Ministry of Education of Republic of Moldova

Technical University of Moldova

Faculty of Computers, Informatics and Microelectronics

Software Engineering Department

Cryptography and Security

Laboratory work #2

Variant 12

Cryptoanalysis of monoalphabetic ciphers

Author: Timur Cravtov
std. gr. FAF-231

Verified by: Maia Zaica
asist. univ

Chișinău
2025

1 Frequency analysis

One of the improvments of Caesar cipher is the use of monoalphabetic substitution cipher, where each letter of the plaintext is replaced by a corresponding letter of the ciphertext alphabet. The ciphertext alphabet is a permutation of the plaintext alphabet. WHile Caesar cipher only shifts the alphabet by a fixed number, monoalphabetic substitution cipher can use any permutation of the alphabet, giving 26! possible keys.

There is a well-known method of breaking monoalphabetic substitution ciphers called frequency analysis. The idea behind frequency analysis is that in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies. For example, in the English language, the letter 'E' is the most frequently used letter, followed by 'T', 'A', 'O', 'I', and 'N' [2]. By analyzing the frequency of letters in the ciphertext and comparing them to known frequencies in the target language, one can make educated guesses about which ciphertext letters correspond to which plaintext letters.

2 Implementation of frequency analysis attack on monoalphabetic substitution cipher

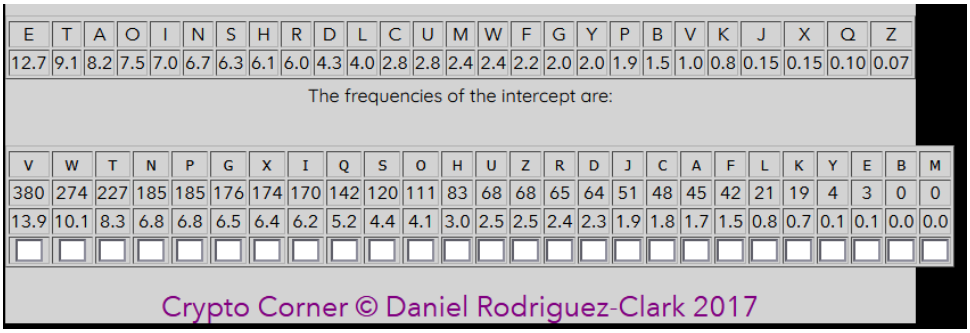
For the frequncy analysis and guessed substitutions I used an online tool [3]. The ciphertext that I had to decrypt corresponding to my variant is the following:

XW ITG RXWQ TSZNPW DGAVSXVKTASV VCCXHXVGHF. WQV ATJP NC ZTXS CNI OVSXKVIFWQTW ZNIGXGJ WN WQV VZATPPXVP XG KXVGGT RVIV AINDJQW WN WQV ASTHLHQTZAVI VTHQ OTF TW 7 T.Z. WQVIV WQV SVWWVIP RVIV NUVGVO AF ZVSWXGJWQVXI PVTSP RXWQ T HTGOSV. WQV NIOVI NC WQV SVWWVIP XG TG VGKVSNUV RTPGNWVO TGO WQV SVWWVIP JXKVG WN T PDAOXIVHWNI. QV IVTO WQVZ TGO NIOVIVOWQV XZUNIWTGW UTIWP HNUXVO. TSS WQV VZUSNFVVP HNDSO RIXWV ITUXOSF, TGOPNZV LGVR PQNIWQTGO. SNGJ SVWWVIP RVIV OXHWTWVO WN PTKV WXZV,PNZVWXZVP DPXGJ CNDI PWVGNJITUQVIP WN T PXGJSV SVWWVI. XC T SVWWVI RTP XG TSTGJDTJV WQTW QV OXO GNW LGNR, WQV PDAOXIVHWNI JTKV XW WN T HTAXGVWVZUSNFVV CTZXSXTI RXWQ XW. WRN WITGPSTWNIP RVIV TSRTFP NG QTGO. TSSVDINUVTG STGJDTJVP HNDSO AV IVTO, TGO RQVG T GVR NGV RTP GVVOVO, TGNCCXHXTS SVTIGVO XW. TIZVGXTG, CNI VYTZUSV, WNNL NGV HTAXGVW UNSFJSNW NGSFT CVR ZNGWQP WN SVTIG, TGO QV RTP UTXO WQV DPDTS 500 CSNIXGP CNI QXP GVRLGNRSVOJV. TCWVI HNUFXGJ, WQV SVWWVIP RVIV IVUSTHVO XG WQVXI VGKVSNUVP XGWQVXI NIXJXGTS NIOVI TGO WQV VGKVSNUVP

