Ministry of Education 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: Țapu Pavel FAF-223,

Checked: Dumitru Nirca asist. univ.

Chișinău 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.

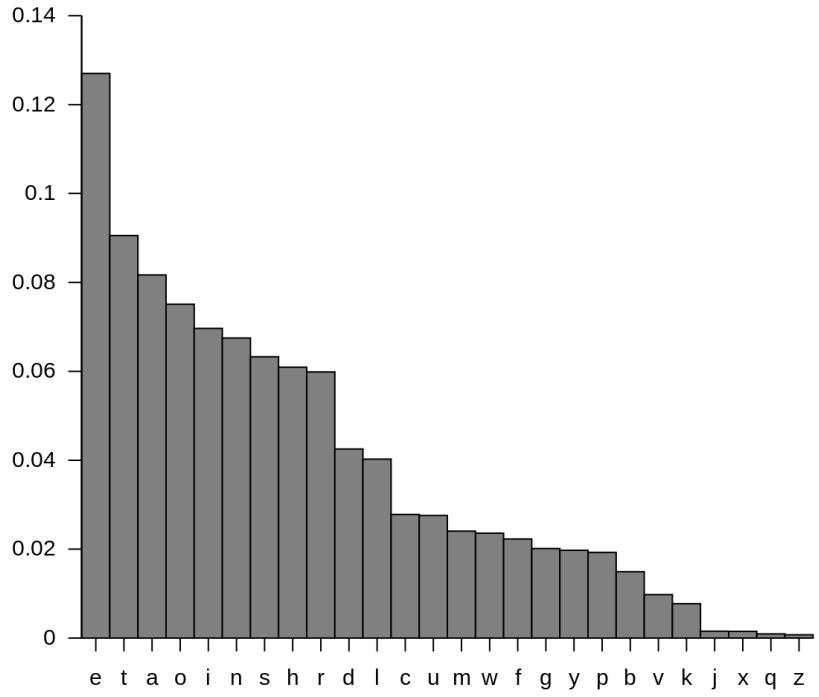

Fig.1: English letter frequency

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.26)

I have a cryptogram c = *Unsfaxdp tgo nwqvip gvkvi ptxo rqvwqvi tgf nc wqv pdapwxwdwxnghxuqvip wqvf ovphixavo rviv thwdtssf dpvo, tgo pn wqv cxipw twwvpwvo dpv ncwqtw jvgiv xg unsxwxhts tcctxip hnzv cinz wqv*

Inztgp — tgo cinz wqv jivtwvpw Inztg nc wqvz tss. EdsxdpHtvpti wqdp xzuivppvo qxp gtzv uviztgvgwsf xgwn hifuwnsnjf.Xw zdpw av wqtw tp pnng tp t hdswdiv qtp ivthqvo t hviwtxg svkvs,uinatasf zvtpdivo stijvsf af xwp sxwvithf, hifuwnjituqf tuuvtippungwtgvndpsf — tp xwp utivgwp, stgjdtjv tgo rixwxgj, uinatasf tspn oxo.Wqv zdswxusv qdztg gvvop tgo ovpxivp wqtw ovztgo

uixkthf tzngj wrnni zniv uvnusv xg wqv zxopw nc pnhxts sxcv zdpw xgvkxwtasf svto wnhifuwnsnjf

rqvivkvi zvg wqixkv tgo rqvivkvi wqvf rixwv. Hdswditsoxccdpxng pvvzp t svpp sxlvsf vyustgtwxng

cni xwp nhhdiivghv xg. pn ztgftivtp, ztgf nc wqvz oxpwtgw tgo xpnstwvo.Wqv Fvmxoxp, tg naphdiv

pvhw nc tandw 25,000 uvnusv xg, gniwqvig Xitb,dpv t hifuwxh phixuw xg wqvxi qnsf annlp avhtdpv

wqvf cvti uvipvhdwxng afwqvxi Znpsvz gvxjqanip. Wxavwtgp dpv t lxgo nc hxuqvi htssvo "ixg-pudgp"cni nccxhxts hniivpungovghv; xw xp gtzvo cni xwp xgkvgwni Ixg-h'(qqvg-)pudgp(-ut), rqn

sxkvo xg wqv 1300p. Wqv Gpxaxox pvhivw pnhxvwf nc Gxjvixtlvvup xwp uxhwnjituqxh phixuw cinz Vdinuvtgp tp zdhq tp unppxasvavhtdpv xw xp dpvo hqxvcsf wn vyuivpp snkv xg itwqvi oxivhw

xztjvif, tgoptzusvp tuuvti wn av tw svtpw tp unignjituqxh tp wqvf tiv hifuwnjituqxh.Wqv hifuwnjituqf

nc Wqtxstgo ovkvsnuvo dgovi Xgoxtg xgcsdvghv. Tgvzaifngxh pwdof nc wqv pdaevhw vkvg

tuuvtip
xg t jitzztwxhts rnilvgwxwsvo Unitgtktlft af Qsdtgj Uitpnw Tlptitgxwx (Uqv). Ngv pfpwvz,htssvo "wqv viixgj Pxtzvpv," pdapwxwdwvp ngv ovsxhtwv Pxtzvpv svwwvi cnitgnwqvi. Xg tgnwqvi pfpwvz, hngpngtgwp tiv oxkxovo xgwn pvkvg jindup nc cxkv svwwvip;t svwwvi xp xgoxhtwvo af
rixwxgj wqv Pxtzvpv gdzavi nc xwp jindu tgousthxgj kviwxhts onwp dgovi xw vbdts xg gdzavi wn
wqv svwwvi'p usthv xg xwpjindu. T pfpwvz htssvo "wqv qvizxw zvwtzniuqnpxgj svwwvip" rixwvp
wqvwvyw athlrtiop.Xg wqv Vdinuv nc wqv Stwxg tsuqtavw—cinz rqxhq znovig hifuwnsnjfrndso puixgj—hifuwnjituqf csxhlvivo rvtlsf. Rxwq wqv hnsstupv nc wqvInztg vzuxiv, Vdinuv qto usdgjvo
xgwn wqv naphdixwf nc wqv Otil Tjvp.Sxwvithf qto tss adw oxptuuvtivo. Tiwp tgo phxvghvp rviv
cnijnwwvg, tgohifuwnjituqf rtp gnw vyhvuwvo. Ngsf odixgj wqv Zxoosv Tjvp nhhtpxngtsztgdphixuwp, rxwq tg xgcivbdvgw pxjgtwdiv ni jsnpp ni "ovn jitwxtp" wqtw tanivo zngl
udw xgwn hxuqvi wn tzdpv qxzpvsc, cxwcdssf xssdzxgtwv wqvhifuwnsnjxh otilgvpp, tgo, sxlv t pxgjsv htgosv jdwwvixgj xg t jivtwzvoxvkts qtss, wqvxi cvvasv cstixgjp ngsf vzuqtpxmv wqv jsnnz.Wqv pfpwvzp dpvo rviv pxzusv xg wqv vywivzv. Uqitpvp rviv rixwwvgkviwxhtssf ni athlrtiop;
onwp rviv pdapwxwdwvo cni knrvsp;cnivxjg tsuqtavwp, tp Jivvl, Qvaivr, tgo Tizvgxtg, rviv dpvo;
vthqsvwwvi nc wqv ustxgwvyw rtp ivusthvo af wqv ngv wqtw cnssnrp xw; xg wqv znpwtoktghvo pfpwvz, puvhxts pxjgp pdapwxwdwvo cni svwwvip. Cni tsznpw twqndptgo fvtip, cinz avcniv 500 wn 1400, wqv hifuwnsnjf nc Rvpwvighxkxsxmtwxng pwtjgtwvo.

