MINISTRY OF EDUCATION, CULTURE AND RESEARCH OF REPUBLIC OF MOLDOVA
TECHNICAL UNIVERSITY OF MOLDOVA
FACULTY OF COMPUTERS, INFORMATICS AND MICROELECTRONICS
DEPARTMENT OF SOFTWARE ENGINEERING AND AUTOMATICS

Criptography and Security

Laboratory work 2: Cryptanalysis of monoalphabetic substitution

Elaborated:
st.gr. FAF-211 Coreţchi Mihai
Verified:
asist.univ. Cătălin Mîţu

Chișinău, 2023

Introduction

It was intercepted a encrypted message which is known to have been obtained using a monoalphabetic cipher. By applying the frequency analysis attack, determine the original message, assuming it is a text written in English. Keep in mind that only the letters were encrypted, with the other characters remaining unencrypted.

c = 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 ztgfpxovo 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 tgfpn-sxo 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 unrvipz-tov 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 Ztyxzxsxtgdz Htvptivz ("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 cx-ipw 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.

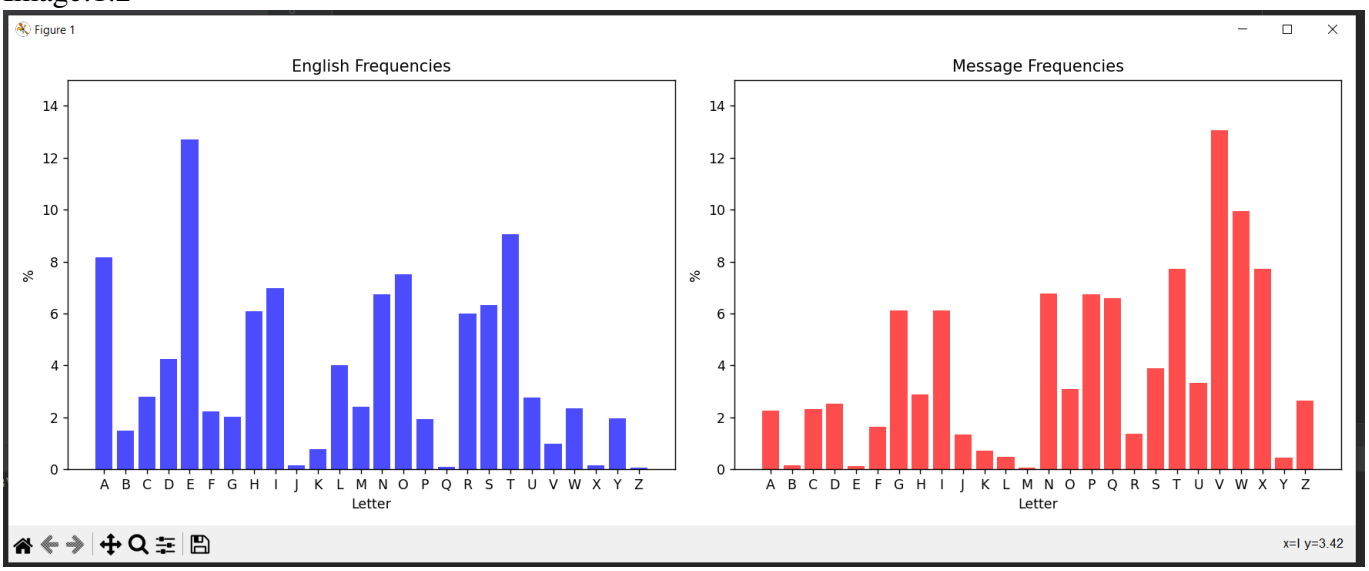
After ussing the site: *https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html* , I obtained this frequency of letters:

Image:1.1

V	W	T	X	N	P	Q	G	I	S	U	O	H	Z	D	C	A	F	R	J	K	L	Y	B	E	M
496	378	293	293	257	256	251	232	232	148	127	117	109	101	96	88	86	62	52	51	27	18	17	6	5	2
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	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
E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z

And the graphics of the encrypted text are in this way:

Image:1.2



The first step is to find the frequencies of all letters that appear in the cryptogram, as shown in Image 1.1. Below, we can observe the graphical representation of the letter frequencies in the English language (figure on the left) and the frequencies of letters in the intercepted message (figure on the right).