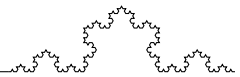
IV-PVTSVO, DPXGJ CNIJVO PVTSP WNXZUIVPP WQV NIXJXGTS RTY. WQV SVWWVIP RVIV IVWDIGVO WN WQV UNPW NCCXHV AF9:30 T.Z.TW 10 T.Z., WQV ZTXS WQTW RTP UTPPXGJ WQINDJQ WQXP HINPPINTOP NC WQVH-NGWXGVGW TIIXKVO TGO RTP QTGOSVO XG WQV PTZV RTF, WQNDJQ RXWQ SVPPQDIIF AVHTDPV XW RTP XG WITGPXW. DPDTSSF XW RNDSO AV ATHL XG WQV UNPW AF 2U.Z., WQNDJQ PNZVWXZVP XW RTP LVUW TP STWV TP 7 U.Z. TW 11 T.Z.,XGWVIHVUWXNGP ZTOV AF WQV UNSXHV CNI UDIUNPVP NC UNSXWXHTS PDIKVXSSTGHVTIIXKVO. TGO TW 4 U.Z., WQV HNDIXVIP AINDJQW WQV SVWWVIP WQTW WQVVZATPPXVP RVIV PVGOXGJ NDW WQTW OTF. WQVPV RVIV ATHL XG WQV PWIVTZ NCHNZ-ZDGXHTWXNGP AF 6:30 U.Z. HNUXVO ZTWVIXTS RTP QTGOVO WN WQVOX-IVHWNI NC WQV HTAXGVW, RQN VYHVIUWVO XGCNIZTWXNG NC PUVHXTS XGWVIVPW TGOINDWVO XW WN WQV UINUVI TJVGHXVP, TP UNSXHV, TIZF, NI ITXSRTFTOZXGXPWITWXNG, TGO PVGW WQV ZTPP NC OXUSNZTWXH ZTWVIXTS WN WQV HNDIW. TSS WNSO, WQV WVG-ZTG HTAXGVW QTGOSVO TG TKVITJV NCAVWRVVG 80 TGO 100 SVWWVIP T OTF.TPWNGXPQXGJSF, WQVXI GXZASV CXGJVIP QTIOSF VKVI PWDCCVO SVWWVIP XGWN WQVRINGJ UTHLVW, OVPUXWV WQV PUVVO RXWQ RQXHQ WQVF RNILVO. XG NGV NC WQVCVR IVHNIOVO ASDGOVIP, TG XGWVIHVUWVO SVWWVI WN WQV ODLV NC ZNOVGT RTPVIINGVNDPSF IV-PVTSVO RXWQ WQV HSNPVSF PXZXSTI PXJGVW NC UTIZT. RQVG WQVODLV GNWXHVO WQV PDAPWXWDWXNG, QV PVGW XW WN UTIZT RXWQ WQV RIF GNWV, "GNWEDPW ZV—FND WNN." ANWQ PWTWVP UINWVPWVO, ADW WQV KXVGGVPV JIVVWVO WQVZRXWQ T ASTGL PWTIV, T PQIDJ, TGO T ASTGO UINCVPPXNG NC XJGNITGHV. OVPUXWVWQXP, WQV VYXPWVGHV NC WQV ASTHL HQTZAVI RTP RVSS LGNRG WN WQV KTIXNDPOVSVJTWVP WN WQV TDPWIXTG HNDIW, TGO RTP VKVG WTHXWSF THLGNRSVOJVO AFWQV TDPWIXTGP. RQVG WQV AIXWXPQ'TZATPPTONI HNZUSTXGVO QDZNINDPSF WQTW QV RTP JVWWXGJ HNUXVPXGPWVTO NC QXP NIXJXGTS HNIIVPUNGOVGHV, WQV HQTGHVSSNI IVUSXVO HNNSSF,"QNR HSDZPF WQVPV UVNUSV TIV!"VGHXUQVIVO HNI-IVPUNGOVGHV RTP PDAEVHWVO WN WQV DPDTS HIFUWTGTSFWXHPRVTWXGJ UINHVPP. WQV KXVGGVPV VGENFVO IVZTILTASV PDHHVPP XG WQXP RNIL.WQV CIVGHQ TZATPPTONI, RQN RTP TUUIXPVO NC XWP PDHHVPPVP CINZ UTU-VIPPNSO QXZ AF T ZTPLVO ZTG NG T AIXOJV, IVZTILVO XG TPWNGX-PQZVGW WQTW"NDI HXUQVIP NC 1200 [JINDUP] QNSO NDW NGSF T SXWWSV RQXSV TJTXGPW WQVTAXSXWF NC WQV TDPWIXTG OVHXUQVIVIP." QV TOOVO WQTW WQNDJQ QV PDJJVPWVOGVR RTFP NC HXUQVIXGJ TGO HNGWXGDTS HQTGJVP NC HXUQVIP, "X PWXSS CXGOZFPVSC RXWQNDW

PVHDIV ZVTGP CNI WQV PVHIVWP X QTKV WN WITGPZXW WNHNGPWTGWXGNUSV, PWNHLQNSZ, TGO PW. UVWVIPADIJ."

In image below we see that the most used letters are V, W, T. Let's make a substitition for letter E, T, A repectively.



