Ministry of Education, Research and Culture
Technical University of Moldova
Software Engineering and Automation Departments

REPORT

Laboratory work No. 2 (v9)

Course: Cryptography and Security

Theme: Cryptanalysis of monoalphabetic ciphers

Author: Corneliu Catlabuga
FAF-213

Checked by: univ. assist.
Cătălin Mîţu

Chisinau 2023

Objective:

Using the frequency analysis attack decrypt the intercepted message.

Task:

Decrypt the following text:

VTHQ GVR PVWWXGJ NC TSAVIWX'P OXPL AINDJQW XGWN USTF T GVR HXUQVITSUQTAVW, XG RQXHQ ANWQ WQV USTXGWVYW TGO WQV HXUQVIWVYW VBDXKTSVGWP TIVHQTGJVO XG IVJTIO WN NGV TGNWQVI. WQVIV TIV TP ZTGF NC WQVPV TSUQTAVWPTP WQVIV TIV UNPXWXNGP NC QXP OXPL, TGO WQXP ZDSWXUSXHXWF ZVTGP WQTW TSAVIWXQVIV OVKXPVO WQV CXIPW UNSFTSUQTAVWXH HXUQVI.WQXP THQXVKVZVGW—HIXWXHTS XG WQV QXPWNIF NC HIFUWNSNJF —TSAVIWX WQVGTONIGVO AF TGNWQVI IVZTILTASV XGKVGWXNG: VGHXUQVIVO HNOV. XW RTP CNIWQXP WQTW QV QTO UDW GDZAVIP XG WQV NDWVI IXGJ. XG T WTASV QV UVIZDWVOWQV GDZAVIP 1 WN 4 XG WRN-, WQIVV-, TGO CNDI-OXJXW JINDUP, CINZ 11 WN4444, TGO DPVO WQVPV TP 336 HNOVJINDUP CNI T PZTSS HNOV. "XG WQXP WTASV,THHNIOXGJ WN TJIVVZVGW, RV PQTSS VGWVI XG WQV KTIXNDP SXGVP TW WQVGDZAVIP RQTWVKVI HNZUSVWV UQITPVP RV USVTPV, CNI VYTZUSV,HNIIVPUNGOXGJ WN 12, 'RV QTKV ZTOV IVTOF WQV PQXUP RQXHQ RV UINZXPVOTGO PDUUSXVO WQVZ RXWQ WINNUP TGO JITXG.' " WQVPV HNOV KTSDVP OXO GNWHQTGJV, TGF ZNIV WQTG WQV ZXYVO TSUQTAVW NC WQV OXPL OXO. ADW WQV OXJXWPIVPDSWXGJ CINZ TG VGHNOXGJ RVIV WQVG VGHXUQVIVO RXWQ WQV OXPL EDPW TP XCWQVF RVIV USTXGWVYW SVWWVIP. XG TSAVIWX'P RNIOP, "WQVPV GDZAVIP X WQVGXGPVIW XG ZF ZVPPTJV THHNIOXGJ WN WQV CNIZDST NC WQV HXUQVI, IVUIVPVGWXGJWQVZ AF WQV SVWWVIP WQTW OVGNWV WQVPV GDZAVIP." WQVPV GDZAVIP WQDPHQTGJVO WQVXI HXUQVIWVYW VBDXKTSVGWP TP WQV OXPL WDIGVO. QVGHV 341,UVIQTUP ZVTGXGJ "UNUV," ZXJQW AVHNZV ZIU TW NGV UNPXWXNG TGO CHN TWTGNWQVI. WQXP HNGPWXWDWVP TG VYHVSSVGW CNIZ NC VGHXUQVIVO HNOV, TGO EDPWQNR UIVHNHXNDP TSAVIWX RTP ZTF AV PVVG AF WQV CTHW WQTW WQV ZTENIUNRVIP NC WQV VTIWQ OXO GNW AVJXG WN VGHXUQVI WQVXI HNOV ZVPPTJVP DGWXS400 FVTIP STWVI, GVTI WQV VGO NC WQV 19WQ HVGWDIF, TGO VKVG WQVG WQVXIPFPWVZP RVIV ZDHQ PXZUSVI WQTG WQXP.TSAVIWX'P WQIVV IVZTILTASV CXIPWP—WQV VTISXVPW RVPWVIG VYUNPXWXNG NCHIFUWTGTSFPXP, WQV XGKVGWXNG NC UNSFTSUQTAVWXV PDAPWXWDWXNG, TGO WQVXGKVGWXNG NC VGHXUQVIVO HNOV—ZTLV QXZ WQV CTWQVI NC RVPWVIGHIFUWNSNJF. ADW TSWQNDJQ QXP WIVTWXPV RTP UDASXPQVO XG XWTSXTG XG THNSSVHWXNG NC QXP RNILP XG 1568, TGO TSWQNDJQ QXP XOVTP RVIV TAPNIAVO AFUTUTS HIFUWNSNJXPWP TGO UVIQTUP XGCSDVGHVO WQV PHXVGHV'P OVKVSNUZVGW,WQVF GVKVI QTO WQV OFGTZXH XZUTHW WQTW PDHQ UINOXJXNDPTHHNZUSXPQZVGWP NDJQW WN QTKV UINODHVO. PFZNGOP' VKTSDTWXNG NC QXPRNIL XG JVGVITS ZTF ANWQ VYUSTXG RQF TGO PDZZTIXMV WQV ZNOVIG KXVR NC QXP HIFUWNSNJXHTS

HNGWIXADWXNGP:"WQXP ZTG NC ZTGF-PXOVO JVGXDP HTZV XGWN WQV RNISO WNN PNNG CNI WQVUVICVHW VYVIHXPV NC QXP PXGJDSTI CTHDSWXVP. RQVWQVI RV IVJTIO QXZ CINZ WQVUNXGW NC KXVR NC TIW, NC PHXVGHV, NI NC SXWVITWDIV, QV NHHDUXVP XG VTHQOVUTIWZVGW WQV UNPXWXNG NC UIVHDIPNI, UXNGVVI, TGO XGOXHTWNI. TSRTFPNIXJXGTS TGO TSRTFP CVIWXSV, QV UINUQVPXVO NC STGOP QV RTP GNW UIXKXSVJVOWN VGWVI, SVTKXGJ WQV ZVZNIF NC OXZ TGO KTIXVO JIVTWGVPP ITWQVI WQTG TGFPNSXO ZNGDZVGW AVQXGO QXZ."UNSFTSUQTAVWXHXWF WNNL TGNWQVI PWVU CNIRTIO XG 1518, RXWQ WQVTUUVTITGHV NC WQV CXIPW UIXGWVO ANNL NG HIFUWNSNJF, RIXWWVG AF NGV NC WQVZNPW CTZNDP XGWVSSVHWDTSP NC QXP OTF. WQXP RTP ENQTGGVP WIXWQVZXDP, TAVGVOXHWXGV ZNGL RQNPV OTAASXGJ XG TSHQVZF TGO NWQVI ZFPWXH UNRVIPZTOV QXZ NGV NC WQV ZNPW IVKVIVO CXJDIVP XG NHHDSW PHXVGHV, RQXSV QXPZNIV PNSXO PHQNSTIPQXU RNG QXZ WQV WXWSV NC "CTWQVI NC AXAXSXNJITUQF." XG1518, T FVTI TGO T QTSC TCWVI QXP OVTWQ, QXP UNSFJITUQXTV SXAIX PVY, SNTGGXPWIXWQVZXX TAATWXP UVTUNSXWTGX, BDNGOTZ PUTGQVXZVGPXP, TO ZTYXZXSXTGDZHTVPTIVZ ("PXY ANNLP NC UNSFJITUQF, AF ENQTGGVP WIXWQVZXDP, TAANW TWRDIMADIJ, CNIZVISF TW PUTGQVXZ, CNI WQV VZUVINI ZTYXZXSXTG") RTPUDASXPQVO. AF CTI WQV ADSL NC WQV KNSDZV HNGPXPWP NC WQV HNSDZGP NCRNIOP UIXGWVO XG STIJV JNWQXH WFUV WQTW WIXWQVZXDP DPVO XG QXP PFPWVZP NCHIFUWNJITUQF. ADW XG WQV RNIL'P ANNL K TUUVTIP, CNI WQV CXIPW WXZV, WQVPBDTIV WTASV, NI WTASVTD. WQXP XP WQV VSVZVGWTS CNIZ NC UNSFTSUQTAVWXHPDAPWXWDWXNG, CNI XW VYQXAXWP TSS TW NGHV TSS WQV HXUQVI TSUQTAVWP XG TUTIWXHDSTI PFPWVZ. WQVPV TIV DPDTSSF TSS WQV PTZV PVBDVGHV NC SVWWVIP, ADWPQXCWVO WN OXCCVIVGW UNPXWXNGP XG IVSTWXNG WN WQV USTXGWVYW TSUQTAVW, TP XGTSAVIWX'P OXPL WQV XGGVI TSUQTAVW TPPDZVO OXCCVIVGW UNPXWXNGP XG IVJTIO WNWQV NDWVI TSUQTAVW. WQV WTASVTD PVWP WQVZ NDW XG NIOVISF CTPQXNG—WQVTSUQTAVWP NC WQV PDHHVPPXKV UNPXWXNGP STXO NDW XG INRP NGV AVSNR WQVNWQVI, VTHQ TSUQTAVW PQXCWVO NGV USTHV WN WQV SVCW NC WQV NGV TANKV. VTHQINR WQDP NCCVIP T OXCCVIVGW PVW NC HXUQVI PDAPWXWDWVP WN WQV SVWWVIP NC WQVUSTXGWVYW TSUQTAVW TW WQV WNU. PXGHV WQVIV HTG AV NGSF TP ZTGF INRP TPWQVIV TIV SVWWVIP XG WQV TSUQTAVW, WQV WTASVTD XP PBDTIV.WQV PXZUSVPW WTASVTD XP NGV WQTW DPVP WQV GNIZTS TSUQTAVW XG KTIXNDPUNPXWXNGP TP WQV HXUQVI TSUQTAVWP. VTHQ HXUQVI TSUQTAVW UINODHVP, XGNWQVI RNIOP, T HTVPTI PDAPWXWDWXNG.