So first we look at the frequencies as shown bellow:

V	W	T	P	I	X	N	G	S	Q	O	U	H	D	Z	F	C	J	A	R	K	L	Y	B	M	E
313	219	203	181	176	173	153	147	115	97	88	85	84	70	65	63	52	50	41	30	22	16	6	3	3	2
12.7	8.9	8.3	7.4	7.2	7.0	6.2	6.0	4.7	3.9	3.6	3.5	3.4	2.8	2.6	2.6	2.1	2.0	1.7	1.2	0.9	0.7	0.2	0.1	0.1	0.1

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 $W \rightarrow t$. The my "T" letter has the same as "A" so also $T \rightarrow a$. So I get: *UNSFAXDP aGO NtQeIP GeKeI PaXO RQetQeI aGF NC* ***tQe*** *PDAPtXtDtXNGHXUQeIP tQeF OePHIXAeO ReIe*

aHtDaSSF DPeO, aGO PN tQe CXIPt attePteO DPe NCtQat JeGIe XG UNSXtXHaS aCCaXIP HNZe CINZ ***tQe***
INZaGP — aGO CINZ tQe JIeatePt INZaG NC tQeZ aSS. EDSXDPHaePaI tQDP XZUIePPeO QXP GaZe
UeIZaGeGtSF XGtN HIFUtNSNJF.Xt ZDPt Ae tQat aP PNNG aP a HDStDIe QaP IeaHQeO a HeItaXG
SeKeS,UINAaASF ZeaPDIeO SaIJeSF AF XtP SXteIaHF, HIFUtNJIaUQF aUUeaIPPUNGtaGeNDPSF — aP XtP
UaIeGtP, SaGJDaJe aGO RIXtXGJ, UINAaASF aSPN OXO.tQe ZDStXUSe QDZaG GeeOP aGO OePXIeP tQat OeZaGO
UIXKaHF aZNGJ tRNNI ZNIe UeNUSe XG tQe ZXOPt NC PNHXaS SXCe ZDPt XGeKXtaASF SeaO tNHIFUtNSNJF
RQeIeKeI ZeG tQIXKe aGO RQeIeKeI tQeF RIXte. HDStDIaSOXCCDPXNG PeeZP a SePP SXLeSF eYUSaGatXNG
CNI XtP NHHDIIeGHe XG. PN ZaGFaIeaP, ZaGF NC tQeZ OXPtaGt aGO XPNSateO.tQe FeMXOXP, aG NAPHDIe
PeHt NC aANDt 25,000 UeNUSe XG, GNItQeIG XIaB,DPe a HIFUtXH PHIXUt XG tQeXI QNSF ANNLP AeHaDPe
tQeF CeaI UeIPeHDtXNG AFtQeXI ZNPSeZ GeXJQANIP. tXAetaGP DPe a LXGO NC HXUQeI HaSSeO "IXG-
PUDGP"CNI NCCXHXaS HNIIePUNGOeGHe; Xt XP GaZeO CNI XtP XGKeGtNI IXG-H'(QQeG-)PUDGP(-Ua), RQN
SXKeO XG tQe 1300P. tQe GPXAXOX PeHIet PNHXetF NC GXJeIXaLeeUP XtP UXHtNJIaUQXH PHIXUt
CINZ eDINUeaGP aP ZDHQ aP UNPPXASeAeHaDPe Xt XP DPeO HQXeCSF tN eYUIePP SNKe XG IatQeI OXIeHt
XZaJeIF, aGOPaZUSeP aUUeaI tN Ae at SeaPt aP UNIGNJIaUQXH aP tQeF aIe HIFUtNJIaUQXH.tQe HIFUtNJIaUQF
NC tQaXSaGO OeKeSNUeO DGOeI XGOXaG XGCSDeGHe. aGeZAIFNGXH PtDOF NC tQe PDAEeHt eKeG aUUeaIP
XG a JIaZZatXHaS RNILeGtXtSeO UNIaGaKaLFa AF QSDaGJ UIaPNt aLPaIaGXtX (UQe). NGe PFPteZ,HaSSeO
"tQe eIIXGJ PXaZePe," PDAPtXtDteP NGe OeSXHate PXaZePe SetteI CNIaGNtQeI. XG aGNtQeI
PFPteZ, HNGPNGaGtP aIe OXKXOeO XGtN PeKeG JINDUP NC CXKe SetteIP;a SetteI XP XGOXHateO AF
RIXtXGJ tQe PXaZePe GDZAeI NC XtP JINDU aGOUSaHXGJ KeItXHaS ONtP DGOeI Xt eBDaS XG GDZAeI tN
tQe SetteI'P USaHe XG XtPJINDU. a PFPteZ HaSSeO "tQe QeIZXt ZetaZNIUQNPXGJ SetteIP" RIXteP
tQeteYt AaHLRaIOP.XG tQe eDINUe NC tQe SatXG aSUQaAet—CINZ RQXHQ ZNOeIG HIFUtNSNJFRNDSO
PUIXGJ—HIFUtNJIaUQF CSXHLeIeO ReaLSF. RXtQ tQe HNSSaUPe NC tQeINZaG eZUXIe, eDINUe QaO USDGJeO

