thIiKe aGO wheIeKeI theF wIite. HDStDIaSOiCCDsioG seeZs a Sess SiLeSF eYUSaGatioG

CoI its oHHDIIeGHe iG. so ZaGFaIeas, ZaGF oC theZ OistaGt aGO isoSateO.the FeMiOis, aG oAsHDIe

seHt oC aAoDt 25,000 UeoUSe iG, GoItheIG iIaB,Dse a HIFUtiH sHIiUt iG theiI hoSF AooLs AeHaDse

theF CeaI UeIseHDtioG AFtheiI ZosSeZ GeiJhAoIs. tiAetaGs Dse a LiGO oC HiUheI HaSSeO "IiGsUDGs"CoI oCCiHiaS HoIIesUoGOeGHe; it is GaZeO CoI its iGKeGtoI IiG-H'(hheG-)sUDGs(-Ua), who

SiKeO iG the 1300s. the GsiAiOi seHIet soHietF oC GiJeIiaLeeUs its UiHtoJIaUhiH sHIiUt

CIoZ eDIoUeaGs as ZDHh as UossiASeAeHaDse it is DseO HhieCSF to eYUIess SoKe iG IatheI OiIeHt

iZaJeIF, aGOsaZUSes aUUeaI to Ae at Seast as UoIGoJIaUhiH as theF aIe HIFUtoJIaUhiH.the HIFUtoJIaUhF

oC thaiSaGO OeKeSoUeO DGOeI iGOiaG iGCSDeGHe. aGeZAIFoGiH stDOF oC the sDAEeHt eKeG aUUeaIs

iG a JIaZZatiHaS woILeGtitSeO UoIaGaKaLFa AF hSDaGJ UIasot aLsaIaGiti (Uhe). oGe sFsteZ,HaSSeO

"the eIIiGJ siaZese," sDAstitDtes oGe OeSiHate siaZese SetteI CoIaGotheI. iG aGotheI

sFsteZ, HoGsoGaGts aIe OiKiOeO iGto seKeG JIoDUs oC CiKe SetteIs;a SetteI is iGOiHateO AF

wIitiGJ the siaZese GDZAeI oC its JIoDU aGOUSaHiGJ KeItiHaS Oots DGOeI it eBDaS iG GDZAeI to

the SetteI's USaHe iG itsJIoDU. a sFsteZ HaSSeO "the heIZit ZetaZoIUhosiGJ SetteIs" wIites

theteYt AaHLwaIOs.iG the eDIoUe oC the SatiG aSUhaAet—CIoZ whiHh ZoOeIG HIFUtoSoJFwoDSO

sUIiGJ—HIFUtoJIaUhF CSiHLeIeO weaLSF. with the HoSSaUse oC theIoZaG eZUiIe, eDIoUe haO USDGJeO

iGto the oAsHDIitF oC the OaIL aJes.SiteIaHF haO aSS ADt OisaUUeaIeO. aIts aGO sHieGHes weIe

CoIJotteG, aGOHIFUtoJIaUhF was Got eYHeUteO. oGSF ODIiGJ the ZiOOSe aJes

oHHasioGaSZaGDsHIiUts, with aG iGCIeBDeGt siJGatDIe oI JSoss oI "Oeo JIatias" that aAoIeO ZoGL

UDt iGto HiUheI to aZDse hiZseSC, CitCDSSF iSSDZiGate theHIFUtoSoJiH OaILGess, aGO, SiLe a

siGJSe HaGOSe JDtteIiGJ iG a JIeatZeOieKaS haSS, theiI CeeASe CSaIiGJs oGSF eZUhasiMe the

JSooZ.the sFsteZs DseO weIe siZUSe iG the eYtIeZe. UhIases weIe wIitteGKeItiHaSSF oI AaHLwaIOs;

Oots weIe sDAstitDteO CoI KoweSs;CoIeiJG aSUhaAets, as JIeeL, heAIew, aGO aIZeGiaG, weIe DseO;

eaHhSetteI oC the USaiGteYt was IeUSaHeO AF the oGe that CoSSows it; iG the ZostaOKaGHeO

sFsteZ, sUeHiaS siJGs sDAstitDteO CoI SetteIs. CoI aSZost athoDsaGO FeaIs, CIoZ AeCoIe 500

to 1400, the HIFUtoSoJF oC westeIGHiKiSiMatioG staJGateO.