Theoretical considerations:

Table 1: English language letter frequency

E	T	A	O	I	N	S	H	R	D	L	C	U
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
M	W	F	G	Y	P	B	V	K	J	X	Q	Z
2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.1	0.07

Implementation, practical results:

Table 2: Encrypted text letter frequency

V	W	T	X	N	P	Q	G	I	S	U	O	H
13.1	9.9	7.7	7.7	6.8	6.7	6.6	6.1	6.1	3.9	3.3	3.1	2.9
Z	D	C	A	F	R	J	K	L	Y	B	E	M
2.7	2.5	2.3	2.3	1.6	1.4	1.3	0.7	0.5	0.4	0.2	0.1	0.1

1. V → e due to being the highest frequency

c = eTHQ GeR PeWWXGJ NC TSAeIWX'P OXPL AINDJQW XGWN USTF T GeR HXUQeITSUQTAeW, XG RQXHQ ANWQ WQe USTXGWeYW TGO WQe HXUQeIWeYW eBDXKTSeGWP TIeHQTGJeO XG IeJTIO WN NGe TGNWQeI. WQeIe TIe TP ZTGF NC WQePe TSUQTAeWPTP WQeIe TIe UNPXWXNGP NC QXP OXPL, TGO WQXP ZDSWXUSXHXWF ZeTGP WQTW TSAeIWXQeIe OeKXPeO WQe CXIPW UNSFTSUQTAeWXH HXUQeI.WQXP THQXeKeZeGW—HIXWXHTS XG WQe QXPWNIF NC HIFUWNSNJF —TSAeIWX WQeGTONIGeO AF TGNWQeI IeZTILTASe XGKeGWXNG: eGHXUQeIeO HNOe. XW RTP CNIWQXP WQTW Qe QTO UDW GDZAeIP XG WQe NDWeI IXGJ. XG T WTASe Qe UeIZDWeOWQe GDZAeIP 1 WN 4 XG WRN-, WQIee-, TGO CNDI-OXJXW JINDUP, CINZ 11 WN4444, TGO DPeO WQePe TP 336 HNOeJINDUP CNI T PZTSS HNOe. "XG WQXP WTASe,THHNIOXGJ WN TJIeeZeGW, Re PQTSS eGWeI XG WQe KTIXNDP SXGeP TW WQeGDZAeIP RQTWeKeI HNZUSeWe UQITPeP Re USeTPe, CNI eYTZUSe,HNIIePUNGOXGJ WN 12, 'Re QTKe ZTOe IeTOF WQe PQXUP RQXHQ Re UINZXPeOTGO PDUUSXeO WQeZ RXWQ WINNUP TGO JITXG.' " WQePe HNOe KTSDeP OXO GNWHQTGJe, TGF ZNIe WQTG WQe ZXYeO TSUQTAeW NC WQe OXPL OXO. ADW WQe OXJXWPIePDSWXGJ CINZ TG eGHNOXGJ ReIe WQeG eGHXUQeIeO RXWQ WQe OXPL EDPW TP XCWQeF ReIe USTXGWeYW SeWWeIP. XG TSAeIWX'P RNIOP, "WQePe GDZAeIP X WQeGXGPeIW XG ZF ZePPTJe THHNIOXGJ WN WQe CNIZDST NC WQe HXUQeI, IeUIePeGWXGJWQeZ AF WQe SeWWeIP WQTW OeGNWe WQePe GDZAeIP." WQePe GDZAeIP WQDPHQTGJeO WQeXI HXUQeIWeYW eBDXKTSeGWP TP WQe OXPL WDIGeO. QeGHe 341,UeIQTUP ZeTGXGJ "UNUe," ZXJQW AeHNZe ZIU TW NGe UNPXWXNG TGO CHN TWTGNWQeI. WQXP HNGPWXWDWeP TG eYHeSSeGW CNIZ NC eGHXUQeIeO HNOe, TGO EDPWQNR UIeHNHXNDP TSAeIWX RTP ZTF Ae PeeG AF WQe CTHW WQTW WQe ZTENIUNReIP NC

WQe eTIWQ OXO GNW AeJXG WN eGHXUQeI WQeXI HNOe ZePPTJeP DGWXS400 FeTIP STWeI, GeTI WQe eGO NC WQe 19WQ HeGWDIF, TGO eKeG WQeG WQeXIPFPWeZP ReIe ZDHQ PXZUSeI WQTG WQXP.TSAeIWX'P WQIee IeZTILTASe CXIPWP—WQe eTISXePW RePWeIG eYUNPXWXNG NCHIFUWTGTSFPXP, WQe XGKeGWXNG NC UNSFTSUQTAeWXe PDAPWXWDWXNG, TGO WQeXGKeGWXNG NC eGHXUQeIeO HNOe —ZTLe QXZ WQe CTWQeI NC RePWeIGHIFUWNSNJF. ADW TSWQNDJQ QXP WIeTWXPe RTP UDASXPQeO XG XWTSXTG XG THNSSeHWXNG NC QXP RNILP XG 1568, TGO TSWQNDJQ QXP XOeTP ReIe TAPNIAeO AFUTUTS HIFUWNSNJXPWP TGO UeIQTUP XGCSDeGHeO WQe PHXeGHe'P OeKeSNUZeGW,WQeF GeKeI QTO WQe OFGTZXH XZUTHW WQTW PDHQ UINOXJXNDPTHHNZUSXPQZeGWP NDJQW WN QTKe UINODHeO. PFZNGOP' eKTSDTWXNG NC QXPRNIL XG JeGeITS ZTF ANWQ eYUSTXG RQF TGO PDZZTIXMe WQe ZNOeIG KXeR NC QXP HIFUWNSNJXHTS HNGWIXADWXNGP:"WQXP ZTG NC ZTGF-PXOeO JeGXDP HTZe XGWN WQe RNISO WNN PNNG CNI WQeUeICeHW eYeIHXPe NC QXP PXGJDSTI CTHDSWXeP. RQeWQeI Re IeJTIO QXZ CINZ WQeUNXGW NC KXeR NC TIW, NC PHXeGHe, NI NC SXWeITWDIe, Qe NHHDUXeP XG eTHQOeUTIWZeGW WQe UNPXWXNG NC UIeHDIPNI, UXNGeeI, TGO XGOXHTWNI. TSRTFPNIXJXGTS TGO TSRTFP CeIWXSe, Qe UINUQePXeO NC STGOP Qe RTP GNW UIXKXSeJeOWN eGWeI, SeTKXGJ WQe ZeZNIF NC OXZ TGO KTIXeO JIeTWGePP ITWQeI WQTG TGFPNSXO ZNGDZeGW AeQXGO QXZ."UNSFTSUQTAeWXHXWF WNNL TGNWQeI PWeU CNIRTIO XG 1518, RXWQ WQeTUUeTITGHe NC WQe CXIPW UIXGWeO ANNL NG HIFUWNSNJF, RIXWWeG AF NGe NC WQeZNPW CTZNDP XGWeSSeHWDTSP NC QXP OTF. WQXP RTP ENQTGGeP WIXWQeZXDP, TAeGeOXHWXGe ZNGL RQNPe OTAASXGJ XG TSHQeZF TGO NWQeI ZFPWXH UNReIPZTOe QXZ NGe NC WQe ZNPW IeKeIeO CXJDIeP XG NHHDSW PHXeGHe, RQXSe QXPZNIe PNSXO PHQNSTIPQXU RNG QXZ WQe WXWSe NC "CTWQeI NC AXAXSXNJITUQF." XG1518, T FeTI TGO T QTSC TCWeI QXP OeTWQ, QXP UNSFJITUQXTe SXAIX PeY, SNTGGXPWIXWQeZXX TAATWXP UeTUNSXWTGX, BDNGOTZ PUTGQeXZeGPXP, TO ZTYXZXSXTGDZHTePTIeZ ("PXY ANNLP NC UNSFJITUQF, AF ENQTGGeP WIXWQeZXDP, TAANW TWRDIMADIJ, CNIZeISF TW PUTGQeXZ, CNI WQe eZUeINI ZTYXZXSXTG") RTPUDASXPQeO. AF CTI WQe ADSL NC WQe KNSDZe HNGPXPWP NC WQe HNSDZGP NCRNIOP UIXGWeO XG STIJe JNWQXH WFUe WQTW WIXWQeZXDP DPeO XG QXP PFPWeZP NCHIFUWNJITUQF. ADW XG WQe RNIL'P ANNL K TUUeTIP, CNI WQe CXIPW WXZe, WQePBDTIe WTASe, NI WTASeTD. WQXP XP WQe eSeZeGWTS CNIZ NC UNSFTSUQTAeWXHPDAPWXWDWXNG, CNI XW eYQXAXWP TSS TW NGHe TSS WQe HXUQeI TSUQTAeWP XG TUTIWXHDSTI PFPWeZ. WQePe TIe DPDTSSF TSS WQe PTZe PeBDeGHe NC SeWWeIP, ADWPQXCWeO WN OXCCeIeGW UNPXWXNGP XG IeSTWXNG WN WQe USTXGWeYW TSUQTAeW, TP XGTSAeIWX'P OXPL WQe XGGeI TSUQTAeW TPPDZeO OXCCeIeGW UNPXWXNGP XG IeJTIO WNWQe NDWeI TSUQTAeW. WQe WTASeTD PeWP WQeZ NDW XG NIOeISF CTPQXNG—WQeTSUQTAeWP NC WQe PDHHePPXKe UNPXWXNGP STXO NDW XG INRP NGe AeSNR WQeNWQeI, eTHQ TSUQTAeW PQXCWeO NGe USTHe WN WQe SeCW NC WQe NGe TANKe. eTHQINR WQDP NCCeIP T OXCCeIeGW PeW NC HXUQeI PDAPWXWDWeP WN WQe SeWWeIP NC WQeUSTXGWeYW TSUQTAeW TW WQe WNU. PXGHe WQeIe HTG Ae NGSF TP ZTGF INRP TPWQeIe TIe SeWWeIP XG WQe TSUQTAeW, WQe WTASeTD XP PBDTIe.WQe PXZUSePW WTASeTD XP NGe WQTW DPeP WQe GNIZTS TSUQTAeW XG KTIXNDPUNPXWXNGP TP WQe HXUQeI TSUQTAeWP. eTHQ HXUQeI TSUQTAeW UINODHeP, XGNWQeI RNIOP, T HTePTI PDAPWXWDWXNG.