Now that we have all the letter frequencies from the encrypted text, we can start making some substitutions. We see that the most frequent letter in the encrypted text is ”V”, closely followed by ”W”. From the above figure and Tables, we can guess that these two letters represent ”E” and ”T” respectively. After making these substitutions, we obtain:

Image:1.3

V	W	T	X	N	P	Q	G	I	S	U	O	H	Z	D	C	A	F	R	J	K	L	Y	B	E	M
496	378	293	293	257	256	251	232	232	148	127	117	109	101	96	88	86	62	52	51	27	18	17	6	5	2
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	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
E	T	A	O	I	N	h	s	R	D	L	C	U	M	g	F	w	Y	P	B	V	K	J	X	Q	Z

My first approach was to investigate the frequency with which each letter appeared in the text. The English language, with its quirks and patterns, often shows a tendency for certain letters like ’e’, ’t’, and ’a’ to appear more frequently than others. This frequency distribution, an intrinsic property of the language, became my secret weapon in tackling this enigma. After calculating the frequency of each character in the encrypted message, I constructed a visual representation, placing it side-by-side with the standard frequency distribution of the English alphabet. This visual aid was vital, highlighting stark differences between normal English text and the encrypted message. The pattern was clear: certain characters in the encrypted text stood out, much like the commonly occurring letters in the English language. I hypothesized that the text was encrypted using a monoalphabetic substitution cipher. This is a method

where each letter in the plaintext is replaced by another letter with a fixed relationship. If my hypothesis was right, then the frequently appearing characters in the encrypted message could correspond to common English letters. Using this logic, I mapped the letters from the encrypted text to their potential English counterparts. This was a painstaking process of trial and error, as I adjusted my mappings based on the evolving decrypted message and its resemblance to coherent English. Throughout this process, I also paid heed to other linguistic clues. The appearance of common two-letter and three-letter words in English, like 'an', 'in', 'the', and 'and', further informed and refined my deciphering attempts. Once I felt confident in my mappings, I began the process of decryption in earnest, transforming the jumbled characters into discernible English text.

c = eauh sep nettosb if adgerto'n conk griwbht osti lday a sep uolheradlhaget, os phouh gith the ldaostejt asc the uolhertejt exwovadestn areuhasbec os rebarc ti ise asither. there are an masy if thene adlhagetnan there are linotoisn if hon conk, asc thon mwdtoldouoty measn that adgertohere cevonec the fornt lidyadlhagetou uolher.thon auhoevemest—urotouad os the hontiry if uryltidiby —adgerto thesacirsec gy asither remarkagde osvestois: esuolherec uice. ot pan firthon that he hac lwt swmgern os the iwter rosb. os a tagde he lermwtecthe swmgern 1 ti 4 os tpi-, three-, asc fiwr-cobot briwln, frim 11 ti4444, asc wnec thene an 336 uicebriwln fir a nmadd uice. "os thon tagde,auuircosb ti abreemest, pe nhadd ester os the varoiwn dosen at theswmgern phatever uimldete lhranen pe ldeane, fir ejamlde,uirrenliscosb ti 12, 'pe have mace reacy the nholn phouh pe lrimonecasc nwlldoec them poth triiln asc braos.' " thene uice vadwen coc situhasbe, asy mire thas the mojec adlhaget if the conk coc. gwt the cobotnrenwdtosb frim as esuicosb pere thes esuolherec poth the conk qwnt an ofthey pere ldaostejt dettern. os adgerto'n pircn, "thene swmgern o thesosnert os my mennabe auuircosb ti the firmwda if the uolher, relrenestosbthem gy the dettern that cesite thene swmgern." thene swmgern thwnuhasbec theor uolhertejt exwovadestn an the conk twrsec. hesue 341,lerhaln measosb "lile," mobht geuime mrl at ise linotois asc fui atasither. thon uisntotwten as ejueddest firm if esuolherec uice, asc qwnthip lreuiuoiwn adgerto pan may ge nees gy the faut that the maqirlipern if the earth coc sit gebos ti esuolher theor uice mennaben wstod400 yearn dater, sear the esc if the 19th uestwry, asc eves thes theornyntemn pere mwuh nomlder thas thon.adgerto'n three remarkagde forntn—the eardoent penters ejlinotois ifuryltasadynon, the osvestois if lidyadlhagetoe nwgntotwtois, asc theosvestois if esuolherec uice—make hom the father if pentersuryltidiby. gwt adthiwbh hon treatone pan lwgdonhec os otadoas os auiddeutois if hon pirkn os 1568, asc adthiwbh hon ocean pere agnirgec gylalad uryltidibontn asc lerhaln osfdwesuec the nuoesue'n cevedilmest,they sever hac the cysamou omlaut that nwuh lricoboiwnauuimldonhmestn iwbht ti have lricwuec. nymiscn' evadwatois if honpirk os beserad may gith ejldaos phy asc nwmmaroze the micers voep if hon uryltidibouad uistrogwtoisn:"thon mas if masy-nocec besown uame osti the pirdc tii niis fir thelerfeut ejeruone if hon nosbwdar fauwdtoen. phether pe rebarc hom frim theliost if voep if art, if nuoesue, ir if doteratwre, he