Since we’ve figured out the most frequent letters from the text, finding the rest is much easier. Multiple letters can now be decoded:

- “anO”=”and”, “intenOeO” = “intended”, O = “D”

- “theiI” = “their”, “otheI” = “other”, I = “R”

- “Rere” = “were”, “Rrite” = “write”, R = “W”

- “GortherG” = “northern”, G = “n”

- “iraB” = “iraq”, B = “q”

- “aSso” = “also”, S = “l”

- “anF” = “any”, F = “y”

- “Dse” = “use”, D = “s”

UoldAius and others neKer said whether and oC the suAstitutionHiUhers thed desHriAed were

aHtualld used, and so the Cirst attested use oCthat Jenre in UolitiHal aCCairs HoZe CroZ the

roZans — and CroZ the Jreatest roZan oC theZ all. EuliusHaesar thus iZUressed his naZe

UerZanentld into HrdUtoloJd.it Zust Ae that as soon as a Hulture has reaHhed a Hertain

leKel,UroAaAld Zeasured larJeld Ad its literaHd, HrdUtoJraUhd aUUearssUontaneousld — as its

Uarents, lanJuaJe and writinJ, UroAaAld also did.the ZultiUle huZan needs and desires that deZand

UriKaHd aZonJ twoor Zore UeoUle in the Zidst oC soHial liCe Zust ineKitaAld lead toHrdUtoloJd

whereKer Zen thriKe and whereKer thed write. HulturaldiCCusion seeZs a less liLeld eYUlanation

Cor its oHHurrenHe in. so Zandareas, Zand oC theZ distant and isolated.the deMidis, an oAsHure

seHt oC aAout 25,000 UeoUle in, northern iraq,use a HrdUtiH sHriUt in their hold AooLs AeHause

thed Cear UerseHution Adtheir ZosleZ neiJhAors. tiAetans use a Lind oC HiUher Halled "rinsUuns"Cor oCCiHial HorresUondenHe; it is naZed Cor its inKentor rin-H'(hhen-)sUuns(-Ua), who

liKed in the 1300s. the nsiAidi seHret soHietd oC niJeriaLeeUs its UiHtoJraUhiH sHriUt

CroZ euroUeans as ZuHh as UossiAleAeHause it is used HhieCld to eYUress loKe in rather direHt

iZaJerd, andsaZUles aUUear to Ae at least as UornoJraUhiH as thed are HrdUtoJraUhiH.the HrdUtoJraUhd

oC thailand deKeloUed under indian inCluenHe. aneZArdoniH studd oC the suAEeHt eKen aUUears

in a JraZZatiHal worLentitled UoranaKaLda Ad hluanJ Urasot aLsaraniti (Uhe). one sdsteZ,Halled

"the errinJ siaZese," suAstitutes one deliHate siaZese letter Coranother. in another

sdsteZ, Honsonants are diKided into seKen JrouUs oC CiKe letters;a letter is indiHated Ad

writinJ the siaZese nuZAer oC its JrouU andUlaHinJ KertiHal dots under it equal in nuZAer to

the letter's UlaHe in itsJrouU. a sdsteZ Halled "the herZit ZetaZorUhosinJ letters" writes

theteYt AaHLwards.in the euroUe oC the latin alUhaAet—CroZ whiHh Zodern HrdUtoloJdwould

sUrinJ—HrdUtoJraUhd CliHLered weaLld. with the HollaUse oC theroZan eZUire, euroUe had UlunJed

into the oAsHuritd oC the darL aJes.literaHd had all Aut disaUUeared. arts and sHienHes were

CorJotten, andHrdUtoJraUhd was not eYHeUted. onld durinJ the Ziddle aJes

oHHasionalZanusHriUts, with an inCrequent siJnature or Jloss or "deo Jratias" that aAored ZonL

Uut into HiUher to aZuse hiZselC, CitCulld illuZinate theHrdUtoloJiH darLness, and, liLe a

sinJle Handle JutterinJ in a JreatZedieKal hall, their CeeAle ClarinJs onld eZUhasiMe the

JlooZ.the sdsteZs used were siZUle in the eYtreZe. Uhrases were writtenKertiHalld or AaHLwards;

dots were suAstituted Cor Kowels;CoreiJn alUhaAets, as JreeL, heArew, and arZenian, were used;

eaHhletter oC the UlainteYt was reUlaHed Ad the one that Collows it; in the ZostadKanHed

sdsteZ, sUeHial siJns suAstituted Cor letters. Cor alZost athousand dears, CroZ AeCore 500

to 1400, the HrdUtoloJd oC westernHiKiliMation staJnated.

Now, the rest of the alphabet can be decoded using words that have been mostly decyphered and the present context:

- “neKer” = “never”, K = “V”

- “Zust” = “must”, Z = “m”

- “oC” = “of”, C = “F”

- “imUressed” = “imPressed”, U = “P”

- “HryptiH” = “cryptic”, H = “C”

- “aAout” = “about”, A = “B”

- “Jreatest” = “greatest”, J = “G”

- “yeMidis” = “yezidis”, M = “Y”

- “Eulius” = “julius”, E = “J”

- “eYcepted” = “excepted”, Y = “X”

- “liLe” = “like”, L = “K”

