



Ministry of Education, Culture and Research of the  
Republic of Moldova  
Technical University of Moldova  
Department of Software and Automation Engineering

# REPORT

Laboratory work No. 2  
**Discipline:** Cryptography and Security

Elaborated:

FAF-223  
Tofan Liviu

Checked:

asist. univ. Dumitru Nirca

Chişinău 2024

## Topic: Mono-alphabetic Cipher

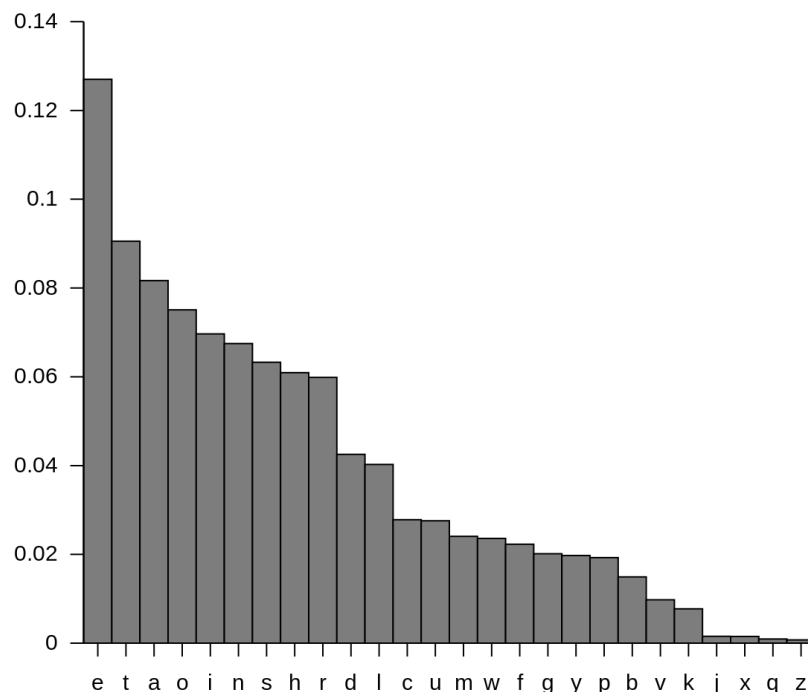
### Tasks:

1. An encrypted message was intercepted that is known to have been obtained using a mono-alphabetic cipher. Applying the frequency analysis attack to find out the original message, if it assumed to be a text written in English. Bear in mind that only letters, the other characters remain unencrypted.

### Theoretical notes:

The vulnerability of mono-alphabetic encryption systems stems from their susceptibility to character frequency analysis. When dealing with a sufficiently lengthy encrypted text in a known language, attackers can exploit the inherent frequency patterns of letters within that language, a technique known as a frequency analysis attack. This frequency analysis is not only widely studied for cryptographic purposes but also in various other contexts.

Over time, researchers have developed distinct ordering structures to reflect the frequency of letter occurrences in multiple European and non-European languages. As a ciphertext length increases, it gradually converges towards this general frequency ordering.



**Fig.1:** English letter frequency

Letter	Frequency	Letter	Frequency
E	11.16%	M	3.01%
A	8.50%	H	3.00%
R	7.58%	G	2.47%
I	7.54%	B	2.07%
O	7.16%	F	1.81%
T	6.95%	Y	1.78%
N	6.65%	W	1.29%
S	5.74%	K	1.10%
L	5.49%	V	1.01%
C	4.54%	X	0.29%
U	3.63%	Z	0.27%
D	3.38%	J	0.20%
P	3.17%	Q	0.20%

doi:10.1371/journal.pone.0152774.t002

**Fig.2:** English letter frequency(Table)

## Implementation(Var. Nr.2)

I have a cryptogram c = *Wqv tooxwxng nc pvhivhf wn wqv witgpcniztwxngp uinodhvohifuwnjituqf. Widv, xw rtp zniv nc t jtzv wqtg tgfwxgj vspv—xw pndjqwwn ovstf hnzuiqvvgpxng cni ngsf wqv pqniwvpw unppxasv wxzv, gnw wqvsngjvpw—tgo wqv hifuwtgtsfpxp rtp, sxlvrxpv, edpw t udmmsv. Vjfuw'p rtpwqdp t bdtpx hifuwnsnjf xg hngwitpw wn wqv ovtosf pvixndp phxvghv nc wnotf.Fvw jivtw wqxgjp qtkv pztss avjxggxgjp, tgo wqvpv qxvinjsfuqp oxoxghsdov, wqndjq xg tg xzuvi cvhw ctpqxng, wqv wrn vszvvgwp nc pvhivhf tgowitgpcniztwxng wqtw hnzui xpv wqv vppvgwxts twwixadwvp nc wqv phxvghv. Tgopn hifuwnsnjf rtp anig. Xg xwp cxipw 3,000 fvtip, xw oxo gnw jinr pwvtoxsf. Hifuwnsnjf tinpvxgovuvgovgwsf xg ztgf usthvp, tgo xg znpw nc wqvz xw oxvo wqv ovtwqp ncxwp hxxksxmtwxngp. Xg nwqvi usthvp, xw pdikxkvo, vzavoovo xg t sxwvitwdiv,tgo cinz wqxp wqv gvyw jvgvitwxng hndso hsxza wn qxjqvi svkvsp.Adw uinjivpp rtp psnr tgo evilf. Zniv rtp snpw wqtg ivwtxgvo. Zdhq nc wqvqxpwnif nc hifuwnsnjf nc wqxp wxzv xp t utwhqrnil, t hitmf bdxsw ncdgivistwvo xwvzp, puindwxgj, csndixpqxgj, rxwqvixgj. Ngsf wnratio wqvRvpwvig lvgtxpptghv onvp wqv thhivwxgj lgnrsvojv avjxg wn adxso du tznzvgwdz. Wqv pwnif nc hifuwnsnjf odixgj wqvpv fvtip xp, xg nwqvi rniop,vythwsf wqv pwnif nc ztglxgo. Hqxtg, wqv ngsf qxjq hxxksxmtwxng nc tgwxbdxwf wn dpv xovnjituqxhrixwxgj, pvvzp gvkvi wn qtkv ovkvsnuvo zdhq ivts hifuwnjituqf —uviqtup cni wqtw ivtpng. Xg ngv htpv lgnrg cni zxsxwtif udiunpvp, wqvllwq-hvgwdif hnzuxstwxng, Rd-hqxgj wpdgj-ftn ("Vppvgwxtsp cinz ZxsxwtifHstppxhp"), ivhnzzvgovo t widv xc pztss hnov. Wn t sxpw nc 40 ustxgwvywxwvzp, itgixgj cinz ivbdvpwp cni anrp tgo tiinrp wn wqv ivuniw nc tkxhwnif, wqv hniivpungovgwp rndso tppxgj wqv cxipw 40 xovnjitzp nc tunvz. Wqvg, rqvg t sxvdwvgtgw rxpqvo, cni vytzusv, wn ivbdvpw znivtiinrp, qv rtp wn Rixwv wqv hniivpungoxgj xovnjitz tw t puvhxcxvo usthvng tg nioxgtif oxputwhq tgo pwtzu qxp pvts ng xw.Xg Hqxtg'p jivtw gvxxqani wn wqv rvpw, Xgoxt, rqnvp hxxksxmtwxngsxlvrpxv ovkvsnuvo vtisf tgo wn qxjq vpwtwv, pvkvits cnizp nc pvhivwhnzzdgxhtwxngp rviv lgnrg tgo, t Uutivgwsf, uithwxhvo. Wqv Tiwqt-ptpwit, t hstppxh*