2. W→t; Q→h; “WQe”0 resembles the word “the” and the substitutions have maching frequencyes.

c = eTHh GeR PettXGJ NC TSAeItX'P OXPL AINDJht XGtN USTF T GeR HXUheITSUhTAet, XG RhXHh ANth the USTXGteYt TGO the HXUheIteYt eBDXKTSeGtP TIeHhTGJeO XG IeJTIO tN NGe TGNtheI. theIe TIe TP ZTGF NC thePe TSUhTAetPTP theIe TIe UNPXtXNGP NC hXP OXPL, TGO thXP ZDStXUSXHXtF ZeTGP thTt TSAeItXheIe OeKXPeO the CXIPt UNSFTSUhTAetXH HXUheI.thXP THhXeKeZeGt—HIXtXHTS XG the hXPtNIF NC HIFUtNSNJF —TSAeItX theGTONIGeO AF TGNtheI IeZTILTASe XGKeGtXNG: eGHXUheIeO HNOe. Xt RTP CNIthXP thTt he hTO UDt GDZAeIP XG the NDteI IXGJ. XG T tTASe he UeIZDteOthe GDZAeIP 1 tN 4 XG tRN-, thIee-, TGO CNDI-OXJXt JINDUP, CINZ 11 tN4444, TGO DPeO thePe TP 336 HNOeJINDUP CNI T PZTSS HNOe. "XG thXP tTASe,THHNIOXGJ tN TJIeeZeGt, Re PhTSS eGteI XG the KTIXNDP SXGeP Tt theGDZAeIP RhTteKeI HNZUSete UhITPeP Re USeTPe, CNI eYTZUSe,HNIIePUNGOXGJ tN 12, 'Re hTKe ZTOe IeTOF the PhXUP RhXHh Re UINZXPeOTGO PDUUSXeO theZ RXth tINNUP TGO JITXG.' " thePe HNOe KTSDeP OXO GNtHhTGJe, TGF ZNIe thTG the ZXYeO TSUhTAet NC the OXPL OXO. ADt the OXJXtPIePDStXGJ CINZ TG eGHNOXGJ ReIe theG eGHXUheIeO RXth the OXPL EDPt TP XCtheF ReIe USTXGteYt SetteIP. XG TSAeItX'P RNIOP, "thePe GDZAeIP X theGXGPeIt XG ZF ZePPTJe THHNIOXGJ tN the CNIZDST NC the HXUheI, IeUIePeGtXGJtheZ AF the SetteIP thTt OeGNte thePe GDZAeIP." thePe GDZAeIP thDPHhTGJeO theXI HXUheIteYt eBDXKTSeGtP TP the OXPL tDIGeO. heGHe 341,UeIhTUP ZeTGXGJ "UNUe," ZXJht AeHNZe ZIU Tt NGe UNPXtXNG TGO CHN TtTGNtheI. thXP HNGPtXtDteP TG eYHeSSeGt CNIZ NC eGHXUheIeO HNOe, TGO EDPthNR UIeHNHXNDP TSAeItX RTP ZTF Ae PeeG AF the CTHt thTt the ZTENIUNReIP NC the eTIth OXO GNt AeJXG tN eGHXUheI theXI HNOe ZePPTJeP DGtXS400 FeTIP StteI, GeTI the eGO NC the 19th HeGtDIF, TGO eKeG theG theXIPFPteZP ReIe ZDHh PXZUSeI thTG thXP.TSAeItX'P thIee IeZTILTASe CXIPtP—the eTISXePt RePteIG eYUNPXtXNG NCHIFUtTGTSFPXP, the XGKeGtXNG NC UNSFTSUhTAetXe PDAPtXtDtXNG, TGO theXGKeGtXNG NC eGHXUheIeO HNOe—ZTLe hXZ the CTtheI NC RePteIGHIFUtNSNJF. ADt TSthNDJh hXP tIeTtXPe RTP UDASXPheO XG XtTSXTG XG THNSSeHtXNG NC hXP RNILP XG 1568, TGO TSthNDJh hXP XOeTP ReIe TAPNIAeO AFUTUTS HIFUtNSNJXPtP TGO UeIhTUP XGCSDeGHeO the PHXeGHe'P OeKeSNUZeGt,theF GeKeI hTO the OFGTZXH XZUTHt thTt PDHh UINOXJXNDPTHHNZUSXPhZeGtP NDJht tN hTKe UINODHeO. PFZNGOP' eKTSDTtXNG NC hXPRNIL XG JeGeITS ZTF ANth eYUSTXG RhF TGO PDZZTIXMe the ZNOeIG KXeR NC hXP HIFUtNSNJXHTS HNGtIXADtXNGP:"thXP ZTG NC ZTGF-PXOeO JeGXDP HTZe XGtN the RNISO tNN PNNG CNI theUeICeHt eYeIHXPe NC hXP PXGJDSTI CTHDStXeP. RhetheI Re IeJTIO hXZ CINZ theUNXGt NC KXeR NC TIt, NC PHXeGHe, NI NC SXteITtDIe, he NHHDUXeP XG eTHhOeUTItZeGt the UNPXtXNG NC UIeHDIPNI, UXNGeeI, TGO XGOXHTtNI. TSRTFPNIXJXGTS TGO TSRTFP CeItXSe, he UINUhePXeO NC STGOP he RTP GNt UIXKXSeJeOtN eGteI, SeTKXGJ the ZeZNIF NC OXZ TGO KTIXeO JIeTtGePP ITtheI thTG TGFPNSXO ZNGDZeGt AehXGO hXZ."UNSFTSUhTAetXHXtF tNNL TGNtheI PteU CNIRTIO XG 1518, RXth theTUUeTITGHe NC the CXIPt UIXGteO ANNL NG HIFUtNSNJF, RIXtteG AF NGe NC theZNPt CTZNDP XGteSSeHtDTSP NC hXP OTF. thXP RTP ENhTGGeP tIXtheZXDP, TAeGeOXHtXGe ZNGL RhNPe OTAASXGJ XG TSHheZF TGO NtheI ZFPtXH UNReIPZTOe hXZ NGe NC the ZNPt IeKeIeO CXJDIeP XG NHHDSt PHXeGHe, RhXSe hXPZNIe PNSXO PHhNSTIPhXU RNG hXZ the tXtSe NC "CTtheI NC AXAXSXNJITUhF." XG1518, T FeTI TGO T hTSC TCteI hXP OeTth, hXP UNSFJITUhXTe SXAIX PeY, SNTGGXPtIXtheZXX TAATtXP UeTUNSXtTGX, BDNGOTZ PUTGheXZeGPXP, TO ZTYXZXSXTGDZHTePTIeZ ("PXY ANNLP NC UNSFJITUhF, AF ENhTGGeP tIXtheZXDP, TAANt TtRDIMADIJ, CNIZeISF Tt PUTGheXZ, CNI the eZUeINI ZTYXZXSXTG") RTPUDASXPheO. AF CTI the ADSL NC the KNSDZe HNGPXPtP NC the HNSDZGP NCRNIOP UIXGteO XG STIJe JNthXH tFUe thTt tIXtheZXDP DPeO XG hXP PFPteZP NCHIFUtNJITUhF. ADt XG the RNIL'P ANNL K TUUeTIP, CNI the CXIPt tXZe, thePBDTIe tTASe, NI tTASeTD. thXP XP the eSeZeGtTS CNIZ NC UNSFTSUhTAetXHPDAPtXtDtXNG, CNI Xt eYhXAXtP TSS Tt NGHe TSS the HXUheI

TSUhTAetP XG TUTItXHDSTI PFPteZ. thePe TIe DPDTSSF TSS the PTZe PeBDeGHe NC SetteIP, ADtPhXCteO tN OXCCeIeGt UNPXtXNGP XG IeSTtXNG tN the USTXGteYt TSUhTAet, TP XGTSAeItX'P OXPL the XGGeI TSUhTAet TPPDZeO OXCCeIeGt UNPXtXNGP XG IeJTIO tNthe NDteI TSUhTAet. The tTASeTD PetP theZ NDt XG NIOeISF CTPhXNG—theTSUhTAetP NC the PDHHePPXKe UNPXtXNGP STXO NDt XG INRP NGe AeSNR theNtheI, eTHh TSUhTAet PhXCteO NGe USTHe tN the SeCt NC the NGe TANKe. eTHhINR thDP NCCeIP T OXCCeIeGt Pet NC HXUheI PDAPtXtDteP tN the SetteIP NC theUSTXGteYt TSUhTAet Tt the tNU. PXGHe theIe HTG Ae NGSF TP ZTGF INRP TPtheIe TIe SetteIP XG the TSUhTAet, the tTASeTD XP PBDTIe.the PXZUSePt tTASeTD XP NGe thTt DPeP the GNIZTS TSUhTAet XG KTIXNDPUNPXtXNGP TP the HXUheI TSUhTAetP. eTHh HXUheI TSUhTAet UINODHeP, XGNtheI RNIOP, T HTePTI PDAPtXtDtXNG.