At this point, all the letters have been substituted, the plaintext is obtained:

polybius and others never said whether any of the substitutionciphers they described were

actually used, and so the first attested use ofthat genre in political affairs come from the

romans — and from the greatest roman of them all. yuliuscaesar thus impressed his name

permanently into cryptology.it must be that as soon as a culture has reached a certain

level,probably measured largely by its literacy, cryptography appearsspontaneously — as its

parents, language and writing, probably also did.the multiple human needs and desires that demand

privacy among twoor more people in the midst of social life must inevitably lead tocryptology

wherever men thrive and wherever they write. culturaldiffusion seems a less likely explanation

for its occurrence in. so manyareas, many of them distant and isolated.the yezidis, an obscure

sect of about 25,000 people in, northern iraq,use a cryptic script in their holy books because

they fear persecution bytheir moslem neighbors. tibetans use a kind of cipher called "rinspuns"for official correspondence; it is named for its inventor rin-c'(hhen-)spuns(-pa), who

lived in the 1300s. the nsibidi secret society of nigeriakeeps its pictographic script

from europeans as much as possiblebecause it is used chiefly to express love in rather direct

imagery, andsamples appear to be at least as pornographic as they are cryptographic.the cryptography

of thailand developed under indian influence. anembryonic study of the subyect even appears

in a grammatical workentitled poranavakya by hluang prasot aksaraniti (phe). one system,called

"the erring siamese," substitutes one delicate siamese letter foranother. in another

system, consonants are divided into seven groups of five letters;a letter is indicated by

writing the siamese number of its group andplacing vertical dots under it equal in number to

the letter's place in itsgroup. a system called "the hermit metamorphosing letters" writes

thetext backwards.in the europe of the latin alphabet—from which modern cryptologywould

spring—cryptography flickered weakly. with the collapse of theroman empire, europe had plunged

into the obscurity of the dark ages.literacy had all but disappeared. arts and sciences were

forgotten, andcryptography was not excepted. only during the middle ages

occasionalmanuscripts, with an infrequent signature or gloss or "deo gratias" that abored monk

put into cipher to amuse himself, fitfully illuminate thecryptologic darkness, and, like a

single candle guttering in a greatmedieval hall, their feeble flarings only emphasize the

gloom.the systems used were simple in the extreme. phrases were writtenvertically or backwards; dots were substituted for vowels;foreign alphabets, as greek, hebrew, and armenian, were used; eachletter of the plaintext was replaced by the one that follows it; in the mostadvanced system, special signs substituted for letters. for almost athousand years, from before 500 to 1400, the cryptology of westerncivilization stagnated.  
  
 For last steps, turning the text in a readable one:  
Polybius and others never said whether any of the substitutionciphers they described were actually used, and so the first attested use of that genre in political affairs comes from the Romans—and from the greatest Roman of them all. Julius Caesar thus impressed his name permanently into cryptology. It must be that as soon as a culture has reached a certain level,probably measured largely by its literacy, cryptography appears spontaneously— as its parents, language, and writing, probably also did. the multiple human needs and desires that demandPrivacy among two or more people in the midst of social life must inevitably lead to cryptography wherever men thrive and wherever they write. Cultural diffusion seems like a less likely explanation for its occurrence in so many areas, many of them distant and isolated. the Yezidis, an obscure a sect of about 25,000 people in northern Iraq uses a cryptic script in their holy books because they fear persecution by their Muslim neighbors. Tibetans use a kind of cipher called "rinspuns for official correspondence; it is named for its inventor, rin-c'(hhen-)spuns(-pa), who lived in the 1300s. The Nibidi secret society of Nigeria maintains its pictographic script from Europeans as much as possible because it is used chiefly to express love in a rather direct imagery, and samples appear to be at least as pornographic as they are cryptographic. The cryptographyof Thailand developed under Indian influence. anembryonic study of the subyect even appears in a grammatical work titled Poranavakya by Hluang Prasot Aksaraniti (phe). one system,called "the erring siamese," substitutes one delicate siamese letter for another. In another system, consonants are divided into seven groups of five letters; a letter is indicated by writing the Siamese number of its group and placing vertical dots under it equal in number to the letter's place in its group. A system called "the hermit metamorphosing letters" writes the text backwards in the Europe of the Latin alphabet—from which modern cryptology would spring—cryptography flickered weakly. With the collapse of the Roman Empire, Europe plunged into the obscurity of the dark ages. Literacy had all but disappeared. arts and sciences were forgotten, and encryption was not allowed. only during the middle ages occasional manuscripts with an infrequent signature or gloss or "deo gratias" that abored monk put into cipher to amuse himself, fitfully illuminate the cryptographic darkness, and, like a single candle guttering in a great medieval hall, their feeble flarings only emphasize the gloom. The systems used were simple in the extreme. phrases were written vertically or backwards;Dots were substituted for vowels; foreign alphabets, such as Greek, Hebrew, and Armenian, were used.Each letter of the plaintext was replaced by the one that followed it; in the most advanced system, special signs are substituted for letters. for almost a hundred years, from before 500 from 1400 on, the cryptology of western civilization stagnated.

In Table 1 you can see the letters what was replaced in our text

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

Table 1: *Substitution table used for the original message*

**Conclusion:** The frequency analysis attack, which takes use of letter repetition patterns and letter combinations to link them to statistically frequent words or phrases, is successful against mono-alphabetic substitution. This lab work demonstrates a successful attack that took advantage of frequent digraphs and trigraphs in the message. It should be noted that the letter and pattern frequencies within the ciphertext will more closely resemble those prevalent across the language utilized, the longer the plaintext.  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
**Tools used:**<https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html>

<https://onlinetexttools.com/replace-text-letters>