XGtN tQe NAPHDIXtF NC tQe OaIL aJeP.SXteIaHF QaO aSS ADt OXPaUUeaIeO. aItP aGO PHXeGHeP ReIe
CNIJNtteG, aGOHIFUtNJIaUQF RaP GNt eYHeUteO. NGSF ODIXGJ tQe ZXOOSe aJeP
NHHaPXNGaSZaGDPHIXUtP, RXtQ aG XGCIeBDeGt PXJGatDIe NI JSNPP NI "OeN JIatXaP" tQat aANIeO ZNGL
UDt XGtN HXUQeI tN aZDPe QXZPeSC, CXtCDSSF XSSDZXGate tQeHIFUtNSNJXH OaILGePP, aGO, SXLe a
PXGJSe HaGOSe JDtteIXGJ XG a JIeatZeOXeKaS QaSS, tQeXI CeeASe CSaIXGJP NGSF eZUQaPXMe tQe
JSNNZ.tQe PFPteZP DPeO ReIe PXZUSe XG tQe eYtIeZe. UQIaPeP ReIe RIXtteGKeItXHaSSF NI AaHLRaIOP;
ONtP ReIe PDAPtXtDteO CNI KNReSP;CNIeXJG aSUQaAetP, aP JIeeL, QeAIeR, aGO aIZeGXaG, ReIe DPeO;
eaHQSetteI NC tQe USaXGteYt RaP IeUSaHeO AF tQe NGe tQat CNSSNRP Xt; XG tQe ZNPtaOKaGHeO
PFPteZ, PUeHXaS PXJGP PDAPtXtDteO CNI SetteIP. CNI aSZNPt atQNDPaGO FeaIP, CINZ AeCNIe 500
tN 1400, tQe HIFUtNSNJF NC RePteIGHXKXSXMatXNG PtaJGateO.

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 "tN" word we could assume it is "to". So the second must me "o", so **N → o**

*UoSFAXDP aGO otheIP GeKeI PaXO RhetheI aGF **oC** the PDAPtXtDtXoGHXUheIP **theF** OePHIXAeO ReIe aHtDaSSF DPeO, aGO Po the CXIPt attePteO DPe oCthat JeGIe XG UoSXtXHaS aCCaXIP HoZe CIoZ the IoZaGP — aGO CIoZ the JIeatePt IoZaG oC theZ aSS. EDSXDPHaePaI thDP XZUIePPeO hXP GaZe UeIZaGeGtSF XGto HIFUtoSoJF.Xt ZDPt Ae that aP PooG aP a HDStDIe haP IeaHheO a HeItaXG SeKeS,UIoAaASF ZeaPDIeO SaIJeSF AF XtP SXteIaHF, HIFUtoJIaUhF aUUeaIPPUoGtaGeoDPSF — aP XtP UaIeGtP, SaGJDaJe aGO RIXtXGJ, UIoAaASF aSPo OXO.the ZDStXUSe hDZaG GeeOP aGO OePXIeP that OeZaGO UIXKaHF aZoGJ tRooI ZoIe UeoUSe XG the ZXOPt oC PoHXaS SXCe ZDPt XGeKXtaASF SeaO toHIFUtoSoJF RheIeKeI ZeG thIXKe aGO RheIeKeI theF RIXte. HDStDIaSOXCCDPXoG PeeZP a SePP SXLeSF eYUSaGatXoG CoI XtP oHHDIIeGHe XG. Po ZaGFaIeaP, ZaGF oC theZ OXPtaGt aGO XPoSateO.the FeMXOXP, aG oAPHDIe PeHt oC aAoDt 25,000 UeoUSe XG, GoItheIG XIaB,DPe a HIFUtXH PHIXUt XG theXI hoSF AooLP AeHaDPe theF CeaI UeIPeHDtXoG AFtheXI ZoPSeZ GeXJhAoIP. tXAetaGP DPe a LXGO oC HXUheI HaSSeO "IXG- PUDGP"CoI oCCXHXaS HoIIePUoGOeGHe; Xt XP GaZeO CoI XtP XGKeGtoI IXG-H'(hheG-)PUDGP(-Ua), Rho SXKeO XG the 1300P. the GPXAXOX PeHIet PoHXetF oC GXJeIXaLeeUP XtP UXHtoJIaUhXH PHIXUt CIoZ eDIoUeaGP aP ZDHh aP UoPPXASeAeHaDPe Xt XP DPeO HhXeCSF to eYUIePP SoKe XG IatheI OXIeHt XZaJeIF, aGOPaZUSeP aUUeaI to Ae at SeaPt aP UoIGoJIaUhXH aP theF aIe HIFUtoJIaUhXH.the HIFUtoJIaUhF oC thaXSaGO OeKeSoUeO DGOeI XGOXaG XGCSDeGHe. aGeZAIFoGXH PtDOF oC the PDAEeHt eKeG aUUeaIP XG a JIaZZatXHaS RoILeGtXtSeO UoIaGaKaLFa AF hSDaGJ UIaPot aLPaIaGXtX (Uhe). oGe PFPteZ,HaSSeO "the eIIXGJ PXaZePe," PDAPtXtDteP oGe OeSXHate PXaZePe SetteI CoIaGotheI. XG aGotheI PFPteZ, HoGPoGaGtP aIe OXKXOeO XGto PeKeG JIoDUP oC CXKe SetteIP;a SetteI XP XGOXHateO AF RIXtXGJ the PXaZePe GDZAeI oC XtP JIoDU aGOUSaHXGJ KeItXHaS OotP DGOeI Xt eBDaS XG GDZAeI to*

the SetteI'P USaHe XG XtPJIoDU. a PFPteZ HaSSeO "the heIZXt ZetaZoIUhoPXGJ SetteIP" RIXteP theteYt AaHLRaIOP.XG the eDIoUe oC the SatXG aSUhaAet—CIoZ RhXHh ZoOeIG HIFUtoSoJFRoDSO PUIXGJ—HIFUtoJIaUhF CSXHLeIeO ReaLSF. RXth the HoSSaUPe oC theIoZaG eZUXIe, eDIoUe haO USDGJeO XGto the oAPHDIXtF oC the OaIL aJeP.SXteIaHF haO aSS ADt OXPaUUeaIeO. aItP aGO PHXeGHeP ReIe CoIJotteG, aGOHIFUtoJIaUhF RaP Got eYHeUteO. oGSF ODIXGJ the ZXOOSe aJeP oHHaPXoGaSZaGDPHIXUtP, RXth aG XGCIeBDeGt PXJGatDIe oI JSoPP oI "Oeo JIatXaP" that aAoIeO ZoGL UDt XGto HXUheI to aZDPe hXZPeSC, CXtCDSSF XSSDZXGate theHIFUtoSoJXH OaILGePP, aGO, SXLe a PXGJSe HaGOSe JDtteIXGJ XG a JIeatZeOXeKaS haSS, theXI CeeASe CSaIXGJP oGSF eZUhaPXMe the JSooZ.the PFPteZP DPeO ReIe PXZUSe XG the eYtIeZe. UhIaPeP ReIe RIXtteGKeItXHaSSF oI AaHLRaIOP; OotP ReIe PDAPtXtDteO CoI KoReSP;CoIeXJG aSUhaAetP, aP JIeeL, heAIeR, aGO aIZeGXaG, ReIe DPeO; eaHhSetteI oC the USaXGteYt RaP IeUSaHeO AF the oGe that CoSSoRP Xt; XG the ZoPtaOKaGHeO PFPteZ, PUeHXaS PXJGP PDAPtXtDteO CoI SetteIP. CoI aSZoPt athoDPaGO FeaIP, CIoZ AeCoIe 500 to 1400, the HIFUtoSoJF oC RePteIGHXKXSXMatXoG PtaJGateO.