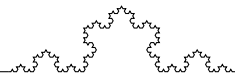
Xt IaG RXtQ aSZNPt DGAeSXeKaASe eCCXHXeGHF. tQe AaJP NC ZaXS CNI OeSXKeIFtQat ZNIGXGJ tN tQe eZAaPPXeP XG KXeGGa ReIe AINDJQt tN tQe ASaHLHQaZAeI eaHQ OaF at 7 a.Z. tQeIe tQe SetteIP ReIe NUeGeO AF ZeStXGJtQeXI PeaSP RXtQ a HaGOSe. tQe NIOeI NC tQe SetteIP XG aG eGKeSNUe RaPGNteO aGO tQe SetteIP JXKeG tN a PDAOXIeHtNI. Qe IeaO tQeZ aGO NIOeIeOtQe XZUNItaGt UaItP HNUXeO. aSS tQe eZUSNFeeP HNDSO RIXte IaUXOSF, aGOPNZe LGeR PQNItQaGO. SNGJ SetteIP ReIe OXHtateO tN PaKe tXZe,PNZetXZeP DPXGJ CNDI PteGNJIaUQeIP tN a PXGJSe SetteI. XC a SetteI RaP XG aSaGJDaJe tQat Qe OXO GNt LGNR, tQe PDAOXIeHtNI JaKe Xt tN a HaAXGeteZUSNFee CaZXSXaI RXtQ Xt. tRN tIaGPSatNIP ReIe aSRaFP NG QaGO. aSSeDINUeaG SaGJDaJeP HNDSO Ae IeaO, aGO RQeG a GeR NGe RaP GeeOeO, aGNCCXHXaS SeaIGeO Xt. aIZeGXaG, CNI eYaZUSe, tNNL NGe HaAXGet UNSFJSNt NGSFa CeR ZNGtQP tN SeaIG, aGO Qe RaP UaXO tQe DPDaS 500 CSNIXGP CNI QXP GeRLGNRSeOJe. aCteI HNUFXGJ, tQe SetteIP ReIe IeUSaHeO XG tQeXI eGKeSNUeP XGtQeXI NIXJXGaS NIOeI aGO tQe eGKeSNUeP Ie-PeaSeO, DPXGJ CNIJeO PeaSP tNXZUIePP tQe NIXJXGaS RaY. tQe SetteIP ReIe IetDIGeO tN tQe UNPt NCCXHe AF9:30 a.Z.at 10 a.Z., tQe ZaXS tQat RaP UaPPXGJ tQINDJQ tQXP HINPPINaOP NC tQeHNGtXGeGt aIIXKeO aGO RaP QaGOSeO XG tQe PaZe RaF, tQNDJQ RXtQ SePPQDIIF AeHaDPe Xt RaP XG tIaGPXt. DPDaSSF Xt RNDSO Ae AaHL XG tQe UNPt AF 2U.Z., tQNDJQ PNZetXZeP Xt RaP LeUt aP Sate aP 7 U.Z. at 11 a.Z.,XGteIHeUtXNGP ZaOe AF tQe UNSXHe CNI UDIUNPeP NC UNSXtXHaS PDIKeXSSaGHeaIIXKeO. aGO at 4 U.Z., tQe HNDIXeIP AINDJQt tQe SetteIP tQat tQeeZAaPPXeP ReIe PeGOXGJ NDt tQat OaF. tQePe ReIe AaHL XG tQe PtIeaZ NCHNZZDGXHatXNGP AF 6:30 U.Z. HNUXeO ZateIXaS RaP QaGOeO tN tQeOXIeHtNI NC tQe HaAXGet, RQN eYHeIUteO XGCNIZatXNG NC PUeHXaS XGteIePt aGOINDteO Xt tN tQe UINUeI aJeGHXeP, aP UNSXHe, aIZF, NI IaXSRaFaOZXGXPtIatXNG, aGO PeGt tQe



ZaPP NC OXUSNZatXH ZateIXaS tN tQe HNDIt. aSS tNSO, tQe teG-ZaG HaAXGet QaGOSeO aG aKeIaJe NCAetReeG 80 aGO 100 SetteIP a OaF.aPtNGXPQXGJSF, tQeXI GXZASe CXGJeIP QaIOSF eKeI PtDCCeO SetteIP XGtN tQeRINGJ UaHLet, OePUXte tQe PUeeO RXtQ RQXHQ tQeF RNILeO. XG NGe NC tQeCeR IeHNIOeO ASDGOeIP, aG XGteIHeUteO SetteI tN tQe ODLe NC ZNOeGa RaPeIINGeNDPSF IePeaSeO RXtQ tQe HSNPeSF PXZXSaI PXJGet NC UaIZa. RQeG tQeODLe GNtXHeO tQe PDAPtXtDtXNG, Qe PeGt Xt tN UaIZa RXtQ tQe RIF GNte, "GNtEDPt Ze—FND tNN." ANtQ PtateP UINtePteO, ADt tQe KXeGGePe JIeeteO tQeZRXtQ a ASaGL PtaIe, a PQIDJ, aGO a ASaGO UINCePPXNG NC XJGNIaGHe. OePUXtetQXP, tQe eYXPteGHe NC tQe ASaHL HQaZAeI RaP ReSS LGNRG tN tQe KaIXNDPOeSeJateP tN tQe aDPtIXaG HNDIt, aGO RaP eKeG taHXtSF aHLGNRSeOJeO AFtQe aDPtIXaGP. RQeG tQe AIXtXPQ'aZAaPPaONI HNZUSaXGeO QDZNINDPSF tQat Qe RaP JettXGJ HNUXePXGPteaO NC QXP NIXJXGaS HNIIePUNGOeGHe, tQe HQaGHeSSNI IeUSXeO HNNSSF,"QNR HSDZPF tQePe UeNUSe aIe!"eGHXUQeIeO HNIIePUNGOeGHe RaP PDAEeHteO tN tQe DPDaS HIFUtaGaSFtXHPReatXGJ UINHePP. tQe KXeGGePe eGENFeO IeZaILaASe PDHHePP XG tQXP RNIL.tQe CIeGHQ aZAaPPaONI, RQN RaP aUUIXPeO NC XtP PDHHePPeP CINZ UaUeIPPNSO QXZ AF a ZaPLeO ZaG NG a AIXOJe, IeZaILeO XG aPtNGXPQZeGt tQat"NDI HXUQeIP NC 1200 [JINDUP] QNSO NDt NGSF a SXttSe RQXSe aJaXGPt tQeaAXSXtF NC tQe aDPtIXaG OeHXUQeIeIP." Qe aOOeO tQat tQNDJQ Qe PDJJePteOGeR RaFP NC HXUQeIXGJ aGO HNGtXGDaS HQaGJeP NC HXUQeIP, "X PtXSS CXGOZFPeSC RXtQNDt PeHDIe ZeaGP CNI tQe PeHIetP X QaKe tN tIaGPZXt tNHNGPtaGtXGNUSe, PtNHLQNSZ, aGO Pt. UeteIPADIJ."