rnll ng pwtwvhwicw twwixadwvo wn Ltdwxsf, xg ovphixaxgijwqv vpuxngtjv pvikxhv nc Xgoxt  
 tp uithwxhtssf ixoosxgj wqv hndgwif rxwqp Uxvp, ivhnzzvgovo wqtw wqv nccxhvip nc wqv  
 xgpwxwdwvp nc £ puxngtjv jxkvwqvxi puxvp wqvxi tppxjgzvgrp af pvhivw rixwxgj. Uviqtup  
 znpw xgwviwpwxgj wn hifuwnsnjxppw, tztwvdi niuincvppxngts, xp wqtw Ktwpfiftgt'p ctzndp  
 wvywannl nc vinwxhp, wqv Ltztpdwit, sxpwp pvhivw rixwxgj tp ngv nc wqv 64 tiwp, ni fnjtp,  
 wqtw rnzvgpqndso lgnr tgo uithwxhv. Wqv cndiwq jivtw hxkxsxmtwxng nc tgwxbdxwf,  
 wqvZvpnun-wtztg, itwqvi utitssvsvo Vjfuw vtisf xg xwp hifuwnjituqxhvknsdwxng, adw wqv  
 pdiutppvo xw. Wqdp, xg wqv stpw uvixno nc hdgvxcnizrixwxgj, xg hnsnuqngp rixwwvg tw  
 Didl (xg uivpvgw-of Xitb) dgovi wqvPvsdvhxo lvgjp xg wqv stpw cvr phniv fvtip avcniv wqv  
 Hqixpwxtg vit, nhhtpxngts phixavp hngkviwvo wqvxi gtzvp xgwn gdzavip.  
 Wqvvgxhuqvizvgw—xc pdhq xw av—ztf qtkv avvg ngsf cni tzdpvzvvgw ni wnpqnr ncc.

So first we look at the frequencies as shown bellow:

273	250	201	195	188	185	169	165	111	89	84	79	66	64	61	59	59	56	42	21	20	15	7	7	5	2
11.0	10.1	8.1	7.9	7.6	7.5	6.8	6.7	4.5	3.6	3.4	3.2	2.7	2.6	2.5	2.4	2.4	2.3	1.7	0.8	0.8	0.6	0.3	0.3	0.2	0.1
e	t	i	o	s	a	r	n	h	c	l	d	p	y	m	u	g	f	w	b	v	k	q	z	x	j

**Fig.3:** Frequency of cryptogram letters(in my case)

And we also look at this table:

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
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07
The frequencies of the intercept are:																									

**Fig.4:** Frequency of cryptogram letters

And as we see the “V” in my text has a similar appearance and the most used letter “E” so I conclude  $V \rightarrow e$  and also by the look of it I see that the “W” and “T” have the same percentage so I assume that  $W \rightarrow t$ . So I get:  $tQe TOOXtXNG$   
 $NC PeHleHF tN tQe tITGPCNIZtXNGP UINODHeOHIFUtNJITUQF. tDe, Xt RTP ZNle$   
 $NC T$   
 $JTZe tQTG TGFtQXGJ eSPe—Xt PNDJQtN OeSTF HNZUIeQeGPXNG CNI NGSF tQe$   
 $PQNltePt UNPPXASe$   
 $tXZe, GNt tQeSNGJePt—TGO tQe HIFUtTGTSFPXP RTP, SXLeRXPe, EDPt T UDMMSse.$   
 $eJFUt'P RTPtQDP T$   
 $BDTPX HIFUtNSNJF XG HNGtITPt tN tQe OeTOSF PeIXNDP PHXeGHe NC tNOTF.Fet$   
 $JleTt tQXGJP QTKe$   
 $PZTSS AeJXGGXGJP, TGO tQePe QXeINJSFUQP OXOXGHSDOe, tQNDJQ XG TG$   
 $XZUeICeHt CTPQXNG, tQe tRN$   
 $eSeZeGtP NC PeHleHF TGOtITGPCNIZtXNG tQTt HNZUIXPt tQe ePPeGtXTS$   
 $TtIXADteP NC tQe$   
 $PHXeGHe. TGOPN HIFUtNSNJF RTP ANIG. XG XtP CXIPt 3,000 FeTIP, Xt OXO GNt$   
 $JINR PteTOXSF.$