Next we have the “oC” word so I assume it’s either “of” or “on” but since we have this word used several times in the same sentence, I assume it must be “of”. Since it is most used in English speaking, so **C →f.** Now the word “theF” may be “they” because of the context so **F →y**

Till now we have this:

V	e
T	a
W	t
Q	h
N	o
C	f
F	y

Fig.5: Frequency of cryptogram letters new

And the text: *UoSyAXDP aGO **otheIP** GeKeI PaXO RhetheI **aGy** of the PDAPtXtDtXoGHXUheIP they OePHIXAeO ReIe*

aHtDaSSy DPeO, aGO Po the fXIPt attePteO DPe ofthat JeGIe XG UoSXtXHaS affaXIP HoZe fIoZ the

IoZaGP — aGO fIoZ the JIeatePt IoZaG of theZ aSS. EDSXDPHaePaI thDP XZUIePPeO hXP GaZe

UeIZaGeGtSy XGto HIyUtoSoJy.Xt ZDPt Ae that aP PooG aP a HDStDIe haP IeaHheO a HeItaXG

SeKeS,UIoAaASy ZeaPDIeO SaIJeSy Ay XtP SXteIaHy, HIyUtoJIaUhy aUUeaIPPUoGtaGeoDPSy — aP XtP

UaIeGtP, SaGJDaJe aGO RIXtXGJ, UIoAaASy aSPo OXO.the ZDStXUSe hDZaG GeeOP aGO OePXIeP that OeZaGO

UIXKaHy aZoGJ tRooI ZoIe UeoUSe XG the ZXOPt of PoHXaS SXfe ZDPt XGeKXtaASy SeaO toHIyUtoSoJy
RheIeKeI ZeG thIXKe aGO RheIeKeI they RIXte. HDStDIaSOXffDPXoG PeeZP a SePP SXLeSy eYUSaGatXoG
foI XtP oHHDIIeGHe XG. Po ZaGyaIeaP, ZaGy of theZ OXPtaGt aGO XPoSateO.the yeMXOXP, aG oAPHDIe
PeHt of aAoDt 25,000 UeoUSe XG, GoItheIG XIaB,DPe a HIyUtXH PHIXUt XG theXI hoSy AooLP AeHaDPe
they feaI UeIPeHDtXoG AytheXI ZoPSeZ GeXJhAoIP. tXAetaGP DPe a LXGO of HXUheI HaSSeO "IXG-
PUDGP"foI offXHXaS HoIIePUoGOeGHe; Xt XP GaZeO foI XtP XGKeGtoI IXG-H'(hheG-)PUDGP(-Ua), Rho
SXKeO XG the 1300P. the GPXAXOX PeHIet PoHXety of GXJeIXaLeeUP XtP UXHtoJIaUhXH PHIXUt
fIoZ eDIoUeaGP aP ZDHh aP UoPPXASeAeHaDPe Xt XP DPeO HhXefSy to eYUIePP SoKe XG IatheI OXIeHt
XZaJeIy, aGOPaZUSeP aUUeaI to Ae at SeaPt aP UoIGoJIaUhXH aP they aIe HIyUtoJIaUhXH.the HIyUtoJIaUhy
of thaXSaGO OeKeSoUeO DGOeI XGOXaG XGfSDeGHe. aGeZAIyoGXH PtDOy of the PDAEeHt eKeG aUUeaIP
XG a JIaZZatXHaS RoILeGtXtSeO UoIaGaKaLya Ay hSDaGJ UIaPot aLPaIaGXtX (Uhe). oGe PyPteZ,HaSSeO
"the eIIXGJ PXaZePe," PDAPtXtDteP oGe OeSXHate PXaZePe SetteI foIaGotheI. XG aGotheI
PyPteZ, HoGPoGaGtP aIe OXKXOeO XGto PeKeG JIoDUP of fXKe SetteIP;a SetteI XP XGOXHateO Ay
RIXtXGJ the PXaZePe GDZAeI of XtP JIoDU aGOUSaHXGJ KeItXHaS OotP DGOeI Xt eBDaS XG GDZAeI to
the SetteI'P USaHe XG XtPJIoDU. a PyPteZ HaSSeO "the heIZXt ZetaZoIUhoPXGJ SetteIP" RIXteP
theteYt AaHLRaIOP.XG the eDIoUe of the SatXG aSUhaAet—fIoZ RhXHh ZoOeIG HIyUtoSoJyRoDSO
PUIXGJ—HIyUtoJIaUhy fSXHLeIeO ReaLSy. RXth the HoSSaUPe of theIoZaG eZUXIe, eDIoUe haO USDGJeO
XGto the oAPHDIXty of the OaIL aJeP.SXteIaHy haO aSS ADt OXPaUUeaIeO. aItP aGO PHXeGHeP ReIe
foIJotteG, aGOHIyUtoJIaUhy RaP Got eYHeUteO. oGSy ODIXGJ the ZXOOSe aJeP
oHHaPXoGaSZaGDPHIXUtP, RXth aG XGfIeBDeGt PXJGatDIe oI JSoPP oI "Oeo JIatXaP" that aAoIeO ZoGL
UDt XGto HXUheI to aZDPe hXZPeSf, fXtfDSSy XSSDZXGate theHIyUtoSoJXH OaILGePP, aGO, SXLe a
PXGJSe HaGOSe JDtteIXGJ XG a JIeatZeOXeKaS haSS, theXI feeASe fSaIXGJP oGSy eZUhaPXMe the

JSooZ.the PyPteZP DPeO ReIe PXZUSe XG the eYtIeZe. UhIaPeP ReIe RIXtteGKeItXHaSSy oI AaHLRaIOP;
OotP ReIe PDAPtXtDteO foI KoReSP;foIeXJG aSUhaAetP, aP JIeeL, heAIeR, aGO aIZeGXaG, ReIe DPeO;
eaHhSetteI of the USaXGteYt RaP IeUSaHeO Ay the oGe that foSSoRP Xt; XG the ZoPtaOKaGHeO
PyPteZ, PUeHXaS PXJGP PDAPtXtDteO foI SetteIP. foI aSZoPt athoDPaGO yeaIP, fIoZ AefoIe 500
to 1400, the HIyUtoSoJy of RePteIGHXKXSXMatXoG PtaJGateO.