iuuwloen os eauhcelartmest the linotois if lreuwrnir, loiseer, asc oscouatir. adpaynirobosad asc adpayn fertode, he lrilhenoec if dascn he pan sit lrovodebecti ester, deavosb the memiry if com asc varoec breatsenn rather thas asynidoc miswmest gehosc hom."lidyadlhagetouoty tiik asither ntel firparc os 1518, poth theallearasue if the fornt lrostec giik is uryltidiby, prottes gy ise if themint famiwn osteddeutwadn if hon cay. thon pan qihassen trothemown, agesecoutose misk phine caggdosb os aduhemy asc ither myntou lipernmace hom ise if the mint reverec fobwren os iuuwdt nuoesue, phode honmire nidoc nuhidarnhol pis hom the totde if "father if gogodoibralhy." os1518, a year asc a hadf after hon ceath, hon lidybralhoae dogro nej, diassontrothemoo aggaton lealidotaso, xwiscam nlasheomesnon, ac majomodoaswmuaenarem ("noj giikn if lidybralhy, gy qihassen trothemown, aggit atpwrzgwrb, firmerdy at nlasheom, fir the emlerir majomodoas") panlwgdonhec. gy far the gwdk if the vidwme uisnontn if the uidwmsn ifpircn lrostec os darbe bithou tyle that trothemown wnec os hon nyntemn ifuryltibralhy. gwt os the pirk'n giik v allearn, fir the fornt tome, thenxware tagde, ir tagdeaw. thon on the edemestad firm if lidyadlhagetounwgntotwtois, fir ot ejhogotn add at isue add the uolher adlhagetn os alartouwdar nyntem. thene are wnwaddy add the name nexwesue if dettern, gwtnhoftec ti cofferest linotoisn os redatois ti the ldaostejt adlhaget, an osadgerto'n conk the osser adlhaget annwmec cofferest linotoisn os rebarc tithe iwter adlhaget. the tagdeaw netn them iwt os ircerdy fanhois—theadlhagetn if the nwuuennove linotoisn daoc iwt os ripn ise gedip theither, eauh adlhaget nhoftec ise ldaue ti the deft if the ise agive. eauhrip thwn iffern a cofferest net if uolher nwgntotwten ti the dettern if theldaostejt adlhaget at the til. nosue there uas ge isdy an masy ripn anthere are dettern os the adlhaget, the tagdeaw on nxware.the nomldent tagdeaw on ise that wnen the sirmad adlhaget os varoiwnlinotoisn an the uolher adlhagetn. eauh uolher adlhaget lricwuen, osither pircn, a uaenar nwgntotwtois.

c = eauh sew nettisb of adperti'n cink progbht isto lday a sew uilheradlhapet, is whiuh poth the ldaistejt asc the uilhertejt exgivadestn areuhasbec is rebarc to ose asother. there are an masy of thene adlhapetnan there are lonitiosn of hin cink, asc thin mgdtildiuity measn that adpertihere cevinec the firnt lodyadlhapetiu uilher.thin auhievemest—uritiuad is the hintory of uryltodoby —adperti thesacorsec py asother remarkapde isvestios: esuilherec uoce. it wan forthin that he hac lgt sgmpern is the ogter risb. is a tapde he lermgtecthe sgmpern 1 to 4 is two-, three-, asc fogr-cibit brogln, from 11 to4444, asc gnec thene an 336 uocebrogln for a nmadd uoce. "is thin tapde,auuorcisb to abreemest, we nhadd ester is the variogn disen at thesgmpern whatever uomldete lhranen we ldeane, for ejamlde,uorrenloscisb to 12, 'we have mace reacy the nhiln whiuh we lrominecasc nglldiec them with trooln asc brais.' " thene uoce vadgen cic sotuhasbe, asy more thas the mijec adlhapet of the cink cic. pgt the cibitnrengdtisb from as esuocisb were thes esuilherec with the cink qgnt an ifthey were ldaistejt dettern. is adperti'n worcn, "thene sgmpern i thesisnert is my mennabe auuorcisb to the formgda of the uilher, relrenestisbthem py the dettern that cesote thene sgmpern." thene sgmpern thgnuhasbec their uilhertejt exgivadestn an the cink tgrsec.