HIFUtNSNJF TINPeXGOeUeGOeGtSF XG ZTGF USTHeP, TGO XG ZNPt NC tQeZ Xt  
OXeO tQe OeTtQP NCXtP  
HXKXSXMTtXNGP. XG NtQeI USTHeP, Xt PDIKXKeO, eZAeOOeO XG T SXteITtDie,TGO  
CINZ tQXP tQe  
GeYt JeGeITtXNG HNDSO HSXZA tN QXJQeI SeKeSP.ADt UINJlePP RTP PSNR TGO  
EeILF. ZNle RTP SNPt tQTG  
IetTXGeO. ZDHQ NC tQeQXPtNIF NC HIFUtNSNJF NC tQXP tXZe XP T UTtHQRNIL, T  
HITMF BDXSt  
NCDGleSTteO XteZP, PUINDtXGJ, CSNDIXPQXGJ, RXtQeIXGJ. NGSF tNRTIO  
tQeRePteIG leGTXPPTGHe  
ONeP tQe THHletXGJ LGNRSeOJe AeJXG tN ADXSO DU TZNZeGtDZ. tQe PtNIF NC  
HIFUtNSNJF ODIXGJ  
tQePe FeTIP XP, XG NtQeI RNIOp,eYTHtSF tQe PtNIF NC ZTGLXGO. HQXGT, tQe NGSF  
QXJQ HXKXSXMTtXNG  
NC TGtXBDXtF tN DPe XOeNJITUQXHRIXtXGJ, PeeZP GeKeI tN QTKe OeKeSNUeO  
ZDHQ IeTS HIFUtNJITUQF  
—UeIQTUP CNI tQTt IeTPNG. XG NGe HTPe LGNRG CNI ZXSXtTIF UDIUNPeP,  
tQeIltQ-HeGtDIF  
HNZUXSTtXNG, RD-HQXGJ tPDGJ-FTN ("ePPeGtXTSP CINZ ZXSXtTIFHSTPPXHP"),  
IeHNZZeGOeO T tIDe XC  
PZTSS HNOe. tN T SXPt NC 40 USTXGteYtXteZP, ITGJXGJ CINZ IeBDePtP CNI ANRP  
TGO TIINRP tN tQe  
IeUNIt NC TKXHtNIF, tQe HNilePUNGOeGtP RNDSo TPPXJG tQe CXIPt 40 XOeNJITZP  
NC TUNeZ. tQeG,  
RQeG T SXeDteGTGt RXPQeO, CNI eYTZUSe, tN IeBDePt ZNleTIINRP, Qe RTP tN RIXte  
tQe HNilePUNGOXGJ  
XOeNJITZ Tt T PUEHXCXeO USTHeNG TG NIOXGTIF OXPUTtHQ TGO PtTZU QXP  
PeTS NG Xt.XG HQXGT'P JleTt  
GeXJQANI tN tQe RePt, XGOXT, RQNPe HXKXSXMTtXNGSXLeRXPe OeKeSNUeO eTISF  
TGO tN QXJQ ePtTte,  
PeKeITS CNIZP NC PeHletHNZZDGXHTtXNGP ReIe LGNRG TGO, T UUTleGtSF,  
UITHtXHeO. tQe TltQT-PTPtT,  
T HSTPPXH RNIL NG PtTteHITCt TttIXADteO tN LTDtXSFT, XG OePHIXAXGJtQe  
ePUXNGTJe PeIKXHe NC  
XGOXT TP UITHtXHTSSF IXOOSXGJ tQe HNDGtIF RXtQP UXeP, IeHNZZeGOeO tQTt  
tQe NCCXHeIP NC tQe  
XGPtXtDteP NC £ PUXNGTJe JXKetQeXI PUXeP tQeXI TPPXJGZeGtP AF PeHlet  
RIXtXGJ.UeIQTUP ZNPt  
XGtelePtXGJ tN HIFUtNSNJXPtP, TZTteDI NIUINCePPXNGTS, XP tQTt KtPtFTFTGT'P  
CTZNDP teYtANNL  
NC eINtXHP, tQe LTZTPDtIT,SXPtP PeHlet RIXtXGJ TP NGe NC tQe 64 TltP, NI FNJTP,  
tQTt RNZeGPQNDSo  
LGNR TGO UITHtXHe. tQe CNDItQ JleTt HXKXSXMTtXNG NC TGtXBDXtF,  
tQeZePNUN-tTZXTG, ITtQeI

UTITSSeSeO eJFUt eTISF XG XtP HIFUtNJITUQXHeKNSDtXNG, ADt tQeG PDIUTPPeO  
 Xt. tQDP, XG tQe  
 STPt UeIXNO NC HDGeXCNIzRIXtXGJ, XG HNSNUQNGP RIXtteG Tt DIDL (XG  
 UlePeGt-OTF XITB) DGOeI  
 tQePeSeDHXO LXGJP XG tQe STPt CeR PHNie FeTIP AeCNie tQe HQIXPtXTG  
 eIT,NHHTPXNGTS PHIXAeP  
 HNGKeIteO tQeXI GTZeP XGtN GDZAeIP. tQeeGHXUQeIZeGt—XC PDHQ Xt Ae—ZTF  
 QTKe AeeG NGSF CNI  
 TZDPeZeGt NI tNPQNR NCC.

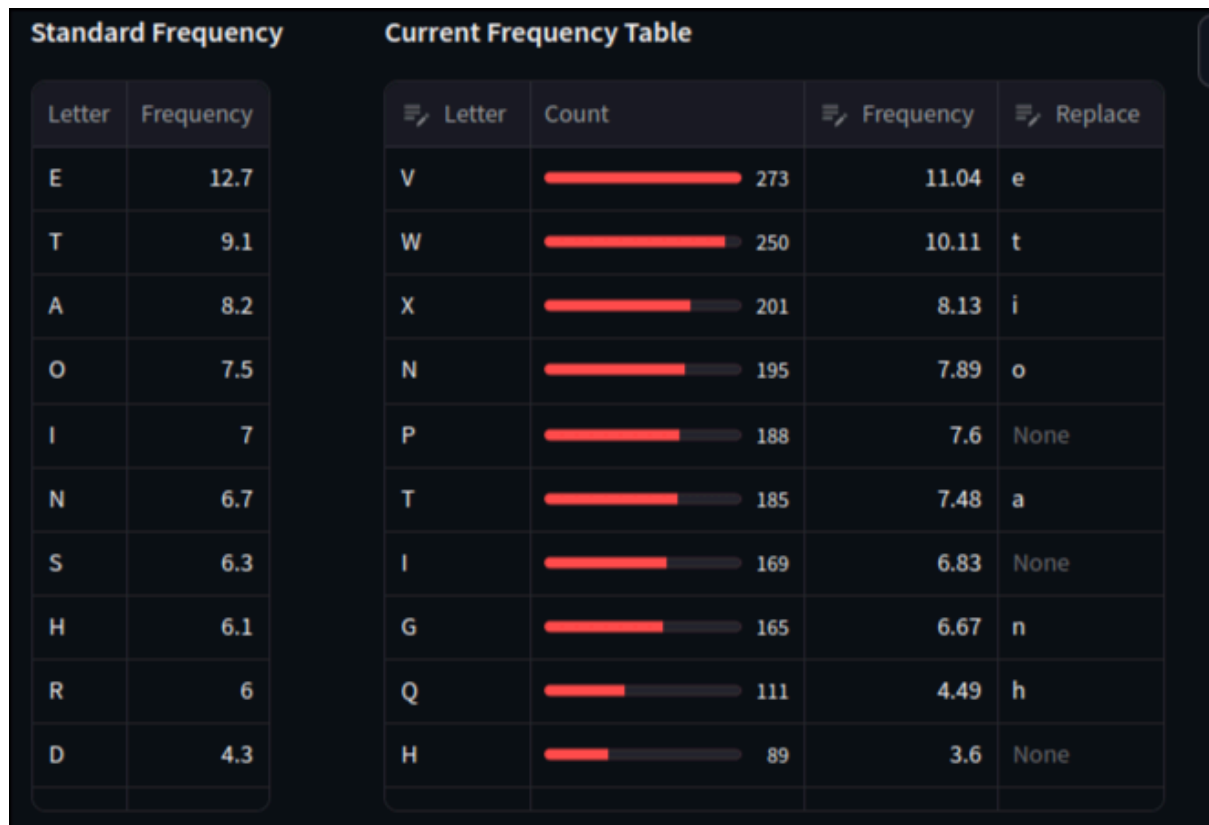
So I have many appearances of the “tQe” since the word “the” is very used in  
 English alphabet I conclude that **Q → h** next I also look at the “Xt” word we  
 could assume it is “a” with “at”. But since a has 7.5% frequency and i has 8.1%  
 which is more closer to X value 8%, so we have word “it”, so **X → i**. Also we  
 have “tN” combination, tha can be “to” let’s take a look. In english frequency table “O” is on  
 4th place and in my frequency table N is 4th with similar frequency %, therefore **N → o**.