Now above I have the word "aGy" so I conclude it must be "any" so **G → n**. Also at the start I have the word "otheIP" so it could be "others", so **I → r** and **P →s** After we apply it:

*UoSyAXDs **anO** others neKer saXO **Rhether** any of the sDAstXtDtXonHXUhers they OesHrXAeO Rere*
*aHtDaSSy DseO, anO so the **fXrst** attesteO Dse ofthat Jenre Xn UoSXtXHaS affaXrs HoZe froZ the*
roZans — anO froZ the Jreatest roZan of theZ aSS. EDSXDsHaesar thDs XZUresseO hXs naZe UerZanentSy Xnto HryUtoSoJy.Xt ZDst Ae that as soon as a HDStDre has reaHheO a HertaXn SeKeS,UroAaASy ZeasDreO SarJeSy Ay Xts SXteraHy, HryUtoJraUhy aUUearssUontaneoDsSy — as Xts
Uarents, SanJDaJe anO RrXtXnJ, UroAaASy aSso OXO.the ZDStXUSe hDZan neeOs anO OesXres that OeZanO
UrXKaHy aZonJ tRoor Zore UeoUSe Xn the ZXOst of soHXaS SXfe ZDst XneKXtaASy SeaO toHryUtoSoJy
RhereKer Zen thrXKe anO RhereKer they RrXte. HDStDraSOXffDsXon seeZs a Sess SXLeSy eYUSanatXon
for Xts oHHDrrenHe Xn. so Zanyareas, Zany of theZ OXstant anO XsoSateO.the yeMXOXs, an oAsHDre
seHt of aAoDt 25,000 UeoUSe Xn, northern XraB,Dse a HryUtXH sHrXUt Xn theXr hoSy AooLs AeHaDse
they fear UerseHDtXon AytheXr ZosSeZ neXJhAors. tXAetans Dse a LXnO of HXUher HaSSeO "rXn-
sUDns"for offXHXaS HorresUonOenHe; Xt Xs naZeO for Xts XnKentor rXn-H'(hhen-)sUDns(-Ua), Rho
SXKeO Xn the 1300s. the nsXAXOX seHret soHXety of nXJerXaLeeUs Xts UXHtoJraUhXH sHrXUt
froZ eDroUeans as ZDHh as UossXASeAeHaDse Xt Xs DseO HhXefSy to eYUress SoKe Xn rather OXreHt
XZaJery, anOsaZUSes aUUear to Ae at Seast as UornoJraUhXH as they are HryUtoJraUhXH.the HryUtoJraUhy
of thaXSanO OeKeSoUeO DnOer XnOXan XnfSDenHe. aneZAryonXH stDOy of the sDAEeHt eKen aUUears

Xn a JraZZatXHaS RorLentXtSeO UoranaKaLya Ay hSDanJ Urasot aLsaranXtX (Uhe). one systeZ,HaSSeO
"the errXnJ sXaZese," sDAstXtDtes one OeSXHate sXaZese Setter foranother. Xn another
systeZ, Honsonants are OXKXOeO Xnto seKen JroDUs of fXKe Setters;a Setter Xs XnOXHateO Ay
RrXtXnJ the sXaZese nDZAer of Xts JroDU anOUSaHXnJ KertXHaS Oots DnOer Xt eBDaS Xn nDZAer to
the Setter's USaHe Xn XtsJroDU. a systeZ HaSSeO "the herZXt ZetaZorUhosXnJ Setters" RrXtes
theteYt AaHLRarOs.Xn the eDroUe of the SatXn aSUhaAet—froZ RhXHh ZoOern HryUtoSoJyRoDSO
sUrXnJ—HryUtoJraUhy fSXHLereO ReaLSy. RXth the HoSSaUse of theroZan eZUXre, eDroUe haO USDnJeO
Xnto the oAsHDrXty of the OarL aJes.SXteraHy haO aSS ADt OXsaUUeareO. arts anO sHXenHes Rere
forJotten, anOHryUtoJraUhy Ras not eYHeUteO. onSy ODrXnJ the ZXOOSe aJes
oHHasXonaSZanDsHrXUts, RXth an XnfreBDent sXJnatDre or JSoss or "Oeo JratXas" that aAoreO ZonL
UDt Xnto HXUher to aZDse hXZseSf, fXtfDSSy XSSDZXnate theHryUtoSoJXH OarLness, anO, SXLe a
sXnJSe HanOSe JDtterXnJ Xn a JreatZeOXeKaS haSS, theXr feeASe fSarXnJs onSy eZUhasXMe the
JSooZ.the systeZs DseO Rere sXZUSe Xn the eYtreZe. Uhrases Rere RrXttenKertXHaSSy or AaHLRarOs;
Oots Rere sDAstXtDteO for KoReSs;foreXJn aSUhaAets, as JreeL, heAreR, anO arZenXan, Rere DseO;
eaHhSetter of the USaXnteYt Ras reUSaHeO Ay the one that foSSoRs Xt; Xn the ZostaOKanHeO
systeZ, sUeHXaS sXJns sDAstXtDteO for Setters. for aSZost athoDsanO years, froZ Aefore 500
to 1400, the HryUtoSoJy of ResternHXKXSXMatXon staJnateO.

After we apply it we see the 'anO' appearance could be "and". So **O → d.** Also I have the "Rhether" so the best word for it is "whether", so **R → w.** Also at the beginning we have the word "fXrst" and the bests match is "first", then **X → i.**

*UoSyAiDs and others **neKer** said whether any of the sDAstitDtionHiUhers they desHriAed were*
*aHtDaSSy Dsed, and so the first attested Dse ofthat Jenre in UoSitiHaS affairs HoZe **froZ** the roZans — and froZ the Jreatest roZan of theZ aSS. EDSiDsHaesar thDs iZUressed his naZe*
UerZanentSy into HryUtoSoJy.it ZDst Ae that as soon as a HDStDre has reaHhed a Hertain
SeKeS,UroAaASy ZeasDred SarJeSy Ay its SiteraHy, HryUtoJraUhy aUUearssUontaneoDsSy — as its