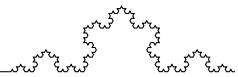
Apparently, the certain words are readable. For example, there is a word "at" and time unit next to it, so we can assume that in "7 a.Z" z is for M. Similarly, we have in the text "7 U.Z" which might mean "U" is for "P". Next, we see use of words "tN" and "tQe, which suggests "N" is for "O" and "Q" is for "H". Let's make these substitutions and see what we get:

Xt IaG RXth aSmout DGAeSXeKaASe eCCXHXeGHF. the AaJu oC maXS CoI OeSXKeIFthat moIGXGJ to the emAauuXeu XG KXeGGa ReIe AIoDJht to the ASaHLHhamAeI eaHh OaF at 7 a.m. theIe the SetteIu ReIe oUeGeO AF meStXGJtheXI ueaSu RXth a HaGOSe. the oIOeI oC the SetteIu XG aG eGKeSoUe RauGoteO aGO the SetteIu JXKeG to a uDAOXIeHtoI. he IeaO them aGO oIOeIeOthe XmUoItaGt UaItu HoUXeO. aSS the emUSoFeeu HoDSO RIXte IaUXOSF, aGOuome LGeR uhoIthaGO. SoGJ SetteIu ReIe OXHtateO to uaKe tXme,uometXmeu DuXGJ CoDI uteGoJIaUheIu to a uXGJSe SetteI. XC a SetteI Rau XG aSaGJDaJe that he OXO Got LGoR, the uDAOXIeHtoI JaKe Xt to a HaAXGetemUSoFee CamXSXaI RXth Xt. tRo tIaGuSatoIu ReIe aSRaFu oG haGO. aSSeDIoUeaG SaGJDaJeu HoDSO Ae IeaO, aGO RheG a GeR



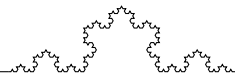
oGe Rau GeeOeO, aGoCCXHXaS SeaIGeO Xt. aImeGXaG, CoI eYamUSe, tooL oGe HaAXGet UoSFJSot oGSFa CeR moGthu to SeaIG, aGO he Rau UaXO the DuDaS 500 CSoIXGu CoI hXu GeRLGoRSeOJe. aCteI HoUFXGJ, the SetteIu ReIe IeUSaHeO XG theXI eGKeSoUeu XGtheXI oIXJXGaS oIOeI aGO the eGKeSoUeu Ie-ueaSeO, DuXGJ CoIJeO ueaSu toXmUIeuu the oIXJXGaS RaY. the SetteIu ReIe IetDIGeO to the Uout oCCXHe AF9:30 a.m.at 10 a.m., the maXS that Rau UauuXGJ thIoDJh thXu HIouuIoaOu oC theHoGtXGeGt aIIXKeO aGO Rau haGOSeO XG the uame RaF, thoDJh RXth SeuuhDIIF AeHaDue Xt Rau XG tIaGuXt. DuDaSSF Xt RoDSO Ae AaHL XG the Uout AF 2U.m., thoDJh uometXmeu Xt Rau LeUt au Sate au 7 U.m. at 11 a.m.,XGteIHeUtXoGu maOe AF the UoSXHe CoI UDIUoueu oC UoSXtXHaS uDIKeXSSaGHeaIIXKeO. aGO at 4 U.m., the HoDIXeIu AIoDJht the SetteIu that theemAauuXeu ReIe ueGOXGJ oDt that OaF. theue ReIe AaHL XG the utIeam oCHommDGXHatXoGu AF 6:30 U.m. HoUXeO mateIXaS Rau haGOeO to theOXIeHtoI oC the HaAXGet, Rho eYHeIUteO XGCoImatXoG oC uUeHXaS XGteIeut aGOIoDteO Xt to the UIoUeI aJeGHXeu, au UoSXHe, aImF, oI IaXSRaFaOmXGXutIatXoG, aGO ueGt the mauu oC OXUSomatXH mateIXaS to the HoDIt. aSS toSO, the teG-maG HaAXGet haGOSeO aG aKeIaJe oCAetReeG 80 aGO 100 SetteIu a OaF.autoGXuhXGJSF, theXI GXmASe CXGJeIu haIOSF eKeI utDCCeO SetteIu XGto theRIoGJ UaHLet, OeuUXte the uUeeO RXth RhXHh theF RoILeO. XG oGe oC theCeR IeHoIOeO ASDGOeIu, aG XGteIHeUteO SetteI to the ODLe oC moOeGa RaueIIoGeoDuSF Ie-ueaSeO RXth the HSoueSF uXmXSaI uXJGet oC UaIma. RheG theODLe GotXHeO the uDAutXtDtXoG, he ueGt Xt to UaIma RXth the RIF Gote, "GotEDut me—FoD too." Aoth utateu UIoteuteO, ADt the KXeGGeue JIeeteO themRXth a ASaGL utaIe, a uhIDJ, aGO a ASaGO UIoCeuuXoG oC XJGoIaGHe. OeuUXtethXu, the eYXuteGHe oC the ASaHL HhamAeI Rau ReSS LGoRG to the KaIXoDuOeSeJateu to the aDutIXaG HoDIt, aGO Rau eKeG taHXtSF aHLGoRSeOJeO AFthe aDutIXaGu. RheG the AIXtXuh'amAauuaOoI HomUSaXGeO hDmoIoDuSF that he Rau JettXGJ HoUXeuXGuteaO oC hXu oIXJXGaS HoIIeuUoGOeGHe, the HhaGHeSSoI IeUSXeO HooSSF,"hoR HSDmuF theue UeoUSe aIe!"eGHXUheIeO HoIIeuUoGOeGHe Rau uDAEeHteO to the DuDaS HIFUtaGaSFtXHuReatXGJ UIoHeuu. the KXeGGeue eGEoFeO IemaILaASe uDHHeuu XG thXu RoIL.the CIeGHh amAauuaOoI, Rho Rau aUUIXueO oC Xtu uDHHeuueu CIom UaUeIuuoSO hXm AF a mauLeO maG oG a AIXOJe, IemaILeO XG autoGXuhmeGt that"oDI HXUheIu oC 1200 [JIoDUu] hoSO oDt oGSF a SXttSe RhXSe aJaXGut theaAXSXtF oC the aDutIXaG OeHXUheIeIu." he aOOeO that thoDJh he uDJJeuteOGeR RaFu oC HXUheIXGJ aGO HoGtXGDaS HhaGJeu oC HXUheIu, "X utXSS CXGOmFueSC RXthoDt ueHDIe meaGu CoI the ueHIetu X haKe to tIaGumXt toHoGutaGtXGoUSe, utoHLhoSm, aGO ut. UeteIuADIJ."