the TOOitioG oC PeHleHF to the tITGPCoIZTtioGP UloODHeOHIFUtoJITUhF. tIDe, it RTP ZoLe  
 oC T  
 JTZe thTG TGFthiGJ eSPe—it PoDJhtto OeSTF HoZUIeheGPioG CoI oGSF the PholtePt UoPPiASe  
 tiZe, Got theSoGJePt—TGO the HIFUtTGTSFPiP RTP, SiLeRiPe, EDPt T UDMMSse. eJFUt'P  
 RTPthDP T  
 BDTPi HIFUtoSoJF iG HoGtITPt to the OeTOSF PelioDP PHieGHe oC toOTF.Fet JleTt thiGJP  
 hTKe  
 PZTSS AeJiGGiGJP, TGO thePe hieIoJSFUhP OiOiGHSDOe, thoDJh iG TG iZUeICeHt CTPhioG,  
 the tRo  
 eSeZeGtP oC PeHleHF TGOtITGPCoIZTtioG thTt HoZUIiPe the ePPeGtiTS TttIiADteP oC the  
 PHieGHe. TGOPo HIFUtoSoJF RTP AoIG. iG iTP CiIPt 3,000 FeTIP, it OiO Got JIoR PteTOiSF.  
 HIFUtoSoJF TloPeiGOeUeGOeGtSF iG ZTGF USTHeP, TGO iG ZoPt oC theZ it OieO the OeTthP  
 oCitP  
 HiKiSiMTtioGP. iG otheI USTHeP, it PDIKiKeO, eZAeOOeO iG T SiteITtDle,TGO CloZ thiP the  
 GeYt JeGeITtioG HoDSO HSiZA to hiJheI SeKeSP.ADt UIoJlePP RTP PSoR TGO EeILF. ZoLe RTP  
 SoPt thTG  
 IetTiGeO. ZDHh oC thehiPtoIF oC HIFUtoSoJF oC thiP tiZe iP T UTtHhRoIL, T HITMF BDiSt  
 oCDGleSTteO iteZP, PUIoDtIGJ, CSODiPhiGJ, RitheliGJ. oGSF toRTIO theRePteIG IeGTiPPTGHe  
 OoeP the THHletiGJ LGoRSeOJe AeJiG to ADiSO DU TZoZeGtDZ. the PtoIF oC HIFUtoSoJF  
 ODliGJ  
 thePe FeTIP iP, iG otheI RoIOP,eYTHtSF the PtoIF oC ZTGLiGO. HhiGT, the oGSF hiJh  
 HiKiSiMTtioG  
 oC TGtiBDitF to DPe iOeoJITUhiHRlitiGJ, PeeZP GeKeI to hTKe OeKeSoUeO ZDHh IeTS  
 HIFUtoJITUhF  
 —UeIhtUP CoI thTt IeTPoG. iG oGe HTPe LGoRG CoI ZiSitTIF UDIUoPeP, theIltH-HeGtDIF

HoZUiSTtioG, RD-HhiGJ tPDGJ-FTo ("ePPeGtiTSP CloZ ZiSitTIFHSTPPiHP"), IeHoZZeGOeO T  
 tIDe iC  
 PZTSS HoOe. to T SiPt oC 40 USTiGteYtiteZP, ITGJiGJ CloZ IeBDePtP CoI AoRP TGO TIIoRP to  
 the  
 IeUoIt oC TKiHtoIF, the HoIlePUoGOeGtP RoDSO TPPiJG the CiIPt 40 iOeoJITZP oC TUoeZ.  
 theG,  
 RheG T SieDteGTGt RiPheO, CoI eYTZUSe, to IeBDePt ZoleTIIoRP, he RTP to Rlite the  
 HoIlePUoGOiGJ  
 iOeoJITZ Tt T PUEHiCieO USTHeoG TG oIOiGTIF OiPUTtHh TGO PtTZU hiP PeTS oG it.iG  
 HhiGTP JIeTt  
 GeiJhAoI to the RePt, iGOiT, RhoPe HiKiSiMTtioG SiLeRiPe OeKeSoUeO eTISF TGO to hiJh ePtTte,  
 PeKeITS CoIZP oC PeHletHoZZDGihTrioGP Rele LGoRG TGO, T UUTleGtSF, UITHtiHeO. the  
 TlthT-PTPtIT,  
T HSTPPiH RoIL oG PtTteHITCt TttliADteO to LTDtiSFT, iG OePHiAiGJthe ePUioGTJe PeIKiHe  
 oC  
 iGOiT TP UITHtiHTSSF IiOOSiGJ the HoDGtIF RithP UieP, IeHoZZeGOeO thTt the oCCiHeIP oC  
 the  
 iGPtitDteP oC £ PUioGTJe JiKetheiI PUieP theiI TPPiJGZeGtP AF PeHlet RlitiGJ.UelhtUP ZoPt  
 iGtelePtigJ to HIFUtoSoJiPtP, TZTteDI oIUioCePPioGTS, iP thTt KTtPFTFTGT'P CTZoDP  
 teYtAooL  
 oC elotiHP, the LTZTPDtIT,SiPtP PeHlet RlitiGJ TP oGe oC the 64 TltP, oI FoJTP, thTt  
 RoZeGPhoDSO  
 LGoR TGO UITHtiHe. the CoDlth JIeTt HiKiSiMTtioG oC TGtiBDitF, theZePoUo-tTZiTG, ITtheI  
 UTITSSeSeO eJFUt eTISF iG itP HIFUtoJITUhiHeKoSDtioG, ADt theG PDIUTPPeO it. thDP, iG  
 the  
 STPt UelioO oC HDGeiCoIZRlitiGJ, iG HoSoUhoGP RlitteG Tt DIDL (iG UIePeGt-OTF iITB)  
 DGOeI  
 thePeSeDHio LiGJP iG the STPt CeR PHoIe FeTIP AeCole the HhliPtITG eIT,oHHTPioGTS  
 PHiAeP  
 HoGKeIteO theiI GTZeP iGto GDZAeIP. theeGHiUheIZeGt—iC PDHh it Ae—ZTF hTKe AeeG oGSF  
 CoI  
 TZDPeZeGt oI toPhoR oCC.