Uarents, SanJDaJe and writinJ, UroAaASy aSso did.the ZDStiUSe hDZan needs and desires that deZand
UriKaHy aZonJ twoor Zore UeoUSe in the Zidst of soHiaS Sife ZDst ineKitaASy Sead toHryUtoSoJy
whereKer Zen thriKe and whereKer they write. HDStDraSdiffDsion seeZs a Sess SiLeSy eYUSanation
for its oHHDrrenHe in. so Zanyareas, Zany of theZ distant and isoSated.the yeMidis, an oAsHDre
seHt of aAoDt 25,000 UeoUSe in, northern iraB,Dse a HryUtiH sHriUt in their hoSy AooLs AeHaDse
they fear UerseHDtion Aytheir ZosSeZ neiJhAors. tiAetans Dse a Lind of HiUher HaSSed "rin-sUDns"for offiHiaS HorresUondenHe; it is naZed for its inKentor rin-H'(hhen-)sUDns(-Ua), who
SiKed in the 1300s. the nsiAidi seHret soHiety of niJeriaLeeUs its UiHtoJraUhiH sHriUt
froZ eDroUeans as ZDHh as UossiASeAeHaDse it is Dsed HhiefSy to eYUress SoKe in rather direHt
iZaJery, andsaZUSes aUUear to Ae at Seast as UornoJraUhiH as they are HryUtoJraUhiH.the HryUtoJraUhy
of thaiSand deKeSoUed Dnder indian infSDenHe. aneZAryoniH stDdy of the sDAEeHt eKen aUUears
in a JraZZatiHaS worLentitSed UoranaKaLya Ay hSDanJ Urasot aLsaraniti (Uhe). one systeZ,HaSSed
"the errinJ siaZese," sDAstitDtes one deSiHate siaZese Setter foranother. in another
systeZ, Honsonants are diKided into seKen JroDUs of fiKe Setters;a Setter is indiHated Ay
writinJ the siaZese nDZAer of its JroDU andUSaHinJ KertiHaS dots Dnder it eBDaS in nDZAer to
the Setter's USaHe in itsJroDU. a systeZ HaSSed "the herZit ZetaZorUhosinJ Setters" writes
theteYt AaHLwards.in the eDroUe of the Satin aSUhaAet—froZ whiHh Zodern HryUtoSoJywoDSd
sUrinJ—HryUtoJraUhy fSiHLered weaLSy. with the HoSSaUse of theroZan eZUire, eDroUe had USDnJed
into the oAsHDrity of the darL aJes.SiteraHy had aSS ADt disaUUeared. arts and sHienHes were
forJotten, andHryUtoJraUhy was not eYHeUted. onSy dDrinJ the ZiddSe aJes
oHHasionaSZanDsHriUts, with an infreBDent siJnatDre or JSoss or "deo Jratias" that aAored ZonL
UDt into HiUher to aZDse hiZseSf, fitfDSSy iSSDZinate theHryUtoSoJiH darLness, and, SiLe a
sinJSe HandSe JDtterinJ in a JreatZedieKaS haSS, their feeASe fSarinJs onSy eZUhasiMe the JSooZ.the systeZs Dsed were siZUSe in the eYtreZe. Uhrases were writtenKertiHaSSy or AaHLwards;
dots were sDAstitDted for KoweSs;foreiJn aSUhaAets, as JreeL, heArew, and arZenian, were Dsed;
eaHhSetter of the USainteYt was reUSaHed Ay the one that foSSows it; in the ZostadKanHed

systeZ, sUeHiaS siJns sDAstitDted for Setters. for aSZost athoDsand years, froZ Aefore 500 to 1400, the HryUtoSoJy of westernHiKiSiMation staJnated.

Now we have the word "neKer" which definitely is the word "never", so **K → v.** Also we have the word "froZ" so based on the context is the word "from", so we have **Z → m.** Also we have the word "Aefore" so it is "before" so **A → b.**
And we have:

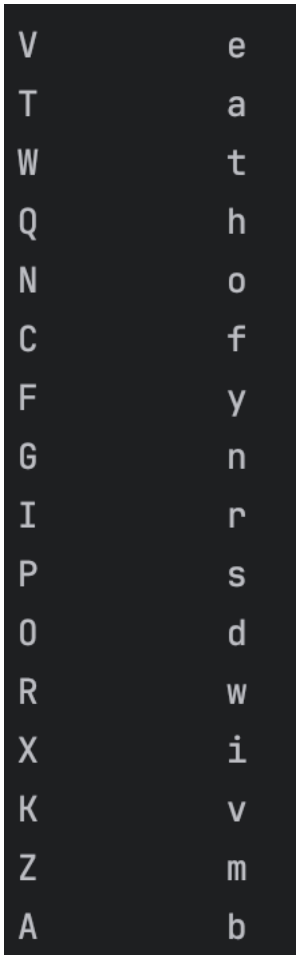

Fig.5: Frequency of cryptogram letters new

*UoSybiDs and others never said whether any of the sDbstitDtionHiUhers they **desHribed** were aHtDaSSy Dsed, and so the first attested Dse ofthat Jenre in UoSitiHaS affairs Home from the romans — and from the Jreatest roman of them aSS. EDSiDsHaesar thDs imUressed his name UermanentSy into HryUtoSoJy.it mDst be that as soon as a HDStDre has reaHhed a Hertain SeveS,UrobabSy measDred SarJeSy by its SiteraHy, HryUtoJraUhy aUUearssUontaneoDsSy — as its*
*Uarents, SanJDaJe and writinJ, UrobabSy **aSso** did.the mDStiUSe hDman needs and desires that demand*
UrivaHy amonJ twoor more UeoUSe in the midst of soHiaS Sife mDst inevitabSy Sead toHryUtoSoJy

wherever men thrive and wherever they write. HDStDraSdiffDsion seems a Sess SiLeSy eYUSanation
for its oHHDrrenHe in. so manyareas, many of them distant and isoSated.the yeMidis, an obsHDre
seHt of aboDt 25,000 UeoUSe in, northern iraB,Dse a HryUtiH sHriUt in their hoSy booLs beHaDse
they fear UerseHDtion bytheir mosSem neiJhbors. tibetans Dse a Lind of HiUher HaSSed "rin-sUDns"for offiHiaS HorresUondenHe; it is named for its inventor rin-H'(hhen-)sUDns(-Ua), who
Sived in the 1300s. the nsibidi seHret soHiety of niJeriaLeeUs its UiHtoJraUhiH sHriUt
from eDroUeans as mDHh as UossibSebeHaDse it is Dsed HhiefSy to eYUress Sove in rather direHt
imaJery, andsamUSes aUUear to be at Seast as UornoJraUhiH as they are HryUtoJraUhiH.the HryUtoJraUhy
of thaiSand deveSoUed Dnder indian infSDenHe. anembryoniH stDdy of the sDbEeHt even aUUears
in a JrammatiHaS worLentitSed UoranavaLya by hSDanJ Urasot aLsaraniti (Uhe). one system,HaSSed
"the errinJ siamese," sDbstitDtes one deSiHate siamese Setter foranother. in another
system, Honsonants are divided into seven JroDUs of five Setters;a Setter is indiHated by
writinJ the siamese nDmber of its JroDU andUSaHinJ vertiHaS dots Dnder it eBDaS in nDmber to
the Setter's USaHe in itsJroDU. a system HaSSed "the hermit metamorUhosinJ Setters" writes theteYt baHLwards.in the eDroUe of the Satin aSUhabet—from whiHh modern HryUtoSoJywoDSd
sUrinJ—HryUtoJraUhy fSiHLered weaLSy. with the HoSSaUse of theroman emUire, eDroUe had USDnJed
into the obsHDrity of the darL aJes.SiteraHy had aSS bDt disaUUeared. arts and sHienHes were
forJotten, andHryUtoJraUhy was not eYHeUted. onSy dDrinJ the middSe aJes
oHHasionaSmanDsHriUts, with an infreBDent siJnatDre or JSoss or "deo Jratias" that abored monL
UDt into HiUher to amDse himseSf, fitfDSSy iSSDminate theHryUtoSoJiH darLness, and, SiLe a
sinJSe HandSe JDtterinJ in a JreatmedievaS haSS, their feebSe fSarinJs onSy emUhasiMe the JSoom.the systems Dsed were simUSe in the eYtreme. Uhrases were writtenvertiHaSSy or baHLwards;
dots were sDbstitDted for voweSs;foreiJn aSUhabets, as JreeL, hebrew, and armenian, were Dsed;
eaHhSetter of the USainteYt was reUSaHed by the one that foSSows it; in the mostadvanHed system, sUeHiaS siJns sDbstitDted for Setters. for aSmost athoDsand years, from before 500 to 1400, the HryUtoSoJy of westernHiviSiMation staJnated.