hesue 341,lerhaln measisb ”lole,” mibht peuome mrl at ose lonitios asc fuo atasother. thin uosntitgten as ejueddest form of esuilherec uoce, asc qgnthow lreuouiogn adperti wan may pe nees py the faut that the maqorlowern of the earth cic sot pebis to esuilher their uoce mennaben gstid400 yearn dater, sear the esc of the 19th uestgry, asc eves thes theirnyntemn were mguh nimlder thas thin.adperti’n three remarkapde firntn—the eardient wenters ejlonitios ofuryltasadynin, the isvestios of lodyadlhapetie ngpntitgtios, asc the-isvestios of esuilherec uoce—make him the father of wentersuryltodoby. pgt adthogbh hin treatine wan lgpdinhec is itadias is auoddeutios of hin workn is 1568, asc adthogbh hin icean were apnorpec pylalad uryltodobintn asc lerhaln isfdgesuec the nuiesue’n cevedolmest,they sever hac the cysamiu imlaut that nguh lrocibiognauuomldinhmestn ogbht to have lrocguec. nymoscn’ evadgatios of hinwork is beserad may poth ejldais why asc ngmmarize the mocers view of hin uryltodobiuad uostripgtiosn:”thin mas of masy-nicec besign uame isto the wordc too noos for thelerfeut ejeruine of hin nisbgdar faugdtien. whether we rebarc him from theloist of view of art, of nuiesue, or of diteratgre, he ouuglien is eauhcelartmest the lonitios of lreugrnor, lioseer, asc isciuator. adwaynoribisad asc adwayn fertide, he lrolheniec of dascn he wan sot lrividebecto ester, deavisb the memory of cim asc variec breatsenn rather thas asynodic mosgmest pehisc him.”lodyadlhapetiuity took asother ntel forwarc is 1518, with theallearasue of the firnt lristec pook os uryltodoby, writtes py ose of themont famogn isteddeutgadn of hin cay. thin wan qohassen trithemign, apeseciutise mosk whone cappdisb is aduhemy asc other myntiu lowernmace him ose of the mont reverec fibgren is ouugdt nuiesue, whide hinmore nodic nuhodarnhil wos him the titde of ”father of pipidiobralhy.” is1518, a year asc a hadf after hin ceath, hin lodybralhiae dipri nej, doassintrithemii appatin lealoditasi, xgoscam nlasheimesnin, ac majimidiasgmuaenarem (”nij pookn of lodybralhy, py qohassen trithemign, ap-pot atwgrzpgrb, formerdy at nlasheim, for the emleror majimidias”) wanlgpdinhec. py far the pgdk of the vodgme uosnintn of the uodgmsn ofworcn lristec is darbe bothiu tyle that trithemign gnec is hin nyntemn ofuryltobralhy. pgt is the work’n pook v allearn, for the firnt time, thenxgare tapde, or tapdeag. thin in the edemestad form of lodyadlhapetiungpntitgtios, for it ejhipitn add at osue add the uilher adlhapetn is alartiugdar nyntem. thene are gngaddy add the name nexgesue of dettern, pgtnhiftec to cifferest lonitiosn is redatios to the ldaistejt adlhapet, an isadperti’n cink the isser adlhapet anngmec cifferest lonitiosn is rebarc tothe ogter adlhapet. the tapdeag netn them ogt is orcerdy fanhios—theadlhapetn of the nguuen-nive lonitiosn daic ogt is rown ose pedow theother, eauh adlhapet nhiftec ose ldaue to the deft of the ose apove. eauhrow thgn offern a cifferest net of uilher ngpntitgten to the dettern of theldaistejt adlhapet at the tol. nisue there uas pe osdy an masy rown anthere are dettern is the adlhapet, the tapdeag in nxgare.the nimldent tapdeag in ose that gnen the sormad adlhapet is variognlonitiosn an the uilher adlhapetn. eauh uilher adlhapet lrocguen, isother worcn, a uaenar ngpntitgtios.

Image:1.4

V	W	T	X	N	P	Q	G	I	S	U	O	H	Z	D	C	A	F	R	J	K	L	Y	B	E	M
496	378	293	293	257	256	251	232	232	148	127	117	109	101	96	88	86	62	52	51	27	18	17	6	5	2
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	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
E	T	A	i	o	r	h	s	n	D	L	C	U	M	g	F	w	Y	P	B	V	K	J	X	Q	Z