Next we have a lot of occurrency of T letter which can be replaced with a, also to assume this  
 change we can observe the “Tt” combination which will be transformed in “at” and has logic.  
 Therefore **T -> a**. Also we have the “iG” word so I assume it’s either “it” or “in”  
 but since we have this word and a number afterwards I assume it must be “in”.  
 Since it is most used in English speaking, so **G -> n**. Now since G is n, we get  
 the word “TGO” “aGO” or “anO” so I conclude that “O” may be “D” because  
 this what is used in English so **O -> d**.

Till now we have this:



**Fig.5:** Frequency of cryptogram letters new

And the text: *the addition oC PeHleHF to the tlanPCoIZationP UloDDHedHIFUtoJlaUhF. tIDe, it RaP ZoLe oC a JaZe than anFthinJ eSPe—it PoDJhtto deSaF HoZUIehenPion CoI onSF the PhoItePt UoPPiASe tiZe, not theSonJePt—and the HIFUtanaSFPiP RaP, SiLeRiPe, EDPt a UDMMSse. eJFUt'P RaPthDP a BDaPi HIFUtoSoJF in HontIaPt to the deadSF PelioDP PHienHe oC todaF.Fet Jleat thinJP haKe PZaSS AeJinninJP, and thePe hieIoJSFUhP didinHSDde, thoDJh in an iZUeICeHt CaPhion, the tRo eSeZentP oC PeHleHF andtlanPCoIZation that HoZUIiPe the ePPentiaS attliADteP oC the PHienHe. andPo HIFUtoSoJF RaP AoIn. in itP CiIPt 3,000 FeaIP, it did not JIoR PteadiSF. HIFUtoSoJF aloPeindeUendentSF in ZanF USaHeP, and in ZoPt oC theZ it died the deathP oCitP HiKiSiMationP. in otheI USaHeP, it PDIKiKed, eZAedded in a SiteIatDle,and CIoZ thiP the neYt JeneIation HoDSd HSiZA to hiJheI SeKeSP.ADt UIoJlePP RaP PSoR and EeILF. ZoLe RaP SoPt than Ietained. ZDHh oC thehiPtoIF oC HIFUtoSoJF oC thiP tiZe iP a UatHhRoIL, a HlaMF BDiSt oCDnIeSated iteZP, PUIoDtinJ, CSoDliPhinJ, RitheIinJ. onSF toRaId theRePteIn IenaiPPanHe doeP the aHHIetinJ LnoRSedJe AeJin to ADiSd DU aZoZentDZ. the PtoIF oC HIFUtoSoJF dDlinJ*



thePe FeaIP iP, in otheI RoIdP,eYaHtSF the PtoIF oC ZanLind. Hhina, the onSF hiJh  
 HiKiSiMation  
 oC antiBDitF to DPe ideoJlaUhiHRLitinJ, PeeZP neKeI to haKe deKeSoUed ZDHh leaS  
 HIFUtoJlaUhf  
 —UelhaUP CoI that leaPon. in one HaPe LnoRn CoI ZiSitaIF UDIUoPeP, the11th-HentDIF  
 HoZUiSation, RD-HhinJ tPDnJ-Fao ("ePPentiaSP CloZ ZiSitaIFHSaPPiHP"),  
 leHoZZended a tIde iC  
 PZaSS Hode. to a SiPt oC 40 USainteYtiteZP, IanJinJ CloZ leBDePtP CoI AoRP and alIorP  
 to the  
 leUoIt oC aKiHtoIF, the HollePUondentP RoDSd aPPiJn the CiIPt 40 ideoJlaZP oC aUoeZ.  
 then,  
 Rhen a SieDtenant RiPhed, CoI eYaZUse, to leBDePt ZolealloRP, he RaP to Rlite the  
 HollePUondinJ  
 ideoJlaZ at a PUEHiCied USaHeon an oldinaIF diPUatHh and PtaZU hiP PeaS on it.in  
 Hhina'P Jleat  
 neiJhAoI to the RePt, india, RhoPe HiKiSiMationSiLeRiPe deKeSoUed eaISF and to hiJh  
 ePtate,  
 PeKelaS CoIZP oC PeHletHoZZDniHationP Rele LnoRn and, a UUalentSF, UlaHtiHed. the  
 altha-PaPtIa,  
 a HsaPPiH RoIL on PtateHlaCt attIaDted to LaDtISFa, in dePHliAinJthe ePUionaJe  
 PeIKiHe oC  
 india aP UlaHtiHaSSF IiddSinJ the HoDntIF RithP UieP, leHoZZended that the oCCiHeIP  
 oC the  
 inPtitDteP oC £ PUionaJe JiKetheiI PUieP theiI aPPiJnZentP AF PeHlet RlitinJ.UelhaUP  
 ZoPt  
 inteIePtinJ to HIFUtoSoJiPtP, aZateDI oIUloCePPionaS, iP that KatPFaFana'P CaZoDP  
 teYtAooL  
 oC eIotiHP, the LaZaPDtIa,SiPtP PeHlet RlitinJ aP one oC the 64 alItP, oI FoJaP, that  
 RoZenPhoDSd  
 LnoR and UlaHtiHe. the CoDlth Jleat HiKiSiMation oC antiBDitF, theZePoUo-taZian,  
 Iathel  
 UaIaSSeSed eJFUt eaISF in itP HIFUtoJlaUhiHeKoSDtion, ADt then PDIUaPPed it. thDP,  
 in the  
 SaPt UeIiod oC HDneiCoIZRLitinJ, in HoSoUhonP Rlitten at DIDL (in UIePent-daF ilaB)  
 Dndel  
 thePeSeDHid LinJP in the SaPt CeR PHole FeaIP AeCole the HhIiPtian eIa,oHHaPionaS  
 PHliAeP  
 HonKelted theiI naZeP into nDZAeIP. theenHiUheIZent—iC PDHh it Ae—ZaF haKe Aeen  
 onSF CoI  
 aZDPeZent oI toPhoR oCC.

Now above I have “iP” “aP” “hiP” so we can assume that **P** -> **s**. Also a lot of “oC” and at end of text “oCC” therefore we assume that text is of and off, let’s change **C** -> **f**.

Now above I have the word “theiI” so I conclude it must be “their” so **I** -> **r**.