3. T→a; N→o; “thTt” and “tN” resemble the words “that” and “to” and the substitutions match the frequencies

c = eaHh GeR PettXGJ oC aSAeItX'P OXPL AIoDJht XGto USaF a GeR HXUheIaSUhaAet, XG RhXHh Aoth the USaXGteYt aGO the HXUheIteYt eBDXKaSeGtP aIeHhaGJeO XG IeJaIO to oGe aGotheI. theIe aIe aP ZaGF oC thePe aSUhaAetPaP theIe aIe UoPXtXoGP oC hXP OXPL, aGO thXP ZDStXUSXHXtF ZeaGP that aSAeItXheIe OeKXPeO the CXIPt UoSFaSUhaAetXH HXUheI.thXP aHhXeKeZeGt—HIXtXHaS XG the hXPtoIF oC HIFUtoSoJF —aSAeItX theGaOoIGeO AF aGotheI IeZaILaASe XGKeGtXoG: eGHXUheIeO HoOe. Xt RaP CoIthXP that he haO UDt GDZAeIP XG the oDteI IXGJ. XG a taASe he UeIZDteOthe GDZAeIP 1 to 4 XG tRo-, thIee-, aGO CoDI-OXJXt JIoDUP, CIoZ 11 to4444, aGO DPeO thePe aP 336 HoOeJIoDUP CoI a PZaSS HoOe. "XG thXP taASe,aHHoIOXGJ to aJIeeZeGt, Re PhaSS eGteI XG the KaIXoDP SXGeP at theGDZAeIP RhateKeI HoZUSete UhIaPeP Re USeaPe, CoI eYaZUSe,HoIIePUoGOXGJ to 12, 'Re haKe ZaOe IeaOF the PhXUP RhXHh Re UIoZXPeOaGO PDUUSXeO theZ RXth tIooUP aGO JIaXG.' " thePe HoOe KaSDeP OXO GotHhaGJe, aGF ZoIe thaG the ZXYeO aSUhaAet oC the OXPL OXO. ADt the OXJXtPIePDStXGJ CIoZ aG eGHoOXGJ ReIe theG eGHXUheIeO RXth the OXPL EDPt aP XCtheF ReIe USaXGteYt SetteIP. XG aSAeItX'P RoIOP, "thePe GDZAeIP X theGXGPeIt XG ZF ZePPaJe aHHoIOXGJ to the CoIZDSa oC the HXUheI, IeUIePeGtXGJtheZ AF the SetteIP that OeGote thePe GDZAeIP." thePe GDZAeIP thDPHhaGJeO theXI HXUheIteYt eBDXKaSeGtP aP the OXPL tDIGeO. heGHe 341,UeIhaUP ZeaGXGJ "UoUe," ZXJht AeHoZe ZIU at oGe UoPXtXoG aGO CHo ataGotheI. thXP HoGPtXtDteP aG eYHeSSeGt CoIZ oC eGHXUheIeO HoOe, aGO EDPthoR UIeHoHXoDP aSAeItX RaP ZaF Ae PeeG AF the CaHt that the ZaEoIUoReIP oC the eaIth OXO Got AeJXG to eGHXUheI theXI HoOe ZePPaJeP DGtXS400 FeaIP SateI, GeaI the eGO oC the 19th HeGtDIF, aGO eKeG theG theXIPFPteZP ReIe ZDHh PXZUSeI thaG thXP.aSAeItX'P thIee IeZaILaASe CXIPtP—the eaISXePt RePteIG eYUoPXtXoG oCHIFUtaGaSFPXP, the XGKeGtXoG oC UoSFaSUhaAetXe PDAPtXtDtXoG, aGO theXGKeGtXoG oC eGHXUheIeO HoOe—ZaLe hXZ the CatheI oC RePteIGHIFUtoSoJF. ADt aSthoDJh hXP tIeatXPe RaP UDASXPheO XG XtaSXaG XG aHoSSeHtXoG oC hXP RoILP XG 1568, aGO aSthoDJh hXP XOeaP ReIe aAPoIAeO AFUaUaS HIFUtoSoJXPtP aGO UeIhaUP XGCSDeGHeO the PHXeGHe'P OeKeSoUZeGt,theF GeKeI haO the OFGaZXH XZUaHt that PDHh UIoOXJXoDPaHHoZUSXPhZeGtP oDJht to haKe UIoODHeO. PFZoGOP' eKaSDatXoG oC hXPRoIL XG JeGeIaS ZaF Aoth eYUSaXG RhF aGO PDZZaIXMe the ZoOeIG KXeR oC hXP HIFUtoSoJXHaS HoGtIXADtXoGP:"thXP ZaG oC ZaGF-PXOeO JeGXDP HaZe XGto the RoISO too PooG CoI theUeICeHt eYeIHXPe oC hXP PXGJDSaI CaHDStXeP. RhetheI Re IeJaIO hXZ CIoZ theUoXGt oC KXeR oC aIt, oC PHXeGHe, oI oC SXteIatDIe, he oHHDUXeP XG eaHhOeUaItZeGt the UoPXtXoG oC UIeHDIPoI, UXoGeeI, aGO XGOXHatoI. aSRaFPoIXJXGaS aGO aSRaFP CeItXSe, he UIoUhePXeO oC SaGOP he RaP Got UIXKXSeJeOto eGteI, SeaKXGJ the ZeZoIF oC OXZ aGO KaIXeO JIeatGePP IatheI thaG aGFPoSXO ZoGDZeGt AehXGO hXZ."UoSFaSUhaAetXHXtF tooL aGotheI PteU CoIRaIO XG 1518, RXth theaUUeaIaGHe oC the CXIPt UIXGteO AooL oG HIFUtoSoJF, RIXtteG AF oGe oC theZoPt CaZoDP XGteSSeHtDaSP oC

hXP OaF. thXP RaP EohaGGeP tIXtheZXDP, aAeGeOXHtXGe ZoGL RhoPe OaAASXGJ XG aSHheZF aGO otheI ZFPtXH UoReIPZaOe hXZ oGe oC the ZoPt IeKeIeO CXJDIeP XG oHHDSt PHXeGHe, RhXSe hXPZoIe PoSXO PHhoSaIPhXU RoG hXZ the tXtSe oC "CatheI oC AXAXSXoJIaUhF." XG1518, a FeaI aGO a haSC aCteI hXP Oeath, hXP UoSFJIaUhXae SXAIX PeY, SoaGGXPtIXtheZXX aAAatXP UeaUoSXtaGX, BDoGOaZ PUaGheXZeGPXP, aO ZaYXZXSXaGDZHaePaIeZ ("PXY AooLP oC UoSFJIaUhF, AF EohaGGeP tIXtheZXDP, aAAot atRDIMADIJ, CoIZeISF at PUaGheXZ, CoI the eZUeIoI ZaYXZXSXaG") RaPUDASXPheO. AF CaI the ADSL oC the KoSDZe HoGPXPtP oC the HoSDZGP oCRoIOP UIXGteO XG SaIJe JothXH tFUe that tIXtheZXDP DPeO XG hXP PFPteZP oCHIFUtoJIaUhF. ADt XG the RoIL'P AooL K aUUeaIP, CoI the CXIPt tXZe, thePBDaIe taASe, oI taASeaD. thXP XP the eSeZeGtaS CoIZ oC UoSFaSUhaAetXHPDAPtXtDtXoG, CoI Xt eYhXAXtP aSS at oGHe aSS the HXUheI aSUhaAetP XG aUaItXHDSaI PFPteZ. thePe aIe DPDaSSF aSS the PaZe PeBDeGHe oC SetteIP, ADtPhXCteO to OXCCeIeGt UoPXtXoGP XG IeSatXoG to the USaXGteYt aSUhaAet, aP XGaSAeItX'P OXPL the XGGeI aSUhaAet aPPDZeO OXCCeIeGt UoPXtXoGP XG IeJaIO tothe oDteI aSUhaAet. the taASeaD PetP theZ oDt XG oIOeISF CaPhXoG—theaSUhaAetP oC the PDHHePPXKe UoPXtXoGP SaXO oDt XG IoRP oGe AeSoR theotheI, eaHh aSUhaAet PhXCteO oGe USaHe to the SeCt oC the oGe aAoKe. eaHhIoR thDP oCCeIP a OXCCeIeGt Pet oC HXUheI PDAPtXtDteP to the SetteIP oC theUSaXGteYt aSUhaAet at the toU. PXGHe theIe HaG Ae oGSF aP ZaGF IoRP aPtheIe aIe SetteIP XG the aSUhaAet, the taASeaD XP PBDaIe.the PXZUSePt taASeaD XP oGe that DPeP the GoIZaS aSUhaAet XG KaIXoDPUoPXtXoGP aP the HXUheI aSUhaAetP. eaHh HXUheI aSUhaAet UIoODHeP, XGotheI RoIOP, a HaePaI PDAPtXtDtXoG.