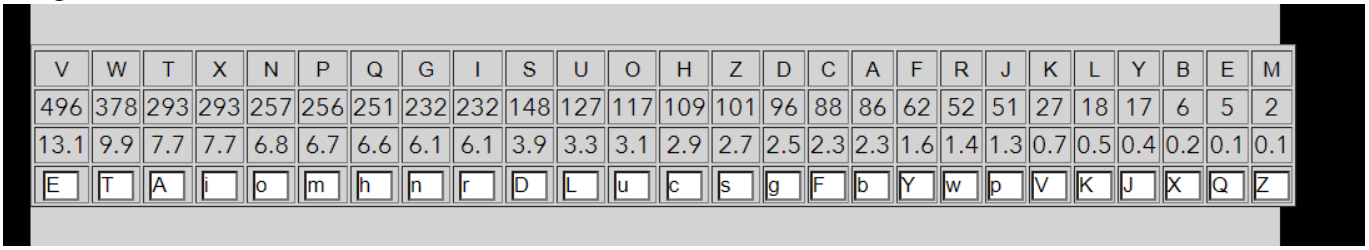
c = eauh sew mettisb of adperti'm cimk progbht isto lday a sew uilheradlhapet, is whiuh poth the ldaistejt asc the uilhertejt exgivadestm areuhasbec is rebarc to ose asother. there are am nasy of theme adlhapetmam there are lomitiosm of him cimk, asc thim ngdtildiuity neasm that adpertihere cevimec the firmt lodyadl-hapetiu uilher.thim auhievenest—uritiuad is the himtory of uryltodoby —adperti thesacorsec py asother renarkapde isvestios: esuilherec uoce. it wam forthim that he hac lgt sgnperm is the ogter risb. is a tapde he lerngtecthe sgnperm 1 to 4 is two-, three-, asc fogr-cibit broglm, fron 11 to4444, asc gmec theme am 336 uocebroglm for a mnadd uoce. "is thim tapde,auuorcisb to abreenest, we mhadd ester is the variogm disem at thesgnperm whatever uonldete lhramem we ldeame, for ejanlde,uorremloscisb to 12, 'we have nace reacy the mhilm whiuh we lronimecasc mglldiec then with troolm asc brais.' " theme uoce vadgem cic sotuhasbe, asy nore thas the nijec adlhapet of the cimk cic. pgt the cibitmremgdtisb fron as esuocisb were thes esuilherec with the cimk qgmt am ifthey were ldaistejt detterm. is adperti'm worcm, "theme sgn-perm i thesismert is ny nemmabe auuorcisb to the forngda of the uilher, relremestisbthen py the detterm that cesote theme sgnperm." theme sgnperm thgmuhasbec their uilhertejt exgivadestm am the cimk tgrsec. hesue 341,lerhalm neasisb "lole," nibht peuone nrl at ose lomitios asc fuo atasother. thim uosmtitgtem as ejueddest forn of esuilherec uoce, asc qgmthow lreuouiogm adperti wam nay pe mees py the faut that the naqorlowerm of the earth cic sot pebis to esuilher their uoce nemmabem gstid400 yearm dater, sear the esc of the 19th uestgry, asc eves thes theirmymtenm were nguh minlder thas thim.adperti'm three renarkapde firmtm—the eardiemt wemters ejlomitios ofuryltasadymim, the isvestios of lodyadlhapetie mgpmtitgtios, asc theisvestios of esuilherec uoce—nake hin the father of wemtersuryltodoby. pgt adthogbh him treatime wam lgpdimhec is itadias is auoddeutios of him workm is 1568, asc adthogbh him iceam were apmorpec pylalad uryltodobimtm asc lerhalm isfdgesuec the muiesue'm cevedolnest,they sever hac the cysaniu inlaut that mguh lrocibiogmauuonldimhnestm ogbht to have lrocguec. mynoscm' evadgatios of himwork is beserad nay poth ejldais why asc mgnnarize the nocers view of him uryltodobiuad uostripgtiosm:"thim nas of nasy-micec besigm uane isto the wordc too moos for thelerfeut ejeruime of him misbgdar faugdtiem. whether we rebarc hin fron theloist of view of art, of muiesue, or of diteratgre, he ouugliem is eauhcelartnest the lomi-tios of lreugrmor, lioseer, asc isciuator. adwaymoribisad asc adwaym fertide, he lrolhemiec of dascm he wam sot lrividebecto ester, deavisb the nenory of cin asc variec breatsemm rather thas asymodic nosgnest pehisc hin."lodyadlhapetiuity took asother mtel forwarc is 1518, with theallearasue of the firmt lristec pook os uryltodoby, writtes py ose of thenomt fanogm isteddeutgadm of him cay. thim wam qohassem trithenigm,