New words appear which suggest is was a right substitition. Now let's find new



words: ”eaHh” - ”each”, ”H” is for ”C” ”theIe” - ”there”, ”I” is for ”r”

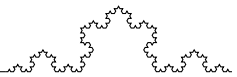
Xt raG RXth aSmoPt DGAeSXeKaASe eCCXcXeGcF. the AaJP oC maXS Cor OeSXKerFthat morGXGJ to the emAaPPXeP XG KXeGGa Rere AroDJht to the ASacLchamAer each OaF at 7 a.m. there the SetterP Rere opeGeO AF meStXGJtheXr PeaSP RXth a caGOSe. the orOer oC the SetterP XG aG eGKeSope RaPGoteO aGO the SetterP JXKeG to a PDAOXrector. he reaO them aGO orOereOthe XmportaGt partP copXeO. aSS the empSoFeeP coDSO RrXte rapXOSF, aGOPome LGeR PhorthaGO. SoGJ SetterP Rere OXctateO to PaKe tXme,PometXmeP DPXGJ CoDr PteGoJrapherP to a PXGJSe Setter. XC a Setter RaP XG aSaGJDaJe that he OXO Got LGoR, the PDAOXrector JaKe Xt to a caAXGetempSoFee CamXSXar RXth Xt. tRo traGPSatorP Rere aSRaFP oG haGO. aSSeDropeaG SaGJDaJeP coDSO Ae reaO, aGO RheG a GeR oGe RaP GeeOeO, aGoCCXcXaS SearGeO Xt. armeGXaG, Cor eYampSe, tooL oGe caAXGet poSFJSot oGSFa CeR moGthP to SearG, aGO he RaP paXO the DPDaS 500 CSorXGP Cor hXP GeRLGoRSeOJe. aCter copFXGJ, the SetterP Rere repSaceO XG theXr eGKeSopeP XGtheXr orXJXGaS orOer aGO the eGKeSopeP re-PeaSeO, DPXGJ CorJeO PeaSP toXmprePP the orXJXGaS RaY. the SetterP Rere retDrGeO to the poPt oCCXce AF9:30 a.m.at 10 a.m., the maXS that RaP paPPXGJ throDJh thXP croP-ProaOP oC thecoGtXGeGt arrXKeO aGO RaP haGOSeO XG the Pame RaF, thoDJh RXth SePPhDrrF AecaDPe Xt RaP XG traGPXt. DPDaSSF Xt RoDSO Ae AacL XG the poPt AF 2p.m., thoDJh PometXmeP Xt RaP Lept aP Sate aP 7 p.m. at 11 a.m.,XGterceptXoGP maOe AF the poSXce Cor pDrpoPeP oC poSXtXcaS PDrKeXS-SaGcearrXKeO. aGO at 4 p.m., the coDrXerP AroDJht the SetterP that theemAaPPXeP Rere PeGOXGJ oDt that OaF. thePe Rere AacL XG the Ptream oCcommDGXcatX-oGP AF 6:30 p.m. copXeO materXaS RaP haGOeO to theOXrector oC the caAXGet, Rho eYcerpteO XGCormatXoG oC PpecXaS XGterePt aGOroDteO Xt to the proper aJeGcXeP, aP poSXce, armF, or raXSRaFaOmXGXPtratXoG, aGO PeGt the maPP oC OXpSomatXc materXaS to the coDrt. aSS toSO, the teG-maG caAXGet haGOSeO aG aKeraJe oCAetReeG 80 aGO 100 SetterP a OaF.aPtoGXPhXGJSF, theXr GX-mASe CXGJerP harOSF eKer PtDCCeO SetterP XGto theRroGJ pacLet, OePpXte the PpeeO RXth RhXch theF RorLeO. XG oGe oC theCeR recorOeO ASDGOerP, aG XGter-cepteO Setter to the ODLe oC moOeGa RaPerroGeoDPSF re-PeaSeO RXth the cSoPeSF PXmXSar PXJGet oC parma. RheG theODLe GotXceO the PDAPtXtDtXoG, he PeGt Xt to parma RXth the RrF Gote, ”GotEDPt me—FoD too.” Aoth PtateP protePteO, ADt the KXeGGePe JreeteO themRXth a ASaGL Ptare, a PhrDJ, aGO a ASaGO pro-CePPXoG oC XJGoraGce. OePpXtethXP, the eYXPteGce oC the ASacL chamAer RaP ReSS LGoRG to the KarXoDPOeSeJateP to the aDPtrXaG coDrt, aGO RaP eKeG tacXtSF acLGoRSeOJeO AFthe aDPtrXaGP. RheG the ArXtXPh’amAaPPaOor comp-SaXGeO hDmoroDPSF that he RaP JettXGJ copXePXGPteaO oC hXP orXJXGaS cor-



rePpoGOeGce, the chaGceSSor repSXeO cooSSF,"hoR cSDmPF thePe peopSe are!"eGcXphereO correPpoGOeGce RaP PDAEecteO to the DPDaS crFptaGaSFtXcPReatXGJ procePP. the KXeGGePe eGEoFeO remarLaASe PDccePP XG thXP RorL.the CreGch amAaPPaOor, Rho RaP apprXPeO oC XtP PDccePPeP Crom paperPPoSO hXm AF a maPLeO maG oG a ArXOJe, remarLeO XG aPtoGXPhmeGt that"oDr cXpherP oC 1200 [JroDpP] hoSO oDt oGSF a SXttSe RhXSe aJaXGPt theaAXSXtF oC the aDPtrXaG OecXpherP." he aOOeO that thoDJh he PDJJePteOGeR RaFP oC cXpherXGJ aGO coGtXGDaS chaGJeP oC cXpherP, "X PtXSS CXGOmFPeSC RXthoDt PecDre meaGP Cor the PecretP X haKe to traGPmXt tocoGPtaGtXGopSe, PtocLhoSm, aGO Pt. peterPADrJ."