4. H→c; I→r; “eaHh”, “theIe” and “aIe” resemble the words “each”, “there” and “are”

c = each GeR PettXGJ oC aSAertX'P OXPL AroDJht XGto USaF a GeR cXUheraSUhaAet, XG RhXch Aoth the USaXGteYt aGO the cXUherteYt eBDXKaSeGtP arechaGJeO XG reJarO to oGe aGother. there are aP ZaGF oC thePe aSUhaAetPaP there are UoPXtXoGP oC hXP OXPL, aGO thXP ZDStXUSXcXtF ZeaGP that aSAertXhere OeKXPeO the CXrPt UoSFaSUhaAetXc cXUher.thXP achXeKeZeGt—crXtXcaS XG the hXPtorF oC crFUtoSoJF —aSAertX theGaOorGeO AF aGother reZarLaASe XGKeGtXoG: eGcXUhereO coOe. Xt RaP CorthXP that he haO UDt GDZAerP XG the oDter rXGJ. XG a taASe he UerZDteOthe GDZAerP 1 to 4 XG tRo-, three-, aGO CoDr-OXJXt JroDUP, CroZ 11 to4444, aGO DPeO thePe aP 336 coOeJroDUP Cor a PZaSS coOe. "XG thXP taASe,accorOXGJ to aJreeZeGt, Re PhaSS eGter XG the KarXoDP SXGeP at theGDZAerP RhateKer coZUSete UhraPeP Re USeaPe, Cor eYaZUSe,correPUoGOXGJ to 12, 'Re haKe ZaOe reaOF the PhXUP RhXch Re UroZXPeOaGO PDUUSXeO theZ RXth trooUP aGO JraXG.' " thePe coOe KaSDeP OXO GotchaGJe, aGF Zore thaG the ZXYeO aSUhaAet oC the OXPL OXO. ADt the OXJXtPrePDStXGJ CroZ aG eGcoOXGJ Rere theG eGcXUhereO RXth the OXPL EDPt aP XCtheF Rere USaXGteYt SetterP. XG aSAertX'P RorOP, "thePe GDZAerP X theGXGPert XG ZF ZePPaJe accorOXGJ to the CorZDSa oC the cXUher, reUrePeGtXGJtheZ AF the SetterP that OeGote thePe GDZAerP." thePe GDZAerP thDPchaGJeO theXr cXUherteYt eBDXKaSeGtP aP the OXPL tDrGeO. heGce 341,UerhaUP ZeaGXGJ "UoUe," ZXJht AecoZe ZrU at oGe UoPXtXoG aGO Cco ataGother. thXP coGPtXtDteP aG eYceSSeGt CorZ oC eGcXUhereO coOe, aGO EDPthoR UrecocXoDP aSAertX RaP ZaF Ae PeeG AF the Cact that the ZaEorUoRerP oC the earth OXO Got AeJXG to eGcXUher theXr coOe ZePPaJeP DGtXS400 FearP Sater, Gear the eGO oC the 19th ceGtDrF, aGO eKeG theG theXrPFPteZP Rere ZDch PXZUSer thaG thXP.aSAertX'P three reZarLaASe CXrPtP—the earSXePt RePterG eYUoPXtXoG oCcrFUtaGaSFPXP, the XGKeGtXoG oC UoSFaSUhaAetXe PDAPtXtDtXoG, aGO theXGKeGtXoG oC eGcXUhereO coOe—ZaLe hXZ the Cather oC RePterGcrFUtoSoJF. ADt aSthoDJh hXP treatXPe RaP UDASXPheO XG XtaSXaG XG acoSSectXoG oC hXP RorLP XG 1568, aGO aSthoDJh hXP XOeaP Rere aAPorAeO AFUaUaS crFUtoSoJXPtP aGO UerhaUP XGCSDeGceO the PcXeGce'P OeKeSoUZeGt,theF GeKer haO the OFGaZXc XZUact that PDch UroOXJXoDPaccoZUSXPhZeGtP oDJht to haKe UroODceO. PFZoGOP' eKaSDatXoG oC hXPRorL XG JeGeraS ZaF Aoth eYUSaXG RhF aGO PDZZarXMe the

ZoOerG KXeR oC hXP crFUtoSoJXcaS coGtrXADtXoGP:"thXP ZaG oC ZaGF-PXOeO JeGXDP caZe XGto the RorSO too PooG Cor theUerCect eYercXPe oC hXP PXGJDSar CacDStXeP. Rhether Re reJarO hXZ CroZ theUoXGt oC KXeR oC art, oC PcXeGce, or oC SXteratDre, he occDUXeP XG eachOeUartZeGt the UoPXtXoG oC UrecDrPor, UXoGeer, aGO XGOXcator. aSRaFPorXJXGaS aGO aSRaFP CertXSe, he UroUhePXeO oC SaGOP he RaP Got UrXKXSeJeOto eGter, SeaKXGJ the ZeZorF oC OXZ aGO KarXeO JreatGePP rather thaG aGFPoSXO ZoGDZeGt AehXGO hXZ."UoSFaSUhaAetXcXtF tooL aGother PteU CorRarO XG 1518, RXth theaUUearaGce oC the CXrPt UrXGteO AooL oG crFUtoSoJF, RrXtteG AF oGe oC theZoPt CaZoDP XGteSSectDaSP oC hXP OaF. thXP RaP EohaGGeP trXtheZXDP, aAeGeOXctXGe ZoGL RhoPe OaAASXGJ XG aScheZF aGO other ZFPtXc UoRerPZaOe hXZ oGe oC the ZoPt reKereO CXJDreP XG occDSt PcXeGce, RhXSe hXPZore PoSXO PchoSarPhXU RoG hXZ the tXtSe oC "Cather oC AXAXSXoJraUhF." XG1518, a Fear aGO a haSC aCter hXP Oeath, hXP UoSFJraUhXae SXArX PeY, SoaGGXPtrXtheZXX aAAatXP UeaUoSXtaGX, BDoGOaZ PUaGheXZeGPXP, aO ZaYXZXSXaGDZcaePareZ ("PXY AooLP oC UoSFJraUhF, AF EohaGGeP trXtheZXDP, aAAot atRDrMADrJ, CorZerSF at PUaGheXZ, Cor the eZUeror ZaYXZXSXaG") RaPUDASXPheO. AF Car the ADSL oC the KoSDZe coGPXPtP oC the coSDZGP oCRorOP UrXGteO XG SarJe JothXc tFUe that trXtheZXDP DPeO XG hXP PFPteZP oCcrFUtoJraUhF. ADt XG the RorL'P AooL K aUUearP, Cor the CXrPt tXZe, thePBDare taASe, or taASeaD. thXP XP the eSeZeGtaS CorZ oC UoSFaSUhaAetXcPDAPtXtDtXoG, Cor Xt eYhXAXtP aSS at oGce aSS the cXUher aSUhaAetP XG aUartXcDSar PFPteZ. thePe are DPDaSSF aSS the PaZe PeBDeGce oC SetterP, ADtPhXCteO to OXCCereGt UoPXtXoGP XG reSatXoG to the USaXGteYt aSUhaAet, aP XGaSAertX'P OXPL the XGGer aSUhaAet aPPDZeO OXCCereGt UoPXtXoGP XG reJarO tothe oDter aSUhaAet. the taASeaD PetP theZ oDt XG orOerSF CaPhXoG—theaSUhaAetP oC the PDccePPXKe UoPXtXoGP SaXO oDt XG roRP oGe AeSoR theother, each aSUhaAet PhXCteO oGe USace to the SeCt oC the oGe aAoKe. eachroR thDP oCCerP a OXCCereGt Pet oC cXUher PDAPtXtDteP to the SetterP oC theUSaXGteYt aSUhaAet at the toU. PXGce there caG Ae oGSF aP ZaGF roRP aPthere are SetterP XG the aSUhaAet, the taASeaD XP PBDare.the PXZUSePt taASeaD XP oGe that DPeP the GorZaS aSUhaAet XG KarXoDPUoPXtXoGP aP the cXUher aSUhaAetP. each cXUher aSUhaAet UroODceP, XGother RorOP, a caePar PDAPtXtDtXoG.