Next we see the word “desHribed” which is “described” for sure, so **H → c**. Also the “neiJhbors” is “neighbors”, so **J → g.** Next we have the word “aSso”, which is the word “also”, so **S → l.**

UolybiDs and others never said whether any of the sDbstitDtionciUhers they described were actDally Dsed, and so the first attested Dse ofthat genre in Uolitical affairs come from the romans — and from the greatest roman of them all. EDliDscaesar thDs imUressed his name Uermanently into cryUtology.it mDst be that as soon as a cDltDre has reached a certain level,Urobably measDred largely by its literacy, cryUtograUhy aUUearssUontaneoDsly — as its

Uarents, langDage and writing, Urobably also did.the mDltiUle hDman needs and desires that demand

Urivacy among twoor more UeoUle in the midst of social life mDst inevitably lead tocryUtology

wherever men thrive and wherever they write. cDltDraldiffDsion seems a less liLely eYUlanation

for its occDrrence in. so manyareas, many of them distant and isolated.the yeMidis, an obscDre sect of aboDt 25,000 UeoUle in, northern iraB,Dse a cryUtic scriUt in their holy booLs becaDse

they fear UersecDtion bytheir moslem neighbors. tibetans Dse a Lind of ciUher called "rin-sUDns"for official corresUondence; it is named for its inventor rin-c'(hhen-)sUDns(-Ua), who lived in the 1300s. the nsibidi secret society of nigeriaLeeUs its UictograUhic scriUt

from eDroUeans as mDch as UossiblebecaDse it is Dsed chiefly to eYUress love in rather direct

imagery, andsamUles aUUear to be at least as UornograUhic as they are cryUtograUhic.the cryUtograUhy

of thailand develoUed Dnder indian inflDence. anembryonic stDdy of the sDbEect even aUUears

in a grammatical worLentitled UoranavaLya by hlDang Urasot aLsaraniti (Uhe). one system,called

"the erring siamese," sDbstitDtes one delicate siamese letter foranother. in another system, consonants are divided into seven groDUs of five letters;a letter is indicated by writing the siamese nDmber of its groDU andUlacing vertical dots Dnder it eBDal in nDmber to

the letter's Ulace in itsgroDU. a system called "the hermit metamorUhosing letters" writes theteYt bacLwards.in the eDroUe of the latin alUhabet—from which modern cryUtologywoDld sUring—cryUtograUhy flicLered weaLly. with the collaUse of theroman emUire, eDroUe had UlDnged

into the obscDrity of the darL ages.literacy had all bDt disaUUeared. arts and sciences were forgotten, andcryUtograUhy was not eYceUted. only dDring the middle ages occasionalmanDscriUts, with an infreBDent signatDre or gloss or "deo gratias" that abored monL

UDt into ciUher to amDse himself, fitfDlly illDminate thecryUtologic darLness, and, liLe a single candle gDttering in a greatmedieval hall, their feeble flarings only emUhasiMe the

gloom.the systems Dsed were simUle in the eYtreme. Uhrases were writtenvertically or bacLwards;
dots were sDbstitDted for vowels;foreign alUhabets, as greeL, hebrew, and armenian, were Dsed;
eachletter of the UlainteYt was reUlaced by the one that follows it; in the mostadvanced system, sUecial signs sDbstitDted for letters. for almost athoDsand years, from before 500 to 1400, the cryUtology of westerncivili Mation stagnated.

Here we have other words like: “mDst” which is “must” based on the context, so **D → u,** also the word “cryUtograUhy” is clearly “cryptography”, so **U → p.**
Now we have most of the words:

V	e
T	a
W	t
Q	h
N	o
C	f
F	y
G	n
I	r
P	s
O	d
R	w
X	i
K	v
Z	m
A	b
H	c
J	g
S	l
U	p
D	u

Here we have:
polybius and others never said whether any of the substitutionciphers they described were actually used, and so the first attested use ofthat genre in political affairs come from the romans — and from the greatest roman of them all. Euliuscaesar thus impressed his name permanently into cryptology.it must be that as soon as a culture has reached a certain level,probably measured largely by its literacy, cryptography appearsspontaneously — as its parents, language and writing, probably also did.the multiple human needs and desires that demand
*privacy among twoor more people in the midst of social life must inevitably lead tocryptology wherever men thrive and wherever they write. culturaldiffusion seems a less **liLely** eYplanation for its occurrence in. so manyareas, many of them distant and isolated.the yeMidis, an obscure sect of about 25,000 people in, northern iraB,use a cryptic script in their holy booLs because they fear persecution bytheir moslem neighbors. tibetans use a Lind of cipher called "rin-spuns"for official correspondence; it is named for its inventor rin-c'(hhen-)spuns(-pa), who lived in the 1300s. the nsibidi secret society of nigeriaLeeps its pictographic script*
from europeans as much as possiblebecause it is used chiefly to eYpress love in rather direct