Next words: "XmprotaGt" - "important", "X" is for "I", "G" is for "n". Also, we see some verb-like words like "reaO", "orOereO" which means "O" is for "D

it ran Rith aSmoPt DnAeSieKaASe eCCiciencF. the AaJP oC maiS Cor deSiKerFthat morninJ to the emAaPPieP in Kienna Rere AroDJht to the ASacLchamAer each daF at 7 a.m. there the SetterP Rere opened AF meStinJtheir PeaSP Rith a candSe. the order oC the SetterP in an enKeSope RaPnoted and the SetterP JiKen to a PDAdirector. he read them and orderedthe important partP copied. aSS the empSoFeeP coDSd Rrite rapidSF, andPome LneR Phorthand. SonJ SetterP Rere dictated to PaKe time,PometimeP DPinJ CoDr PtenoJrapherP to a PinJSe Setter. iC a Setter RaP in aSanJDaJe that he did not LnoR, the PDAdirector JaKe it to a caAinetempSoFee CamiSiar Rith it. tRo tranPSatorP Rere aSRaFP on hand. aSSeDropean SanJDaJeP coDSd Ae read, and Rhen a neR one RaP needed, anoCCiciaS Searned it. armenian, Cor eYampSe, tooL one caAinet poSFJSot onSFa CeR monthP to Searn, and he RaP paid the DPDaS 500 CSorinP Cor hiP neRLnoRSedJe. aCter copFinJ, the SetterP Rere repSaced in their enKeSopeP intheir oriJinaS order and the enKeSopeP re-PeaSed, DPinJ CorJed PeaSP toimprePP the oriJinaS RaY. the SetterP Rere retDrned to the poPt oCCice AF9:30 a.m.at 10 a.m., the maiS that RaP paPPinJ throDJh thiP croPProadP oC thecontinent arriKed and RaP handSed in the Pame RaF, thoDJh Rith SePPhDrrF AecaDPe it RaP in tranPit. DPDaSSF it RoDSd Ae AacL in the poPt AF 2p.m., thoDJh PometimeP it RaP Lept aP Sate aP 7 p.m. at 11 a.m.,interceptionP made AF the poSice Cor pDrpoPeP oC poSiticaS PDrKeiSSancearriKed. and at 4 p.m., the coDrierP AroDJht the SetterP that theemAaPPieP Rere PendinJ oDt that daF. thePe Rere AacL in the Ptream oCcommDnicationP AF 6:30 p.m. copied materiaS RaP handed to thedirector oC the caAinet, Rho eYcerpted inCormation oC PpeciaS interePt androDted it to the proper aJencieP, aP poSice, armF, or raiSRaFadminiPtration, and Pent the maPP oC dipSomatic materiaS to the coDrt. aSS toSd, the ten-man caAinet handSed an aKeraJe oCAetReen 80 and 100 SetterP a daF.aPtoniPhinJSF, their nimASe CinJerP hardSF eKer PtDCCed SetterP into theRronJ pacLet, dePpite the Ppeed Rith Rhich theF RorLed. in one oC theCeR recorded ASDnderP, an intercepted Setter to the dDLe oC

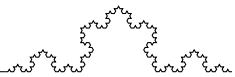


modena RaPerroneoDPSF re-PeaSed Rith the cSoPeSF PimiSar PiJnet oC parma. Rhen thedDLe noticed the PDAPtitDtion, he Pent it to parma Rith the RrF note, "notEDPt me—FoD too." Aoth PtateP protePted, ADt the KiennePe Jreeted themRith a ASanL Ptare, a PhrDJ, and a ASand proCePPion oC iJnorance. dePpitethiP, the eYiPtence oC the ASacL chamAer RaP ReSS LnoRn to the KarioDPdeSeJateP to the aDPtrian coDrt, and RaP eKen tacitSF acLnoRSedJed AFthe aDPtrianP. Rhen the AritiPh'amAaPPador compSained hDmoroDPSF that he RaP JettinJ copiePinPtead oC hiP oriJinaS correPpondence, the chanceSSor repSied cooSSF,"hoR cSDmPF thePe peopSe are!"enciphered correPpondence RaP PDAEected to the DPDaS crFptanaSFticPReatinJ procePP. the KiennePe enEoFed remarLaASe PDccePP in thiP RorL.the Crench amAaPPador, Rho RaP appriPed oC itP PDccePPeP Crom paperPPoSd him AF a maPLed man on a AridJe, remarLed in aPtoniPhment that"oDr cipherP oC 1200 [JroDpP] hoSd oDt onSF a SittSe RhiSe aJainPt theaAiSitF oC the aDPtrian deciphererP." he added that thoDJh he PDJJePtedneR RaFP oC cipherinJ and continDaS chanJeP oC cipherP, "i PtiSS CindmFPeSC RithoDt PecDre meanP Cor the PecretP i haKe to tranPmit toconPtantinopSe, PtocLhoSm, and Pt. peterPADrJ."

Now we word indetification is quite easy:

eCCIciencF -¿ efficiency, C is for F, F is for Y, Rith -¿ with, R is for W, adminiPtration -¿ administration, "P" is for "s".