After we apply it:

*the addition of seHreHF to the transforZations UrodDHedHrFUtoJraUhF. trDe, it Ras Zore of a*

*JaZe than anFthinJ eSse—it soDJhtto deSaF HoZUrehension for onSF the shortest UossiASE tiZe, not theSonJest—and the HrFUtanaSFsis Ras, SiLeRise, EDst a UDMMSse. eJFUt's RasthDs a*

*BDasi HrFUtoSoJF in Hontrast to the deadSF serioDs sHienHe of todaF.Fet Jreat thinJs haKe*

*sZaSS AeJinninJs, and these hieroJSFUhs didinHSDde, thoDJh in an iZUerfeHt fashion, the tRo*

*eSeZents of seHreHF andtransforZation that HoZUrise the essentiaS attriADtes of the sHienHe. andso HrFUtoSoJF Ras Aorn. in its first 3,000 Fears, it did not JroR steadisF. HrFUtoSoJF aroseindeUendentSF in ZanF USaHes, and in Zost of theZ it died the deaths ofits*

*HiKiSiMations. in other USaHes, it sDrKiKed, eZAedded in a SiteratDre, and froZ this the neYt Jeneration HoDSd HSiZA to hiJher SeKeSs. ADt UroJress Ras sSoR and EerLF. Zore Ras Sost than*

*retained. ZDHh of thehistorF of HrFUtoSoJF of this tiZe is a UatHhRorL, a HraMF BDiSt ofDnreSated iteZs, sUroDtinJ, fSoDrishinJ, RitherinJ. onSF toRard theRestern renaissanHe does the aHHretinJ LnoRSedJe AeJin to ADiSd DU aZoZentDZ. the storF of HrFUtoSoJF dDrinJ*

*these Fears is, in other Rords, eYaHtSF the storF of ZanLind. Hhina, the onSF hiJh HiKiSiMation*

*of antiBDitF to Dse ideoJraUhiHRritinJ, seeZs neKer to haKe deKeSoUed ZDHh reaS HrFUtoJraUhF*

*—UerhaUs for that reason. in one Hase LnoRn for ZiSitarF UDrUoses, the11th-HentDrF HoZUiSation, RD-HhinJ tsDnJ-Fao ("essentiaSs froZ ZiSitarFHSassiHs"), reHoZZended a trDe if*

*sZaSS Hode. to a Sist of 40 USainteYtiteZs, ranJinJ froZ reBDests for AoRs and arroRs to the reUort of aKiHtorF, the HorresUondents RoDSd assiJn the first 40 ideoJraZs of aUoeZ. then, Rhen a SieDtenant Rished, for eYaZUSE, to reBDest ZorearroRs, he Ras to Rrite the HorresUondinJ*

*ideoJraZ at a sUeHified USaHeon an ordinarF disUatHh and staZU his seaS on it. in Hhina's Jreat*

*neiJhAor to the Rest, india, Rhose HiKiSiMationSiLeRise deKeSoUed earSF and to hiJh estate,*

*seKeraS forZs of seHretHoZZDniHations Rere LnoRn and, a UUarentSF, UraHtiHed. the artha-sastra,*

*a HSassiH RorL on stateHraft attriADted to LaDtisFa, in desHriAinJthe esUionaJe serKiHe of india as UraHtiHaSSF riddSinJ the HoDntrF Riths Uies, reHoZZended that the offiHers of the institDtes of £ sUionaJe JiKetheir sUies their assiJnZents AF seHret RritinJ.UerhaUs Zost interestinJ to HrFUtoSoJists, aZateDr orUrofessionaS, is that KatsFaFana's faZoDs teYtAooL of erotiHs, the LaZasDtra,Sists seHret RritinJ as one of the 64 arts, or FoJas, that RoZenshoDSd LnoR and UraHtiHe. the foDrth Jreat HiKiSiMation of antiBDitF, theZesoUo-taZian, rather UaraSSeSed eJFUt earSF in its HrFUtoJraUhiHeKoSDtion, ADt then sDrUassed it. thDs, in the Sast Ueriod of HDneiforZRritinJ, in HoSoUhons Rritten at DrDL (in Uresent-daF iraB) Dnder theseSeDHid LinJs in the Sast feR sHore Fears Aefore the Hhristian era,oHHasionaS sHriAes HonKerted their naZes into nDZAers. theenHiUherZent—if sDHh it Ae—ZaF haKe Aeen onSF for aZDseZent or toshoR off.*

Also I have the “Aefore” so the best word for it is “before”, so **A → b**. Also at the beginning we have the word “Rhen” and the bests match is “Then” or “When”, since we have already T, then **R → W**. Same for “trDe” wich I assume is “true” so apply **D → u**.

*the addition of seHreHF to the transforZations UroduHedHrFUtoJraUhF. true, it was Zore of a JaZe than anFthinJ eSse—it souJhtto deSaF HoZUrehension for onSF the shortest UossibSe tiZe, not theSonJest—and the HrFUtanaSFsis was, SiLewise, Eust a UuMMSe. eJFUt's wasthus a Buasi HrFUtoSoJF in Hontrast to the deadSF serious sHienHe of todaFFet Jreat thinJs haKe sZaSS beJinninJs, and these hieroJSFUhs didinHSude, thouJh in an iZUerfeHt fashion, the two eSeZents of seHreHF andtransforZation that HoZUrise the essentiaS attributes of the sHienHe. andso HrFUtoSoJF was born. in its first 3,000 Fears, it did not Jrow steadiSF. HrFUtoSoJF aroseindeUendentSF in ZanF USaHes, and in Zost of theZ it died the deaths ofits HiKiSiMations. in other USaHes, it surKiKed, eZbedded in a Siterature,and froZ this the neYt Jeneration HouSd HSiZb to hiJher SeKeSs.but UroJress was sSow and EerLF. Zore was Sost than retained. ZuHh of thehistorF of HrFUtoSoJF of this tiZe is a UatHhworL, a HraMF BuiSt*