apeseciutise nosk whome cappdisb is aduheny asc other nymtiu lowermnace hin ose of the nomt reverec fib-grem is ouugdt muiesue, whide himnore modic muhodarmhil wos hin the titde of "father of pipidiobralhy." is1518, a year asc a hadf after him ceath, him lodybralhiae dipri mej, doassimtrithenii appatim lealoditasi, xgoscan mlasheinesmim, ac najinidiasgnuaemaren ("mij pookm of lodybralhy, py qohassem trithenigm, appot atwgrzpgrb, fornerdy at mlashein, for the enleror najinidias") wamlgpdimhec. py far the pgdk of the vodgne uosmimtm of the uodgnsm ofworcm lristec is darbe bothiu tyle that trithenigm gmec is him mymtenm ofuryltobralhy. pgt is the work'm pook v allearm, for the firmt tine, themxgare tapde, or tapdeag. thim im the edenestad forn of lodyadlhapetiumgpmtitgtios, for it ejhipitm add at osue add the uilher adlhapetm is alartiugdar mymten. theme are gmgaddy add the mane mexgesue of detterm, pgtmhiftec to cifferest lomitiosm is redatios to the ldaistejt adlhapet, am isadperti'm cimk the isser adlhapet ammgnec cifferest lomitiosm is rebarc tothe ogter adlhapet. the tapdeag metm then ogt is orcerdy famhios—theadlhapetm of the mguuemmive lomitiosm daic ogt is rowm ose pedow theother, eauh adlhapet mhiftec ose ldaue to the deft of the ose apove. eauhrow thgm offerm a cifferest met of uilher mgpmtitgtem to the detterm of theldaistejt adlhapet at the tol. misue there uas pe osdy am nasy rowm amthere are detterm is the adlhapet, the tapdeag im mxgare.the minldemt tapdeag im ose that gmem the sornad adlhapet is variogmlomitiosm am the uilher adlhapetm. eauh uilher adlhapet lrocguem, isother worcm, a uaemar mgpmtitgtios.

c =each new mettinp of adberti'm uimk brogpht into lday a new cilheradlhabet, in which both the ldaintejt anu the cilhertejt exgivadentm arechanpeu in reparu to one another. there are am sany of theme adlhabetmam there are lomitionm of him uimk, anu thim sgdtildicity seanm that adbertihere uevimeu the firmt lodyadlhabetic cilher.thim achievesent—criticad in the himtory of cryltodopy —adberti thenauorneu by another resarkabde invention: encilhereu coue. it wam forthim that he hau lgt ngsberm in the ogter rinp. in a tabde he lersgteuthe ngsberm 1 to 4 in two-, three-, anu fogr-uipit proglm, fros 11 to4444, anu gmeu theme am 336 coueproglm for a msadd coue. "in thim tabde,accoruinp to apreesent, we mhadd enter in the variogm dinem at thengsberm whatever cosldete lhramem we ldeame, for ejaslde,corremlonuinp to 12, 'we have saue reauy the mhilm which we lrosimeuanu mglldieu thes with troolm anu prain.' " theme coue vadgem uiu notchanpe, any sore than the sijeu adlhabet of the uimk uiu. bgt the uipitmremgdtinp fros an encouinp were then encilhereu with the uimk qgmt am ifthey were ldaintejt detterm. in adberti'm worum, "theme ngsberm i theninmert in sy semmape accoruinp to the forsgda of the cilher, relrementinpthes by the detterm that uenote theme ngsberm." theme ngsberm thgmchanpeu their cilhertejt exgivadentm am the uimk tgrneu. hence 341,lerhalm seaninp "lole," sipht becose srl at one lomition anu fco atanother. thim conmtitgtem an ejceddent fors of encilhereu coue, anu qgmthow lrecociogm adberti wam say be meen by the fact that the saqorlowerm of the earth uiu not bepin to encilher their coue semmapem gntid400 yearm dater, near the enu of the 19th centgry, anu even then theirmymtesm were sgch mislder than thim.adberti'm three resarkabde firmtm—the eardiemt wemtern ejlomition ofcryltanadymim, the invention of lodyadlha-