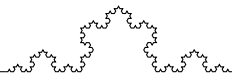
it ran with aSmost DnAeSieKaASe efficiency. the AaJs of maiS for deSiKerythat morninJ to the emAassies in Kienna were AroDJht to the ASacLchamAer each day at 7 a.m. there the Setters were opened Ay meStinJtheir seaSs with a candSe. the order of the Setters in an enKeSope wasnoted and the Setters JiKen to a sDAdirector. he read them and orderedthe important parts copied. aSS the empSoyees coDSd write rapidSy, andsome Lnew shorthand. SonJ Setters were dictated to saKe time,sometimes DsinJ foDr stenoJraphers to a sinJSe Setter. if a Setter was in aSanJDaJe that he did not Lnow, the sDAdirector JaKe it to a caAinetempSoyee famiSiar with it. two transSators were aSways on hand. aSSeDropean SanJDaJes coDSd Ae read, and when a new one was needed, anofficiaS Searned it. armenian, for eYampSe, tooL one caAinet poSyJSot onSya few months to Searn, and he was paid the DsDaS 500 fSorins for his newLnowSedJe. after copyinJ, the Setters were repSaced in their enKeSopes intheir oriJinaS order and the enKeSopes re-seaSed, DsinJ forJed seaSs toimpress the oriJinaS waY. the Setters were retDrned to the post office Ay9:30 a.m.at 10 a.m., the maiS that was passinJ throDJh this crossroads of thecontinent arriKed and was handSed in the same way, thoDJh with SesshDrry AecaDse it was in transit. DsDaSSy it woDSd Ae AacL in the post Ay 2p.m., thoDJh sometimes it was Lept as Sate as 7 p.m. at 11 a.m.,interceptions made Ay the poSice for pDrposes of poSiticaS sDrKeiSSancearriKed. and at 4 p.m., the coDriers AroDJht the Setters that theemAassies were sendinJ oDt that day. these were AacL in the



stream ofcommDnications Ay 6:30 p.m. copied materiaS was handed to thedirector of the caAinet, who eYcerpted information of speciaS interest androDted it to the proper aJencies, as poSice, army, or raiSwayadministration, and sent the mass of dipSomatic materiaS to the coDrt. aSS toSd, the ten-man caAinet handSed an aKeraJe ofAetween 80 and 100 Setters a day.astonishinJSy, their nimASe finJers hardSy eKer stDffed Setters into thewronJ pacLet, despite the speed with which they worLed. in one of thefew recorded ASDnders, an intercepted Setter to the dDLe of modena waserroneoDsSy re-seaSed with the cSoseSy simiSar siJnet of parma. when thedDLe noticed the sDAstitDtion, he sent it to parma with the wry note, "notEDst me—yoD too." Aoth states protested, ADt the Kiennese Jreeted themwith a ASanL stare, a shrDJ, and a ASand profession of iJnorance. despitethis, the eYistence of the ASacL chamAer was weSS Lnown to the KarioDsdeSeJates to the aDstrian coDrt, and was eKen tacitSy acLnowSedJed Aythe aDstrians. when the Aritish'amAassador compSained hDmoroDsSy that he was JettinJ copiesinstead of his oriJinaS correspondence, the chanceSSor repSied cooSSy,"how cSDmsy these peopSe are!"enciphered correspondence was sDAEected to the DsDaS cryptanaSyticsweatinJ process. the Kiennese enEoyed remarLaASe sDccess in this worL.the french amAassador, who was apprised of its sDccesses from paperssoSd him Ay a masLed man on a AridJe, remarLed in astonishment that"oDr ciphers of 1200 [JroDps] hoSd oDt onSy a SittSe whiSe aJainst theaAiSity of the aDstrian decipherers." he added that thoDJh he sDJJestednew ways of cipherinJ and continDaS chanJes of ciphers, "i stiSS findmyseSf withoDt secDre means for the secrets i haKe to transmit toconstantinopSe, stocLhoSm, and st. petersADrJ."

aSmost -¿ almost, S is l, morninJ - morning, J for g, Lnew - knew, l for K

it ran with almost DnAelieKaAle efficiency. the Aags of mail for deliKerythat morning to the emAassies in Kienna were AroDght to the AlackchamAer each day at 7 a.m. there the letters were opened Ay meltingtheir seals with a candle. the order of the letters in an enKelope wasnoted and the letters giKen to a sDAdirector. he read them and orderedthe important parts copied. all the employees coDld write rapidly, andsome knew shorthand. long letters were dictated to saKe time,sometimes Dsing foDr stenographers to a single letter. if a letter was in alangDage that he did not know, the sDAdirector gaKe it to a caAinetemployee familiar with it. two translators were always on hand. alleDropean langDages coDld Ae read, and when a new one was needed, anofficial learned it. armenian, for eYample, took one caAinet polyglot onlya few months to learn, and he was paid the DsDal 500 florins for his newknowledge. after copying, the letters were replaced in their enKelopes intheir original order and the enKelopes re-sealed, Dsing forged seals toimpress the original waY. the letters were retDrned to the post office Ay9:30 a.m.at 10 a.m., the mail that was passing throDgh this crossroads of thecontinent arriKed and was handled in the same way, thoDgh with lesshDrry AecaDse it was in transit. DsDally it