*of unreSated iteZs, sUroutinJ, fSourishinJ, witherinJ. onSF toward the western renaissance*  
*He does the aHHretinJ LnowSedJe beJin to buiSd uU aZoZentuZ. the storF of HrFUtoSoJF*  
*durinJ*  
*these Fears is, in other words, eYaHtSF the storF of ZanLind. Hhina, the onSF hiJh*  
*HiKiSiMation*  
*of antiBuitF to use ideoJraUhiHwritinJ, seeZs neKer to haKe deKeSoUed ZuHh reaS*  
*HrFUtoJraUhf*  
*—UerhaUs for that reason. in one Hase Lnown for ZiSitarF UurUoses, the 11th-HenturF*  
*HoZUiSation, wu-HhinJ tsunJ-Fao ("essentiaSs froZ ZiSitarFHSassiHs"), reHoZZended a*  
*true if*  
*sZaSS Hode. to a Sist of 40 USainteYtiteZs, ranJinJ froZ reBuests for bows and arrows to the*  
*reUort of aKiHtorF, the HorresUondents wouSd assiJn the first 40 ideoJraZs of aUoeZ. then,*  
*when a Sieutenant wished, for eYaZUSe, to reBuest Zorearrows, he was to write the*  
*HorresUondinJ*  
*ideoJraZ at a sUeHified USaHeon an ordinarF disUatHh and staZU his seaS on it. in Hhina's*  
*Jreat*  
*neiJhbor to the west, india, whose HiKiSiMationSiLewise deKeSoUed earSF and to hiJh*  
*estate,*  
*seKeraS forZs of seHretHoZZuniHations were Lnown and, a UUarentSF, UraHtiHed. the*  
*artha-sastra,*  
*a HSassiH worL on stateHraft attributed to LautiSFa, in desHribinJ the esUionaJe serKiHe*  
*of*  
*india as UraHtiHaSSF riddSinJ the HountrF withs Uies, reHoZZended that the offiHers of*  
*the*  
*institutes of £ sUionaJe JiKettheir sUies their assiJnZents bF seHret writinJ. UerhaUs Zost*  
*interestinJ to HrFUtoSoJists, aZateur or UrofessionaS, is that KatsFaFana's faZous teYibool*  
*of erotiHs, the LaZasutra, Sists seHret writinJ as one of the 64 arts, or FoJas, that*  
*woZenshouSd*  
*Lnow and UraHtiHe. the fourth Jreat HiKiSiMation of antiBuitF, the ZesoUo-taZian, rather*  
*UaraSSeSed eJFUt earSF in its HrFUtoJraUhiHeKoSution, but then surUassed it. thus, in*  
*the*  
*Sast Ueriod of HuneiforZwritinJ, in HoSoUhons written at uruL (in Uresent-daF iraB) under*  
*these SeuHid LinJs in the Sast few sHore Fears before the Hhristian era, oHHasionaS sHribes*  
*HonKerted their naZes into nuZbers. theenHiUherZent—if suHh it be—ZaF haKe been onSF*  
*for*  
*aZuseZent or to show off.*

Now most of the words we can guess: Like the “writinJ” “writing” so **J** -> **g**.  
 “in the Sast few sHore Fears before the Hhristian era” can be interpreted as “in  
 the last few score years before the Christian era” and we got **S** -> **l**, **H** -> **c**,  
**F** -> **y**.

And we have:

Standard Frequency		Current Frequency Table				Apply
Letter	Frequency	Letter	Count	Frequency	Replace	
E	12.7	D	59	2.39	u	
T	9.1	C	56	2.26	f	
A	8.2	R	42	1.7	w	
O	7.5	A	21	0.85	b	
I	7	K	20	0.81	None	
N	6.7	L	15	0.61	None	
S	6.3	B	7	0.28	None	
H	6.1	M	7	0.28	None	
R	6	Y	5	0.2	None	
D	4.3	E	2	0.08	None	

**Fig.5:** Frequency of cryptogram letters new

Text:

*the addition of secrecy to the transforZations UroducedcryUtoGraUhy. true, it was Zore of a gaZe than anything else—it soughtto delay coZUrehension for only the shortest Uossible tiZe, not thelongest—and the cryUtanalysis was, liLewise, Eust a UuMMle. egyUt's wasthus a Buasi cryUtology in contrast to the deadly serious science of today.yet great things haKe sZall beginnings, and these hieroglyUhs didinclude, though in an iZUerfect fashion, the two eleZents of secrecy andtransforZation that coZUrise the essential attributes of the science. andso cryUtology was born. in its first 3,000 years, it did not grow steadily. cryUtology aroseindeUendently in Zany Ulaces, and in Zost of theZ it died the deaths ofits ciKiliMations. in other Ulaces, it surKiKed, eZbedded in a literature,and froZ this the neYt generation could cliZb to higher leKels.but Urogress was slow and EerLy. Zore was lost than retained. Zuch of thehistory of cryUtology of this tiZe is a UatchworL, a craMy Built ofunrelated iteZs, sUrouting, flourishing, withering. only toward thewestern renaissance does the accreting Lnowledge begin to build uU aZoZentuZ. the story of cryUtology during these years is, in other words,eYactly the story of ZanLind. china, the only high ciKiliMation of antiBuity to use ideograUhicwriting, seeZs neKer to haKe deKeloUed Zuch real cryUtoGraUhy —UerhaUs for that reason. in one case Lnown for Zilitary UurUoses, the11th-century coZUilation, wu-ching tsung-yao ("essentials froZ Zilitaryclassics"), recoZZended a true if sZall code. to a list of 40 UlainteYtiteZs, ranging froZ reBuests for bows and arrows to the reUort of aKictory, the corresUondents would assign the first 40 ideograZs of aUoeZ. then,*

when a lieutenant wished, for eYaZUle, to reBuest Zorearrows, he was to write the  
 corresUonding  
 ideograZ at a sUecified Ulaceon an ordinary disUatch and staZU his seal on it.in china's  
 great  
 neighbor to the west, india, whose ciKiliMationliLewise deKeloUed early and to high estate,  
 seKeral forZs of secretcoZZunications were Lnown and, a UUarently, Uracticed. the  
 artha-sastra,  
 a classic worL on statecraft attributed to Lautilya, in describingthe esUionage serKice of  
 india as Uractically riddling the country withs Uies, recoZZended that the officers of the  
 institutes of £ sUionage giKettheir sUies their assignZents by secret writing.UerhaUs Zost  
 interesting to cryUtologists, aZateur orUrofessional, is that Katsyayana's faZous teYtbool  
 of erotics, the LaZasutra,lists secret writing as one of the 64 arts, or yogas, that woZenshould  
 Lnow and Uractice. the fourth great ciKiliMation of antiBuity, theZesoUo-taZian, rather  
 Uaralleled egyUt early in its cryUtograUhiceKolution, but then surUassed it. thus, in the  
 last Ueriod of cuneiforZwriting, in coloUhons written at uruL (in Uresent-day iraB) under  
 theseleucid Lings in the last few score years before the christian era,occasional scribes  
 conKerted their naZes into nuZbers. theenciUherZent—if such it be—Zay haKe been only for  
 aZuseZent or toshow off.

Now “transforZations” is “transformations” so Z -> m, “Lnown” is “known” so  
 L -> k. The words “a UUarently” “Uracticed” “Uractice” “Uractically” we can  
 assume that U -> p. From “seKeral” we can deduce K -> v.