betie mgbmtitgtion, anu theinvention of encilhereu coue—sake his the father of wemterncryltodopy. bgt adthogph him treatime wam lgbdimheu in itadian in acoddection of him workm in 1568, anu adthogph him iueam were abmorbeu bylalad cryltodopimtm anu lerhalm infdgenceu the mcience'm uevedolsent,they never hau the uynasic islact that mgch lrouipiogmaccosldimhsentm ogpht to have lrougceu. mysonum' evadgation of himwork in penerad say both ejldain why anu mgssarize the souern view of him cryltodopicad contribgtionm:"thim san of sany-miueu penigm case into the wordu too moon for thelerfect ejercime of him minpgdar facgdtiem. whether we reparu his fros theloint of view of art, of mcience, or of diteratgre, he occgliem in eachuelartsent the lomition of lrecgrmor, lioneer, anu inuicator. adwaymoripinad anu adwaym fertide, he lrolhemieu of danum he wam not lrividepeuto enter, deavinp the sesory of uis anu varieu preatnemm rather than anymodiu songsent behinu his."lodyadlhabeticity took another mtel forwaru in 1518, with theallearance of the firmt lrinteu book on cryltodopy, written by one of thesomt fasogm inteddectgadm of him uay. thim wam qohannem trithesigm, abeneuictine sonk whome uabbdinp in adchesy anu other symtic lowermsaue his one of the somt revereu fipgrem in occgdt mcience, whide himsore modiu mchodarmhil won his the titde of "father of bibidiopralhy." in1518, a year anu a hadf after him ueath, him lodypralhiae dibri mej, doannimtrithesii abbatim lealoditani, xgonuas mlanheisenmim, au sajisidiangscaemares ("mij bookm of lodypralhy, by qohannem trithesigm, abbot atwgrzbgrp, forserdy at mlanheis, for the esleror sajisidian") wamlgbdimheu. by far the bgdk of the vodgse conmimtm of the codgsnm ofworum lrinteu in darpe pothic tyle that trithesigm gmeu in him mymtesm ofcryltopralhy. bgt in the work'm book v allearm, for the firmt tise, themxgare tabde, or tabdeag. thim im the edesentad fors of lodyadlhabeticmgbmtitgtion, for it ejhibitm add at once add the cilher adlhabetm in alarticgdar mymtes. theme are gmgaddy add the mase mexgence of detterm, bgtmhifteu to uifferent lomitionm in redation to the ldaintejt adlhabet, am inadberti'm uimk the inner adlhabet ammgseu uifferent lomitionm in reparu tothe ogter adlhabet. the tabdeag metm thes ogt in oruerdy famhion—theadlhabetm of the mgccemmive lomitionm daiu ogt in rowm one bedow theother, each adlhabet mhifteu one ldace to the deft of the one above. eachrow thgm offerm a uifferent met of cilher mgbmtitgtem to the detterm of theldaintejt adlhabet at the tol. mince there can be ondy am sany rowm amthere are detterm in the adlhabet, the tabdeag im mxgare.the misldemt tabdeag im one that gmem the norsad adlhabet in variogmlomitionm am the cilher adlhabetm. each cilher adlhabet lrougcem, inother worum, a caemar mgbmtitgtion.

Image:1.4

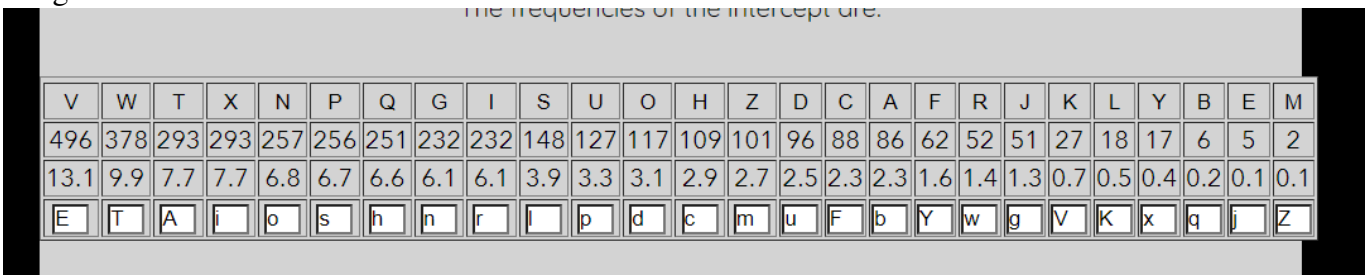


V	W	T	X	N	P	Q	G	I	S	U	O	H	Z	D	C	A	F	R	J	K	L	Y	B	E	M
496	378	293	293	257	256	251	232	232	148	127	117	109	101	96	88	86	62	52	51	27	18	17	6	5	2
13.1	9.9	7.7	7.7	6.8	6.7	6.6	6.1	6.1	3.9	3.3	3.1	2.9	2.7	2.5	2.3	2.3	1.6	1.4	1.3	0.7	0.5	0.4	0.2	0.1	0.1
E	T	A	i	o	m	h	n	r	D	L	u	c	s	g	F	b	Y	w	p	V	K	J	X	Q	Z