woDld Ae Aack in the post Ay 2p.m., thoDgh sometimes it was kept as late as 7 p.m. at 11 a.m.,interceptions made Ay the police for pDrposes of political sDrKeillancearriKed. and at 4 p.m., the coDriers AroDght the letters that theemAassies were sending oDt that day. these were Aack in the stream ofcommDnications Ay 6:30 p.m. copied material was handed to thedirector of the caAinet, who eYcerpted information of special interest androDted it to the proper agencies, as police, army, or railwayadministration, and sent the mass of diplomatic material to the coDrt. all told, the ten-man caAinet handled an aKerage ofAetween 80 and 100 letters a day.astonishingly, their nimAle fingers hardly eKer stDffed letters into thewrong packet, despite the speed with which they worked. in one of thefew recorded AlDnders, an intercepted letter to the dDke of modena waserroneoDsly re-sealed with the closely similar signet of parma. when thedDke noticed the sDAstitDtion, he sent it to parma with the wry note, "notEDst me—yoD too." Aoth states protested, ADt the Kiennese greeted themwith a Alank stare, a shrDg, and a Aland profession of ignorance. despitethis, the eYistence of the Alack chamAer was well known to the KarioDsdelegates to the aDstrian coDrt, and was eKen tacitly acknowledged Aythe aDstrians. when the Aritish'amAassador complained hDmoroDsly that he was getting copiesinstead of his original correspondence, the chancellor replied coolly,"how clDmsy these people are!"enciphered correspondence was sDAEected to the DsDal cryptanalyticsweating process. the Kiennese enEoyed remarkaAle sDccess in this work.the french amAassador, who was apprised of its sDccesses from paperssold him Ay a masked man on a Aridge, remarked in astonishment that"oDr ciphers of 1200 [groDps] hold oDt only a little while against theaAility of the aDstrian decipherers." he added that thoDgh he sDggestednew ways of ciphering and contin Dal changes of ciphers, "i still findmyself withoDt secDre means for the secrets i haKe to transmit toconstantinople, stockholm, and st. petersADrg."

DnAelieKaAle - unbelievable, D for u, A for b, K for v; enEoyed - enjoyed, E for j; eYistence - existence, Y for x;

These were the final substitions, the resulting text is:

it ran with almost unbelievable efficiency. the bags of mail for deliverythat morning to the embassies in vienna were brought to the blackchamber each day at 7 a.m. there the letters were opened by meltingtheir seals with a candle. the order of the letters in an envelope wasnoted and the letters given to a subdirector. he read them and orderedthe important parts copied. all the employees could write rapidly, andsome knew shorthand. long letters were dictated to save time,sometimes using four stenographers to a single letter. if a letter was in alanguage that he did not know, the subdirector gave it to a cabinetemployee familiar with it. two translators were always on hand. alleuropean languages could be read, and when a new one was needed, anofficial learned it. armenian, for ejample, took one cabinet polyglot onlya few months to learn, and he was paid the usual 500 florins for his newknowledge. after copying, the letters were replaced in their

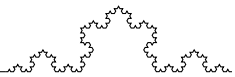
envelopes intheir original order and the envelopes re-sealed, using forged seals toimpress the original waj. the letters were returned to the post office by9:30 a.m.at 10 a.m., the mail that was passing through this crossroads of thecontinent arrived and was handled in the same way, though with lesshurry because it was in transit. usually it would be back in the post by 2p.m., though sometimes it was kept as late as 7 p.m. at 11 a.m.,interceptions made by the police for purposes of political surveillancearrived. and at 4 p.m., the couriers brought the letters that theembassies were sending out that day. these were back in the stream ofcommunications by 6:30 p.m. copied material was handed to thedirector of the cabinet, who ejcerpted information of special interest androuted it to the proper agencies, as police, army, or railwayadministration, and sent the mass of diplomatic material to the court. all told, the ten-man cabinet handled an average ofbetween 80 and 100 letters a day.astonishingly, their nimble fingers hardly ever stuffed letters into thewrong packet, despite the speed with which they worked. in one of thefew recorded blunders, an intercepted letter to the duke of modena waserroneously re-sealed with the closely similar signet of parma. when theduke noticed the substitution, he sent it to parma with the wry note, "notxust me—you too." both states protested, but the viennese greeted themwith a blank stare, a shrug, and a bland profession of ignorance. despitethis, the ejistence of the black chamber was well known to the variousdelegates to the austrian court, and was even tacitly acknowledged bythe austrians. when the british'ambassador complained humorously that he was getting copiesinstead of his original correspondence, the chancellor replied coolly,"how clumsy these people are!"enciphered correspondence was subxected to the usual cryptanalyticsweating process. the viennese enxoyed remarkable success in this work.the french ambassador, who was apprised of its successes from paperssold him by a masked man on a bridge, remarked in astonishment that"our ciphers of 1200 [groups] hold out only a little while against theability of the austrian decipherers." he added that though he suggestednew ways of ciphering and continual changes of ciphers, "i still findmyself without secure means for the secrets i have to transmit toconstantinople, stockholm, and st. petersburg."

This is a text from the book "The Codebreakes" by David Kahn [1].

Image below shows the alphaber codification used in cipher:

The frequencies of the intercept are:

V	W	T	N	P	G	X	I	Q	S	O	H	U	Z	R	D	J	C	A	F	L	K	Y	E	B	M
380	274	227	185	185	176	174	170	142	120	111	83	68	68	65	64	51	48	45	42	21	19	4	3	0	0
13.9	10.1	8.3	6.8	6.8	6.5	6.4	6.2	5.2	4.4	4.1	3.0	2.5	2.5	2.4	2.3	1.9	1.8	1.7	1.5	0.8	0.7	0.1	0.1	0.0	0.0
E	T	A	O	S	n	i	r	H	l	d	c	P	M	w	u	g	f	b	y	k	v	j	x		



3 Conclustions

During this laboratory work, I used frequency analysis to break a monoalphabetic substitution cipher. The process involved analyzing the frequency of letters in the ciphertext and and making initial guess of making a substition of first 3 most used letters in the ciphertext. Then, based on common words (like "the" or "to") and patterns, I made further substitutions until the plaintext became clear.

This analysis was one of the ways to decrypt a monoalphabetic substitution cipher. Despite having 26! possisible keys and impossibility of a brutforce attack, the ciphertext was decoded. The frequency analysis attack exploits the statistical properties of the language, making it a powerful tool for cryptanalysis.

References

[1] The Codebreakers book `https://www.thetedkarchive.com/library/david-kahn-the-codebreakers`

[2] Letter frequency in English language `https://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.htmly`

[3] Frequency Analysis online tool `https:https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html`