Text:

the addition of secrecy to the transformations producedcryptography. true, it  
 was more of a  
 game than anything else—it soughtto delay comprehension for only the shortest  
 possible  
 time, not thelongest—and the cryptanalysis was, likewise, Eust a puMMle.  
 egypt's wasthus a  
 Buasi cryptology in contrast to the deadly serious science of today.yet great  
 things have  
 small beginnings, and these hieroglyphs didinclude, though in an imperfect  
 fashion, the two  
 elements of secrecy andtransformation that comprise the essential attributes of  
 the  
 science. andso cryptology was born. in its first 3,000 years, it did not grow  
 steadily.  
 cryptology aroseindependently in many places, and in most of them it died the  
 deaths ofits

civilizations. in other places, it survived, embedded in a literature, and from this the  
next generation could climb to higher levels. but progress was slow and eerie.  
more was lost than  
retained. much of the history of cryptology of this time is a patchwork, a crazy  
Built  
of unrelated items, sprouting, flourishing, withering. only toward the western  
renaissance  
does the accreting knowledge begin to build up a momentum. the story of  
cryptology during  
these years is, in other words, exactly the story of mankind. china, the only high  
civilization  
of antiquity to use ideographic writing, seems never to have developed much  
real cryptography  
—perhaps for that reason. in one case known for military purposes,  
the 11th-century  
compilation, wu-ching tsung-yao ("essentials from military classics"),  
recommended a true if  
small code. to a list of 40 plain items, ranging from requests for bows and  
arrows to the  
report of a victory, the correspondents would assign the first 40 ideograms of  
a poem. then,  
when a lieutenant wished, for example, to request more arrows, he was to write  
the corresponding  
ideogram at a specified place on an ordinary dispatch and stamp his seal on it. in  
china's great  
neighbor to the west, india, whose civilization likewise developed early and to  
high estate,  
several forms of secret communications were known and, apparently, practiced.  
the artha-sastra,  
a classic work on statecraft attributed to kautilya, in describing the espionage  
service of  
india as practically riddling the country with spies, recommended that the  
officers of the  
institutes of espionage give their spies their assignments by secret  
writing. perhaps most

interesting to cryptologists, amateur or professional, is that vatsyayana's famous *teYtbook* of erotics, the *kamasutra*, lists secret writing as one of the 64 arts, or yogas, that women should know and practice. the fourth great civilization of antiquity, the Mesopotamian, rather paralleled Egypt early in its cryptographic evolution, but then surpassed it. thus, in the last period of cuneiform writing, in colophons written at Uruk (in present-day Iraq) under these Seleucid kings in the last few score years before the Christian era, occasional scribes converted their names into numbers. the encipherment—if such it be—may have been only for amusement or to show off.

Words “*puMMle*” is “puzzle” so **M** → **z**, “*teYtbook*” “textbook” so **Y** → **x**, “*antiBuity*” is “antiquity” so **B** → **q** and last “*Eust*” is “just” so **E** → **j**. These are all letters.

And the alphabet looks something like this:

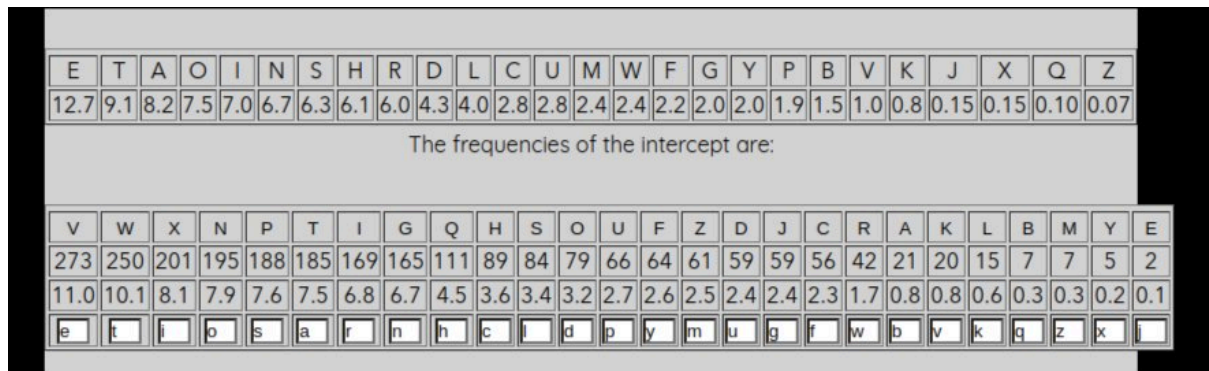


Fig 10. Decrypted Alphabet.

And the Full text is :

the addition of secrecy to the transformations produced cryptography. true, it was more of a game than anything else—it sought to delay comprehension for only the shortest possible time, not the longest—and the cryptanalysis was, likewise, just a puzzle. Egypt's was thus a quasi cryptography in contrast to the deadly serious science of today. yet great things have small beginnings, and these hieroglyphs did include, though in an imperfect fashion, the two elements of secrecy and transformation that comprise the essential attributes of the science. and so cryptography was born. in its first 3,000 years, it did not grow steadily. cryptography arose independently in many places, and in most of them it died the deaths of its



civilizations. in other places, it survived, embedded in a literature, and from this the next generation could climb to higher levels. but progress was slow and jerky. more was lost than

retained. much of the history of cryptology of this time is a patchwork, a crazy quilt of unrelated items, sprouting, flourishing, withering. only toward the western renaissance does the accreting knowledge begin to build up a momentum. the story of cryptology during these years is, in other words, exactly the story of mankind. china, the only high civilization of antiquity to use ideographic writing, seems never to have developed much real cryptography

—perhaps for that reason. in one case known for military purposes, the 11th-century compilation, wu-ching tsung-yao ("essentials from military classics"), recommended a true if small code. to a list of 40 plaintext items, ranging from requests for bows and arrows to the report of a victory, the correspondents would assign the first 40 ideograms of a poem. then, when a lieutenant wished, for example, to request more arrows, he was to write the corresponding

ideogram at a specified place on an ordinary dispatch and stamp his seal on it. in china's great neighbor to the west, india, whose civilization likewise developed early and to high estate, several forms of secret communications were known and, apparently, practiced. the artha-sastra,

a classic work on statecraft attributed to kautilya, in describing the espionage service of india as practically riddling the country with spies, recommended that the officers of the institutes of espionage give their spies their assignments by secret writing. perhaps most interesting to cryptologists, amateur or professional, is that vatsyayana's famous textbook of erotics, the kamasutra, lists secret writing as one of the 64 arts, or yogas, that women should

know and practice. the fourth great civilization of antiquity, the mesopotamian, rather paralleled egypt early in its cryptographic evolution, but then surpassed it. thus, in the last period of cuneiform writing, in colophons written at uruk (in present-day iraq) under the seleucid kings in the last few score years before the christian era, occasional scribes converted their names into numbers. the encipherment—if such it be—may have been only for amusement or to show off.