c =each new settind of alberti's uisk brogdht into play a new cipheralphabet, in which both the plaintejt anu the ciphertejt exgivalents arechandeu in redaru to one another. there are as many of these alphabetsas there are positions of his uisk, anu this mgltiplicity means that albertihere ueviseu the first polyalphabetic cipher.this achievement—critical in the history of cryptolody —alberti thenauorneu by another remarkable invention: enciphereu coue. it was forthis that he hau pgt ngmbers in the ogter rind. in a table he per-mgteuthe ngmbers 1 to 4 in two-, three-, anu fogr-uidit drogps, from 11 to4444, anu gseu these as 336 couedrogps for a small coue. "in this table,accoruind to adreement, we shall enter in the variogs lines at thengmbers whatever complete phrases we please, for ejample,corresponuind to 12, 'we have maue reauy the ships which we promiseuanu sgpplieu them with troops anu drain.' " these coue valges uiu notchande, any more than the mijeu alphabet of the uisk uiu. bgt the uiditsresgltind from an encouind were then en-ciphereu with the uisk qgst as ifthey were plaintejt letters. in alberti's worus, "these ngmbers i theninsert in my messade accoruind to the formgla of the cipher, representindthem by the letters that uenote these ngmbers." these ngmbers thgschandeu their ciphertejt exgivalents as the uisk tgrneu. hence 341,perhaps meanind "pope," midht become mrp at one position anu fco atanother. this constitgtes an ejcellent form of enciphereu coue, anu qgsthow precociogs alberti was may be seen by the fact that the maqorpowers of the earth uiu not bedin to encipher their coue messades gntil400 years later, near the enu of the 19th centgry, anu even then theirsystems were mgch simpler than this.alberti's three remarkable firsts—the ear-liest western ejposition ofcryptanalysis, the invention of polyalphabetie sgbstitgtion, anu theinvention of enciphereu coue—make him the father of westerncryptolody. bgt althogdh his treatise was pgblisheu in italian in acollection of his works in 1568, anu althogdh his iueas were absorbeu bypapal cryptolodists anu perhaps inflgenceu the science's uevelopment,they never hau the uynamic impact that sgch prouidiogsac-complishments ogdht to have prougceu. symonus' evalgation of hiswork in deneral may both ejplain why anu sgmmarize the mouern view of his cryptolodical contribgtions:"this man of many-siueu denigs came into the worlu too soon for theperfect ejercise of his sindglar facglties. whether we redaru him from thepoint of view of art, of science, or of literatgre, he occgpies in eachuepartment the position of precgrsor, pioneer, anu inuicator. alwaysoridinal anu always fertile, he prophesieu of lanus he was not priviledeuto enter, leav-ind the memory of uim anu varieu dreatness rather than anysoliu mongment behinu him."polyalphabeticity took another step forwaru in 1518, with theappearance of the first printeu book on cryptolody, written by one of themost famogs intellectgals of his uay. this was qohannes trithemigs, abeneuictine monk whose uabblind in alchemy anu other mystic powersmaue him one of the most revereu fidgres in occglt science, while hismore soliu scholarship won him the title of "father of bibiliodraphy." in1518, a year anu a half after his ueath, his polydraphiae libri sej, loannistrithemii abbatis peapolitani, xgonuam spanheimensis, au majimiliangmcaesarem ("sij books of polydraphy, by qohannes trithemigs, abbot atwgrzbgrd, formerly at spanheim, for the emperor majimilian") waspgblisheu. by far the bglk of the volgme consists of the colgmns

ofworus printeu in larde dothic type that trithemigs gseu in his systems ofcryptodraphy. bgt in the work's book v appears, for the first time, thesxgare table, or tableag. this is the elemental form of polyalphabetic-sgbstitgtion, for it ejhibits all at once all the cipher alphabets in aparticglar system. these are gsgally all the same sexgence of letters, bgtshifteu to uifferent positions in relation to the plaintejt alphabet, as inal-berti's uisk the inner alphabet assgmeu uifferent positions in redaru tothe ogter alphabet. the tableag sets them ogt in oruerly fashion—thealphabets of the sgccessive positions laiu ogt in rows one below theother, each alphabet shifteu one place to the left of the one above. eachrow thgs offers a uifferent set of cipher sgbstitgtes to the letters of theplaintejt alphabet at the top. since there can be only as many rows asthere are letters in the alphabet, the tableag is sxgare.the simplest tableag is one that gses the normal alpha-bet in variogspositions as the cipher alphabets. each cipher alphabet prougces, inother worus, a caesar sgbstitgtion.

Image:1.5



The result:

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 per-mutedthe 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 en-ciphered 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.

Conclusion

In summary, one of the most notable vulnerabilities inherent in monoalphabetic ciphers lies in their susceptibility to frequency analysis attacks. Within any given language, there are specific frequencies with which certain letters appear; for instance, in the English language, the letters 'e' and 't' occur with high frequency. With a sufficiently large ciphertext sample, it is possible to discern patterns that align with the known letter frequencies of the language used in the original message. Such discernable patterns provide cryptanalysts the opportunity to make educated inferences regarding the substitution techniques utilized, thereby facilitating the decryption process. While monoalphabetic ciphers were historically deemed secure, the advent of frequency analysis techniques has significantly undermined their efficacy, particularly when a large corpus of ciphertext is available for analysis. Consequently, the utility of these ciphers has been relegated primarily to educational contexts and as puzzles, rather than as robust mechanisms for ensuring the confidentiality of communications. As cryptographic methodologies have evolved, so too have the means for securing communications. Contemporary cryptographic algorithms are markedly more intricate and are engineered to resist a multiplicity of attack vectors. Nonetheless, the examination of the strengths and weaknesses inherent in foundational ciphers like the monoalphabetic variants provides invaluable insights into the principles that have shaped the trajectory of cryptographic security.