5. G→n; J→g; O→d; “reJarO to oGe aGother” resembles the expresion “regard to one another”

c = each neR PettXng oC aSAertX'P dXPL AroDght Xnto USaF a neR cXUheraSUhaAet, Xn RhXch Aoth the USaXnteYt and the cXUherteYt eBDXKaSentP arechanged Xn regard to one another. there are aP ZanF oC thePe aSUhaAetPaP there are UoPXtXonP oC hXP dXPL, and thXP ZDStXUSXcXtF ZeanP that aSAertXhere deKXPed the CXrPt UoSFaSUhaAetXc cXUher.thXP achXeKeZent—crXtXcaS Xn the hXPtorF oC crFUtoSogF —aSAertX thenadorned AF another reZarLaASe XnKentXon: encXUhered code. Xt RaP CorthXP that he had UDt nDZAerP Xn the oDter rXng. Xn a taASe he UerZDtedthe nDZAerP 1 to 4 Xn tRo-, three-, and CoDr-dXgXt groDUP, CroZ 11 to4444, and DPed thePe aP 336 codegroDUP Cor a PZaSS code. "Xn thXP taASe,accordXng to agreeZent, Re PhaSS enter Xn the KarXoDP SXneP at thenDZAerP RhateKer coZUSete UhraPeP Re USeaPe, Cor eYaZUSe,correPUondXng to 12, 'Re haKe Zade readF the PhXUP RhXch Re UroZXPedand PDUUSXed theZ RXth trooUP and graXn.' " thePe code KaSDeP dXd notchange, anF Zore than the ZXYed aSUhaAet oC the dXPL dXd. ADt the dXgXtPrePDStXng CroZ an encodXng Rere then encXUhered RXth the dXPL EDPt aP XCtheF Rere USaXnteYt SetterP. Xn aSAertX'P RordP, "thePe nDZAerP X thenXnPert Xn ZF ZePPage accordXng to the CorZDSa oC the cXUher, reUrePentXngtheZ AF the SetterP that denote thePe nDZAerP." thePe nDZAerP thDPchanged theXr cXUherteYt eBDXKaSentP aP the dXPL tDrned. hence 341,UerhaUP ZeanXng "UoUe," ZXght AecoZe ZrU at one UoPXtXon and Cco atanother. thXP conPtXtDteP an eYceSSent CorZ oC encXUhered code, and EDPthoR UrecocXoDP aSAertX RaP ZaF Ae Peen AF the Cact that the ZaEorUoRerP oC the earth dXd not AegXn to encXUher theXr code ZePPageP

DntXS400 FearP Sater, near the end oC the 19th centDrF, and eKen then theXrPFPteZP Rere ZDch PXZUSer than thXP.aSAertX'P three reZarLaASe CXrPtP—the earSXePt RePtern eYUoPXtXon oCcrFUtanaSFPXP, the XnKentXon oC UoSFaSUhaAetXe PDAPtXtDtXon, and theXnKentXon oC encXUhered code—ZaLe hXZ the Cather oC RePterncrFUtoSogF. ADt aSthoDgh hXP treatXPe RaP UDASXPhed Xn XtaSXan Xn acoSSectXon oC hXP RorLP Xn 1568, and aSthoDgh hXP XdeaP Rere aAPorAed AFUaUaS crFUtoSogXPtP and UerhaUP XnCSDenced the PcXence'P deKeSoUZent,theF neKer had the dFnaZXc XZUact that PDch UrodXgXoDPaccoZUSXPhZentP oDght to haKe UrodDced. PFZondP' eKaSDatXon oC hXPRorL Xn generaS ZaF Aoth eYUSaXn RhF and PDZZarXMe the Zodern KXeR oC hXP crFUtoSogXcaS contrXADtXonP:"thXP Zan oC ZanF-PXded genXDP caZe Xnto the RorSd too Poon Cor theUerCect eYercXPe oC hXP PXngDSar CacDStXeP. Rhether Re regard hXZ CroZ theUoXnt oC KXeR oC art, oC PcXence, or oC SXteratDre, he occDUXeP Xn eachdeUartZent the UoPXtXon oC UrecDrPor, UXoneer, and XndXcator. aSRaFPorXgXnaS and aSRaFP CertXSe, he UroUhePXed oC SandP he RaP not UrXKXSegedto enter, SeaKXng the ZeZorF oC dXZ and KarXed greatnePP rather than anFPoSc = each neR PettXng oC aSAertX'P dXPL AroDght Xnto USaF a neR cXUheraSUhaAet, Xn RhXch Aoth the USaXnteYt and the cXUherteYt eBDXKaSentP arechanged Xn regard to one another. there are aP ZanF oC thePe aSUhaAetPaP there are UoPXtXonP oC hXP dXPL, and thXP ZDStXUSXcXtF ZeanP that aSAertXhere deKXPed the CXrPt UoSFaSUhaAetXc cXUher.thXP achXeKeZent—crXtXcaS Xn the hXPtorF oC crFUtoSogF —aSAertX thenadorned AF another reZarLaASe XnKentXon: encXUhered code. Xt RaP CorthXP that he had UDt nDZAerP Xn the oDter rXng. Xn a taASe he UerZDtedthe nDZAerP 1 to 4 Xn tRo-, three-, and CoDr-dXgXt groDUP, CroZ 11 to4444, and DPed thePe aP 336 codegroDUP Cor a PZaSS code. "Xn thXP taASe,accordXng to agreeZent, Re PhaSS enter Xn the KarXoDP SXneP at thenDZAerP RhateKer coZUSete UhraPeP Re USeaPe, Cor eYaZUSe,correPUondXng to 12, 'Re haKe Zade readF the PhXUP RhXch Re UroZXPedand PDUUSXed theZ RXth trooUP and graXn.' " thePe code KaSDeP dXd notchange, anF Zore than the ZXYed aSUhaAet oC the dXPL dXd. ADt the dXgXtPrePDStXng CroZ an encodXng Rere then encXUhered RXth the dXPL EDPt aP XCtheF Rere USaXnteYt SetterP. Xn aSAertX'P RordP, "thePe nDZAerP X thenXnPert Xn ZF ZePPage accordXng to the CorZDSa oC the cXUher, reUrePentXngtheZ AF the SetterP that denote thePe nDZAerP." thePe nDZAerP thDPchanged theXr cXUherteYt eBDXKaSentP aP the dXPL tDrned. hence 341,UerhaUP ZeanXng "UoUe," ZXght AecoZe ZrU at one UoPXtXon and Cco atanother. thXP conPtXtDteP an eYceSSent CorZ oC encXUhered code, and EDPthoR UrecocXoDP aSAertX RaP ZaF Ae Peen AF the Cact that the ZaEorUoRerP oC the earth dXd not AegXn to encXUher theXr code ZePPageP DntXS400 FearP Sater, near the end oC the 19th centDrF, and eKen then theXrPFPteZP Rere ZDch PXZUSer than thXP.aSAertX'P three reZarLaASe CXrPtP—the earSXePt RePtern eYUoPXtXon oCcrFUtanaSFPXP, the XnKentXon oC UoSFaSUhaAetXe PDAPtXtDtXon, and theXnKentXon oC encXUhered code—ZaLe hXZ the Cather oC RePterncrFUtoSogF. ADt aSthoDgh hXP treatXPe RaP UDASXPhed Xn XtaSXan Xn acoSSectXon oC hXP RorLP Xn 1568, and aSthoDgh hXP XdeaP Rere aAPorAed AFUaUaS crFUtoSogXPtP and UerhaUP XnCSDenced the PcXence'P deKeSoUZent,theF neKer had the dFnaZXc XZUact that PDch UrodXgXoDPaccoZUSXPhZentP oDght to haKe UrodDced. PFZondP' eKaSDatXon oC hXPRorL Xn generaS ZaF Aoth eYUSaXn RhF and PDZZarXMe the Zodern KXeR oC hXP crFUtoSogXcaS contrXADtXonP:"thXP Zan oC ZanF-PXded genXDP caZe Xnto the RorSd too Poon Cor theUerCect eYercXPe oC hXP PXngXd ZonDZent AehXnd hXZ."UoSFaSUhaAetXcXtF tooL another PteU CorRard Xn 1518, RXth theaUUearance oC the CXrPt UrXnted AooL on crFUtoSogF, RrXtten AF one oC theZoPt CaZoDP XnteSSectDaSP oC hXP daF. thXP RaP EohanneP trXtheZXDP, aAenedXctXne ZonL RhoPe daAASXng Xn aScheZF and other ZFPtXc UoRerPZade hXZ one oC the ZoPt reKered CXgDreP Xn occDSt PcXence, RhXSe hXPZore PoSXd PchoSarPhXU Ron hXZ the tXtSe oC "Cather oC AXAXSXograUhF." Xn1518, a Fear and a haSC aCter hXP death, hXP UoSFgraUhXae SXArX PeY, SoannXPtrXtheZXX aAAatXP UeaUoSXtanX, BDondaZ PUanheXZenPXP, ad ZaYXZXSXanDZcaePareZ ("PXY AooLP oC UoSFgraUhF, AF EohanneP trXtheZXDP, aAAot

atRDrMADrg, CorZerSF at PUanheXZ, Cor the eZUeror ZaYXZXSXan") RaPUDASXPhed. AF Car the ADSL oC the KoSDZe conPXPtP oC the coSDZnP oCRordP UrXnted Xn Sarge gothXc tFUe that trXtheZXDP DPed Xn hXP PFPteZP oCcrFUtograUhF. ADt Xn the RorL'P AooL K aUUearP, Cor the CXrPt tXZe, thePBDare taASe, or taASeaD. thXP XP the eSeZentaS CorZ oC UoSFaSUhaAetXcPDAPtXtDtXon, Cor Xt eYhXAXtP aSS at once aSS the cXUher aSUhaAetP Xn aUartXcDSar PFPteZ. thePe are DPDaSSF aSS the PaZe PeBDence oC SetterP, ADtPhXCted to dXCCerent UoPXtXonP Xn reSatXon to the USaXnteYt aSUhaAet, aP XnaSAertX'P dXPL the Xnner aSUhaAet aPPDZed dXCCerent UoPXtXonP Xn regard tothe oDter aSUhaAet. the taASeaD PetP theZ oDt Xn orderSF CaPhXon—theaSUhaAetP oC the PDccePPXKe UoPXtXonP SaXd oDt Xn roRP one AeSoR theother, each aSUhaAet PhXCted one USace to the SeCt oC the one aAoKe. eachroR thDP oCCerP a dXCCerent Pet oC cXUher PDAPtXtDteP to the SetterP oC theUSaXnteYt aSUhaAet at the toU. PXnce there can Ae onSF aP ZanF roRP aPthere are SetterP Xn the aSUhaAet, the taASeaD XP PBDare.the PXZUSePt taASeaD XP one that DPeP the norZaS aSUhaAet Xn KarXoDPUoPXtXonP aP the cXUher aSUhaAetP. each cXUher aSUhaAet UrodDceP, Xnother RordP, a caePar PDAPtXtDtXon.