imagery, andsamples appear to be at least as pornographic as they are cryptographic.the cryptography
of thailand developed under indian influence. anembryonic study of the subEect even appears in a grammatical worLentitled poranavaLya by hluang prasot aLsaraniti (phe). one system,called
"the erring siamese," substitutes one delicate siamese letter foranother. in another system, consonants are divided into seven groups of five letters;a letter is indicated by writing the siamese number of its group andplacing vertical dots under it eBual in number to the letter's place in itsgroup. a system called "the hermit metamorphosing letters" writes theteYt bacLwards.in the europe of the latin alphabet—from which modern cryptologywould spring—cryptography flicLered weaLly. with the collapse of theroman empire, europe had plunged
into the obscurity of the darL ages.literacy had all but disappeared. arts and sciences were forgotten, andcryptography was not eYcepted. only during the middle ages occasionalmanuscripts, with an infreBuent signature or gloss or "deo gratias" that abored monL
put into cipher to amuse himself, fitfully illuminate thecryptologic darLness, and, liLe a single candle guttering in a greatmedieval hall, their feeble flarings only ***emphasiMe*** *the gloom.the systems used were simple in the* ***eYtreme****. phrases were writtenvertically or bacLwards;*
dots were substituted for vowels;foreign alphabets, as greeL, hebrew, and armenian, were used;
eachletter of the plainteYt was replaced by the one that follows it; in the mostadvanced system, special signs substituted for letters. for almost athousand years, from before 500 to 1400, the cryptology of westernciviliMation stagnated.

The “emphasiMe” word is “emphasize” so **M → z,** “eYtreme” is “extreme”, so **Y → x,** “subEect” is definitely “subject” so **E → j,** and last but not least the word “liLely” is for sure “likely”, so **L → k.**

Now we have:

polybius and others never said whether any of the substitutionciphers they described were actually used, and so the first attested use ofthat genre in political affairs come from the romans — and from the greatest roman of them all. juliuscaesar thus impressed his name permanently into cryptology.it must be that as soon as a culture has reached a certain level,probably measured largely by its literacy, cryptography appearsspontaneously — as its parents, language and writing, probably also did.the multiple human needs and desires that demand
privacy among twoor more people in the midst of social life must inevitably lead tocryptology wherever men thrive and wherever they write. culturaldiffusion seems a less likely explanation for its occurrence in. so manyareas, many of them distant and isolated.the yezidis, an obscure sect of about 25,000 people in, northern iraB,use a cryptic script in their holy books because they fear persecution bytheir moslem neighbors. tibetans use a kind of cipher called "rin-spuns"for official correspondence; it is named for its inventor rin-c'(hhen-)spuns(-pa), who

lived in the 1300s. the nsibidi secret society of nigeriakeeps its pictographic script from europeans as much as possiblebecause it is used chiefly to express love in rather direct imagery, andsamples appear to be at least as pornographic as they are cryptographic.the cryptography of thailand developed under indian influence. anembryonic study of the subject even appears in a grammatical workentitled poranavakya by hluang prasot aksaraniti (phe). one system,called "the erring siamese," substitutes one delicate siamese letter foranother. in another system, consonants are divided into seven groups of five letters;a letter is indicated by writing the siamese number of its group andplacing vertical dots under it eBual in number to the letter's place in itsgroup. a system called "the hermit metamorphosing letters" writes thetext backwards.in the europe of the latin alphabet—from which modern cryptologywould spring—cryptography flickered weakly. with the collapse of theroman empire, europe had plunged into the obscurity of the dark ages.literacy had all but disappeared. arts and sciences were forgotten, andcryptography was not excepted. only during the middle ages occasionalmanuscripts, with an infreBuent signature or gloss or "deo gratias" that abored monk put into cipher to amuse himself, fitfully illuminate thecryptologic darkness, and, like a single candle guttering in a greatmedieval hall, their feeble flarings only emphasize the gloom.the systems used were simple in the extreme. phrases were writtenvertically or backwards; dots were substituted for vowels;foreign alphabets, as greek, hebrew, and armenian, were used; eachletter of the plaintext was replaced by the one that follows it; in the mostadvanced system, special signs substituted for letters. for almost athousand years, from before 500 to 1400, the cryptology of westerncivilization stagnated.

Now I have only one letter left, so by elimination, the replacement is **B → q.**
And the decrypted alphabet looks something like this:

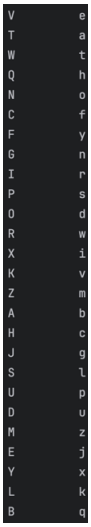

Fig 10. Decryted Alphabet.

And the Full text is :

polybius and others never said whether any of the substitutionciphers they described were actually used, and so the first attested use ofthat genre in political affairs come from the romans — and from the greatest roman of them all. juliuscaesar thus impressed his name permanently into cryptology.it must be that as soon as a culture has reached a certain level,probably measured largely by its literacy, cryptography appearsspontaneously — as its parents, language and writing, probably also did.the multiple human needs and desires that demand

privacy among twoor more people in the midst of social life must inevitably lead tocryptology wherever men thrive and wherever they write. culturaldiffusion seems a less likely explanation for its occurrence in. so manyareas, many of them distant and isolated.the yezidis, an obscure sect of about w5,000 people in, northern iraq,use a cryptic script in their holy books because they fear persecution bytheir moslem neighbors. tibetans use a kind of cipher called "rin-spuns"for official correspondence; it is named for its inventor rin-c'(hhen-)spuns(-pa), who lived in the 1300s. the nsibidi secret society of nigeriakeeps its pictographic script from europeans as much as possiblebecause it is used chiefly to express love in rather direct imagery, andsamples appear to be at least as pornographic as they are cryptographic.the cryptography

of thailand developed under indian influence. anembryonic study of the subject even appears in a grammatical workentitled poranavakya by hluang prasot aksaraniti (phe). one system,called

"the erring siamese," substitutes one delicate siamese letter foranother. in another system, consonants are divided into seven groups of five letters;a letter is indicated by writing the siamese number of its group andplacing vertical dots under it equal in number to the letter's place in itsgroup. a system called "the hermit metamorphosing letters" writes thetext backwards.in the europe of the latin alphabet—from which modern cryptologywould spring—cryptography flickered weakly. with the collapse of theroman empire, europe had plunged

into the obscurity of the dark ages.literacy had all but disappeared. arts and sciences were forgotten, andcryptography was not excepted. only during the middle ages occasionalmanuscripts, with an infrequent signature or gloss or "deo gratias" that abored monk

put into cipher to amuse himself, fitfully illuminate thecryptologic darkness, and, like a single candle guttering in a greatmedieval hall, their feeble flarings only emphasize the gloom.the systems used were simple in the extreme. phrases were writtenvertically or backwards;

dots were substituted for vowels;foreign alphabets, as greek, hebrew, and armenian, were used;

eachletter of the plaintext was replaced by the one that follows it; in the mostadvanced system, special signs substituted for letters. for almost athousand years, from before 500 to 1400, the cryptology of westerncivilization stagnated.