6. X→i; P→s; F→y; C->f; “Xn the hXPtorF oC” resembles the expression “in the history of”

c = each neR setting of aSAerti's disL AroDght into USay a neR ciUheraSUhaAet, in Rhich Aoth the USainteYt and the ciUherteYt eBDiKaSents arechanged in regard to one another. there are as Zany of these aSUhaAetsas there are Uositions of his disL, and this ZDStiUSicity Zeans that aSAertihere deKised the first UoSyaSUhaAetic ciUher.this achieKeZent—criticaS in the history of cryUtoSogy — aSAerti thenadorned Ay another reZarLaASe inKention: enciUhered code. it Ras forthis that he had UDt nDZAers in the oDter ring. in a taASe he UerZDtedthe nDZAers 1 to 4 in tRo-, three-, and foDr-digit groDUs, froZ 11 to4444, and Dsed these as 336 codegroDUs for a sZaSS code. "in this taASe,according to agreeZent, Re shaSS enter in the KarioDs Sines at thenDZAers RhateKer coZUSete Uhrases Re USease, for eYaZUSe,corresUonding to 12, 'Re haKe Zade ready the shiUs Rhich Re UroZisedand sDUUSied theZ Rith trooUs and grain.' " these code KaSDes did notchange, any Zore than the ZiYed aSUhaAet of the disL did. ADt the digitsresDSting froZ an encoding Rere then enciUhered Rith the disL EDst as ifthey Rere USainteYt Setters. in aSAerti's Rords, "these nDZAers i theninsert in Zy Zessage according to the forZDSa of the ciUher, reUresentingtheZ Ay the Setters that denote these nDZAers." these nDZAers thDschanged their ciUherteYt eBDiKaSents as the disL tDrned. hence 341,UerhaUs Zeaning "UoUe," Zight AecoZe ZrU at one Uosition and fco atanother. this constitDtes an eYceSSent forZ of enciUhered code, and EDsthoR UrecocioDs aSAerti Ras Zay Ae seen Ay the fact that the ZaEorUoRers of the earth did not Aegin to enciUher their code Zessages DntiS400 years Sater, near the end of the 19th centDry, and eKen then theirsysteZs Rere ZDch siZUSer than this.aSAerti's three reZarLaASe firsts—the earSiest Restern eYUosition ofcryUtanaSysis, the inKention of UoSyaSUhaAetie sDAstitDtion, and theinKention of enciUhered code—ZaLe hiZ the father of ResterncryUtoSogy. ADt aSthoDgh his treatise Ras UDASished in itaSian in acoSSection of his RorLs in 1568, and aSthoDgh his ideas Rere aAsorAed AyUaUaS cryUtoSogists and UerhaUs infSDenced the science's deKeSoUZent,they neKer had the dynaZic iZUact that sDch UrodigioDsaccoZUSishZents oDght to haKe UrodDced. syZonds' eKaSDation of hisRorL in generaS Zay Aoth eYUSain Rhy and sDZZariMe the Zodern KieR of his cryUtoSogicaS contriADtions:"this Zan of Zany-sided geniDs caZe into the RorSd too soon for theUerfect eYercise of his singDSar facDSties. Rhether Re regard hiZ froZ theUoint of KieR of art, of science, or of SiteratDre, he occDUies in eachdeUartZent the Uosition of UrecDrsor, Uioneer, and indicator. aSRaysoriginaS and aSRays fertiSe, he UroUhesied of Sands he Ras not UriKiSegedto enter, SeaKing the ZeZory of diZ and Karied greatness rather than anysoSid ZonDZent Aehind hiZ."UoSyaSUhaAeticity tooL another steU forRard in 1518, Rith theaUUearance of the first Urinted AooL on cryUtoSogy, Rritten Ay one of theZost faZoDs inteSSectDaSs of his day. this Ras Eohannes tritheZiDs, aAenedictine ZonL Rhose daAASing in aScheZy and other Zystic UoRersZade hiZ one of the Zost reKered figDres in occDSt science, RhiSe hisZore soSid schoSarshiU Ron hiZ the titSe of

"father of AiAiSiograUhy." in1518, a year and a haSf after his death, his UoSygraUhiae SiAri seY, SoannistritheZii aAAatis UeaUoSitani, BDondaZ sUanheiZensis, ad ZaYiZiSianDZcaesareZ ("siY AooLs of UoSygraUhy, Ay Eohannes tritheZiDs, aAAot atRDrMADrg, forZerSy at sUanheiZ, for the eZUeror ZaYiZiSian") RasUDASished. Ay far the ADSL of the KoSDZe consists of the coSDZns ofRords Urinted in Sarge gothic tyUe that tritheZiDs Dsed in his systeZs ofcryUtograUhy. ADt in the RorL's AooL K aUUears, for the first tiZe, thesBDare taASe, or taASeaD. this is the eSeZentaS forZ of UoSyaSUhaAeticsDAstitDtion, for it eYhiAits aSS at once aSS the ciUher aSUhaAets in aUarticDSar systeZ. these are DsDaSSy aSS the saZe seBDence of Setters, ADtshifted to different Uositions in reSation to the USainteYt aSUhaAet, as inaSAerti's disL the inner aSUhaAet assDZed different Uositions in regard tothe oDter aSUhaAet. the taASeaD sets theZ oDt in orderSy fashion—theaSUhaAets of the sDccessiKe Uositions Said oDt in roRs one AeSoR theother, each aSUhaAet shifted one USace to the Seft of the one aAoKe. eachroR thDs offers a different set of ciUher sDAstitDtes to the Setters of theUSainteYt aSUhaAet at the toU. since there can Ae onSy as Zany roRs asthere are Setters in the aSUhaAet, the taASeaD is sBDare.the siZUSest taASeaD is one that Dses the norZaS aSUhaAet in KarioDsUositions as the ciUher aSUhaAets. each ciUher aSUhaAet UrodDces, inother Rords, a caesar sDAstitDtion.

7. R→w; L→k; A→b; U→p; S→l; Y→x; “neR”, “Rhich”, “disL”, “Aoth” and “UsainteYt” resemble the words “new”, “which”, “disk”, “both” and “plaintext”

c = each new setting of alberti's disk broDght into play a new cipheralphabet, in which both the plaintext and the ciphertext eBDiKalents arechanged in regard to one another. there are as Zany of these alphabetsas there are positions of his disk, and this ZDltiplicity Zeans that albertihere deKised the first polyalphabetic cipher.this achieKeZent—critical in the history of cryptology —alberti thenadorned by another reZarkable inKention: enciphered code. it was forthis that he had pDt nDZbers in the oDter ring. in a table he perZDtedthe nDZbers 1 to 4 in two-, three-, and foDr-digit groDps, froZ 11 to4444, and Dsed these as 336 codegroDps for a sZall code. "in this table,according to agreeZent, we shall enter in the KarioDs lines at thenDZbers whateKer coZplete phrases we please, for exaZple,corresponding to 12, 'we haKe Zade ready the ships which we proZisedand sDpplied theZ with troops and grain.' " these code KalDes did notchange, any Zore than the Zixed alphabet of the disk did. bDt the digitsresDlting froZ an encoding were then enciphered with the disk EDst as ifthey were plaintext letters. in alberti's words, "these nDZbers i theninsert in Zy Zessage according to the forZDla of the cipher, representingtheZ by the letters that denote these nDZbers." these nDZbers thDschanged their ciphertext eBDiKalents as the disk tDrned. hence 341,perhaps Zeaning "pope," Zight becoZe Zrp at one position and fco atanother. this constitDtes an excellent forZ of enciphered code, and EDsthow precocioDs alberti was Zay be seen by the fact that the ZaEorpowers of the earth did not begin to encipher their code Zessages Dntil400 years later, near the end of the 19th centDry, and eKen then theirsysteZs were ZDch siZpler than this.alberti's three reZarkable firsts—the earliest western exposition ofcryptanalysis, the inKention of polyalphabetie sDbstitDtion, and theinKention of enciphered code—Zake hiZ the father of westerncryptology. bDt althoDgh his treatise was pDblished in italian in acollection of his works in 1568, and althoDgh his ideas were absorbed bypapal cryptologists and perhaps inflDenced the science's deKelopZent,they neKer had the dynaZic iZpact that sDch prodigioDsaccoZplishZents oDght to haKe prodDced. syZonds' eKalDation of hiswork in general Zay both explain why and sDZZariMe the Zodern Kiew of his cryptological contribDtions:"this Zan of Zany-sided geniDs caZe into the world too soon for theperfect exercise of his singDlar facDlties. whether we regard hiZ froZ thepoint of Kiew of art, of science, or of literatDre, he occDpies in eachdepartZent the position of precDrsor, pioneer, and indicator. alwaysoriginal and always fertile, he prophesied of lands he was not priKilegedto enter, leaKing the ZeZory of diZ and Karied greatness rather than anysolid ZonDZent behind hiZ."polyalphabeticity took another step forward in 1518, with theappearance of the first printed book on cryptology, written by one of theZost faZoDs intellectDals of his day. this was Eohannes tritheZiDs, abenedictine Zonk whose dabbling in alcheZy and other Zystic powersZade hiZ one of the Zost reKered figDres in occDlt science, while

hisZore solid scholarship won hiZ the title of "father of bibiliography." in1518, a year and a half after his death, his polygraphiae libri sex, loannistritheZii abbatis peapolitani, BDondaZ spanheiZensis, ad ZaxiZilianDZcaesareZ ("six books of polygraphy, by Eohannes tritheZiDs, abbot atwDrMbDrg, forZerly at spanheiZ, for the eZperor ZaxiZilian") waspDblished. by far the bDlk of the KolDZe consists of the colDZns ofwords printed in large gothic type that tritheZiDs Dsed in his systeZs ofcryptography. bDt in the work's book K appears, for the first tiZe, thesBDare table, or tableaD. this is the eleZental forZ of polyalphabeticsDbstitDtion, for it exhibits all at once all the cipher alphabets in aparticDlar systeZ. these are DsDally all the saZe seBDence of letters, bDtshifted to different positions in relation to the plaintext alphabet, as inalberti's disk the inner alphabet assDZed different positions in regard tothe oDter alphabet. the tableaD sets theZ oDt in orderly fashion—thealphabets of the sDccessiKe positions laid oDt in rows one below theother, each alphabet shifted one place to the left of the one aboKe. eachrow thDs offers a different set of cipher sDbstitDtes to the letters of theplaintext alphabet at the top. since there can be only as Zany rows asthere are letters in the alphabet, the tableaD is sBDare.the siZplest tableaD is one that Dses the norZal alphabet in KarioDspositions as the cipher alphabets. each cipher alphabet prodDces, inother words, a caesar sDbstitDtion.

8. Z→m; D→u; K→v “Zany”, “ZDltiplicity”, “nDZbers” and “KarioDs” resemble the words “many”, “multiplicity”, “numbers” and “various”

c = each new setting of alberti's disk brought into play a new cipheralphabet, in which both the plaintext and the ciphertext eBuivalents arechanged in regard to one another. there are as many of these alphabetsas there are positions of his disk, and this multiplicity means that albertihere devised the first polyalphabetic cipher.this achievement—critical in the history of cryptology —alberti thenadorned by another remarkable invention: enciphered code. it was forthis that he had put numbers in the outer ring. in a table he permutedthe numbers 1 to 4 in two-, three-, and four-digit groups, from 11 to4444, and used these as 336 codegroups for a small code. "in this table,according to agreement, we shall enter in the various lines at thenumbers whatever complete phrases we please, for example,corresponding to 12, 'we have made ready the ships which we promisedand supplied them with troops and grain.' " these code values did notchange, any more than the mixed alphabet of the disk did. but the digitsresulting from an encoding were then enciphered with the disk Eust as ifthey were plaintext letters. in alberti's words, "these numbers i theninsert in my message according to the formula of the cipher, representingthem by the letters that denote these numbers." these numbers thuschanged their ciphertext eBuivalents as the disk turned. hence 341,perhaps meaning "pope," might become mrp at one position and fco atanother. this constitutes an excellent form of enciphered code, and Eusthow precocious alberti was may be seen by the fact that the maEorpowers of the earth did not begin to encipher their code messages until400 years later, near the end of the 19th century, and even then theirsystems were much simpler than this.alberti's three remarkable firsts—the earliest western exposition ofcryptanalysis, the invention of polyalphabetie substitution, and theinvention of enciphered code—make him the father of westerncryptology. but although his treatise was published in italian in acollection of his works in 1568, and although his ideas were absorbed bypapal cryptologists and perhaps influenced the science's development,they never had the dynamic impact that such prodigiousaccomplishments ought to have produced. symonds' evaluation of hiswork in general may both explain why and summariMe the modern view of his cryptological contributions:"this man of many-sided genius came into the world too soon for theperfect exercise of his singular faculties. whether we regard him from thepoint of view of art, of science, or of literature, he occupies in eachdepartment the position of precursor, pioneer, and indicator. alwaysoriginal and always fertile, he prophesied of lands he was not privilegedto enter, leaving the memory of dim and varied greatness rather than anysolid monument behind him."polyalphabeticity took another step forward in 1518, with theappearance of the first printed book on cryptology, written by one of themost famous intellectuals of his day. this was Eohannes trithemius, abenedictine monk whose dabbling in alchemy and other mystic powersmade him one of the most revered figures in occult

science, while hismore solid scholarship won him the title of "father of bibiliography." in1518, a year and a half after his death, his polygraphiae libri sex, loannistrithemii abbatis peapolitani, Buondam spanheimensis, ad maximilianumcaesarem ("six books of polygraphy, by Eohannes trithemius, abbot atwurMburg, formerly at spanheim, for the emperor maximilian") waspublished. by far the bulk of the volume consists of the columns ofwords printed in large gothic type that trithemius used in his systems ofcryptography. but in the work's book v appears, for the first time, thesBuare table, or tableau. this is the elemental form of polyalphabeticsubstitution, for it exhibits all at once all the cipher alphabets in aparticular system. these are usually all the same seBuence of letters, butshifted to different positions in relation to the plaintext alphabet, as inalberti's disk the inner alphabet assumed different positions in regard tothe outer alphabet. the tableau sets them out in orderly fashion—thealphabets of the successive positions laid out in rows one below theother, each alphabet shifted one place to the left of the one above. eachrow thus offers a different set of cipher substitutes to the letters of theplaintext alphabet at the top. since there can be only as many rows asthere are letters in the alphabet, the tableau is sBuare.the simplest tableau is one that uses the normal alphabet in variouspositions as the cipher alphabets. each cipher alphabet produces, inother words, a caesar substitution.

9. B→q; E→j; M→z “eBuivalents”, “Eust” and “summariMe” resemble the words “equivalents”, “just” and “summarize”

c = each new setting of alberti's disk brought into play a new cipheralphabet, in which both the plaintext and the ciphertext equivalents arechanged in regard to one another. there are as many of these alphabetsas there are positions of his disk, and this multiplicity means that albertihere devised the first polyalphabetic cipher.this achievement—critical in the history of cryptology —alberti thenadorned by another remarkable invention: enciphered code. it was forthis that he had put numbers in the outer ring. in a table he permutedthe numbers 1 to 4 in two-, three-, and four-digit groups, from 11 to4444, and used these as 336 codegroups for a small code. "in this table,according to agreement, we shall enter in the various lines at thenumbers whatever complete phrases we please, for example,corresponding to 12, 'we have made ready the ships which we promisedand supplied them with troops and grain.' " these code values did notchange, any more than the mixed alphabet of the disk did. but the digitsresulting from an encoding were then enciphered with the disk just as ifthey were plaintext letters. in alberti's words, "these numbers i theninsert in my message according to the formula of the cipher, representingthem by the letters that denote these numbers." these numbers thuschanged their ciphertext equivalents as the disk turned. hence 341,perhaps meaning "pope," might become mrp at one position and fco atanother. this constitutes an excellent form of enciphered code, and justhow precocious alberti was may be seen by the fact that the majorpowers of the earth did not begin to encipher their code messages until400 years later, near the end of the 19th century, and even then theirsystems were much simpler than this.alberti's three remarkable firsts—the earliest western exposition ofcryptanalysis, the invention of polyalphabetie substitution, and theinvention of enciphered code—make him the father of westerncryptology. but although his treatise was published in italian in acollection of his works in 1568, and although his ideas were absorbed bypapal cryptologists and perhaps influenced the science's development,they never had the dynamic impact that such prodigiousaccomplishments ought to have produced. symonds' evaluation of hiswork in general may both explain why and summarize the modern view of his cryptological contributions:"this man of many-sided genius came into the world too soon for theperfect exercise of his singular faculties. whether we regard him from thepoint of view of art, of science, or of literature, he occupies in eachdepartment the position of precursor, pioneer, and indicator. alwaysoriginal and always fertile, he prophesied of lands he was not privilegedto enter, leaving the memory of dim and varied greatness rather than anysolid monument behind him."polyalphabeticity took another step forward in 1518, with theappearance of the first printed book on cryptology, written by one of themost famous intellectuals of his day. this was johannes trithemius, abenedictine monk whose dabbling in alchemy and other mystic powersmade him one of the most revered figures in occult

science, while hismore solid scholarship won him the title of "father of bibiliography." in1518, a year and a half after his death, his polygraphiae libri sex, loannistrithemii abbatis peapolitani, quondam spanheimensis, ad maximilianumcaesarem ("six books of polygraphy, by johannes trithemius, abbot atwurzburg, formerly at spanheim, for the emperor maximilian") waspublished. by far the bulk of the volume consists of the columns ofwords printed in large gothic type that trithemius used in his systems ofcryptography. but in the work's book v appears, for the first time, thesquare table, or tableau. this is the elemental form of polyalphabeticsubstitution, for it exhibits all at once all the cipher alphabets in aparticular system. these are usually all the same sequence of letters, butshifted to different positions in relation to the plaintext alphabet, as inalberti's disk the inner alphabet assumed different positions in regard tothe outer alphabet. the tableau sets them out in orderly fashion—thealphabets of the successive positions laid out in rows one below theother, each alphabet shifted one place to the left of the one above. eachrow thus offers a different set of cipher substitutes to the letters of theplaintext alphabet at the top. since there can be only as many rows asthere are letters in the alphabet, the tableau is square.the simplest tableau is one that uses the normal alphabet in variouspositions as the cipher alphabets. each cipher alphabet produces, inother words, a caesar substitution.

Conclusions:

Due to each letter having a set frequency in every lanugate, and ecryption algorithm that uses direct substition can be decrypted by analyzing and substituting the letters that macth the frequencies and mach commonly met words.

Table 3: Final letter substitution for the provided text

V	W	T	X	N	P	Q	G	I	S	U	O	H
e	t	a	i	o	s	h	n	r	l	p	d	c

Z	D	C	A	F	R	J	K	L	Y	B	E	M
m	u	f	b	y	w	g	v	k	x	q	j	z

References:

1. Frequency analysis tool: https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html

2. Github repository: https://github.com/muffindud/CS_Lab/tree/lab2