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: Berco Andrei, FAF - 221

Checked: asist. univ., Nirca Dumitru

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.

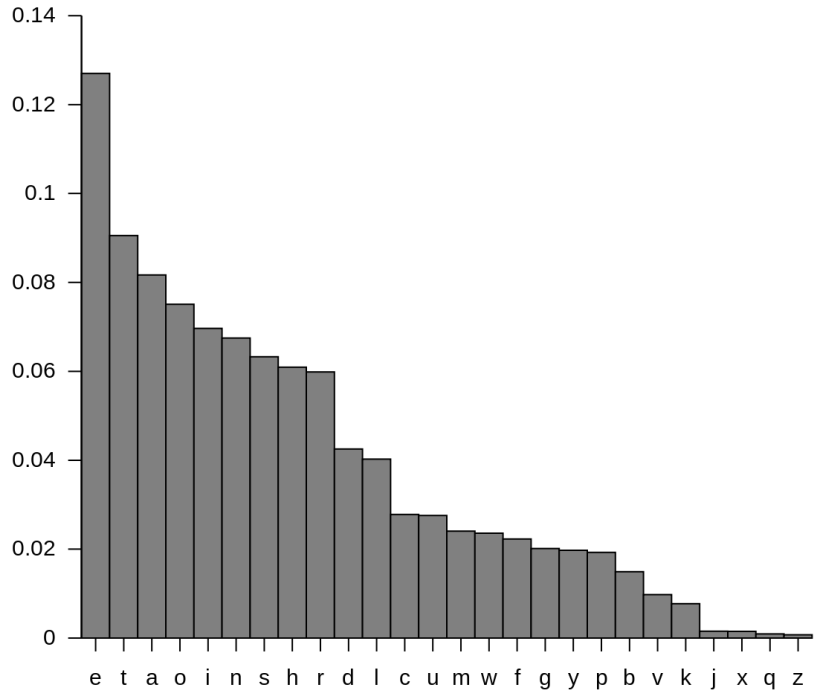

Fig.1: English letter frequency

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.3)

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 "ixgpudgp"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:

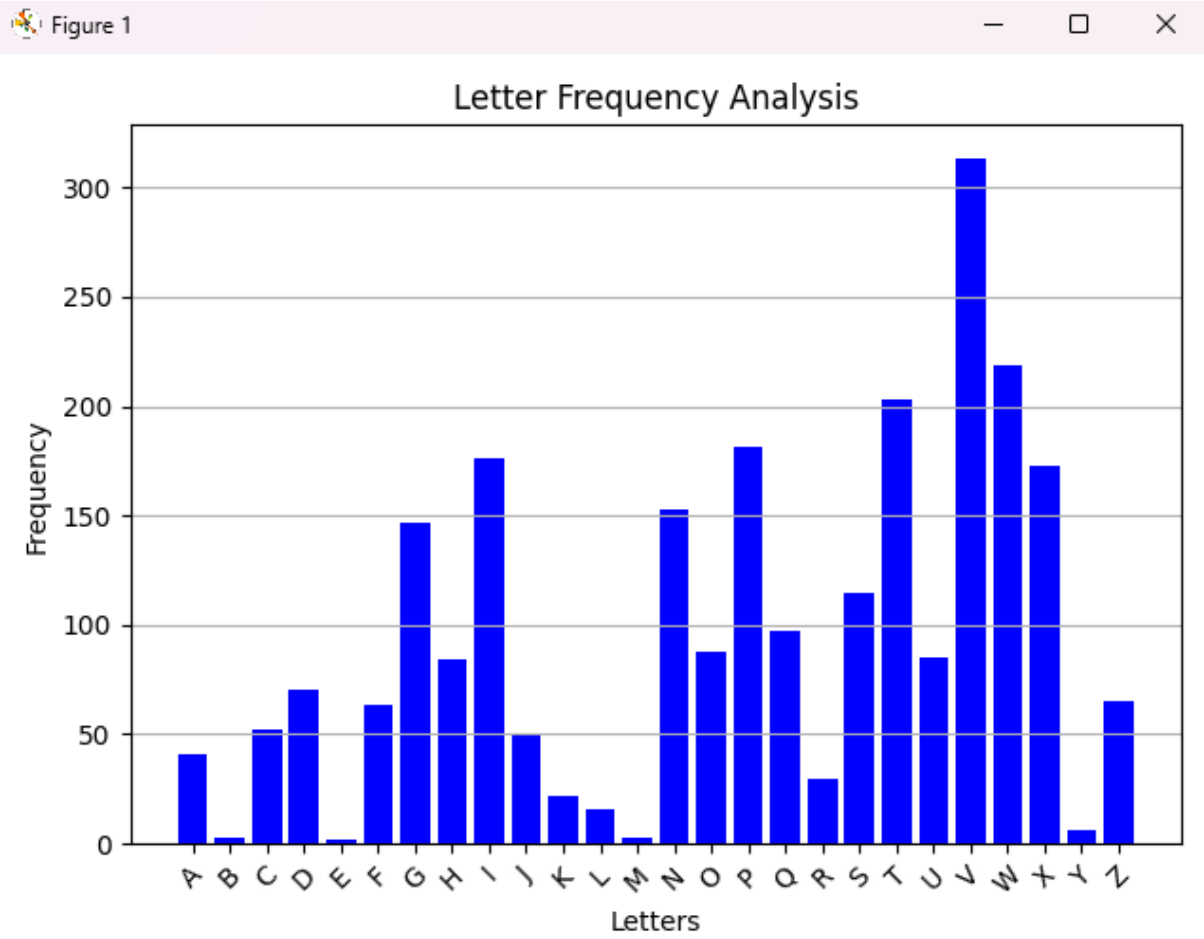

Fig.3: Frequency of cryptogram letters(in my case)

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 tgo nTqEip gEkEi ptxo rqETqEi tgf nc TqE pdapTxTdTxnghxuqEip TqEf oEphixaEo rEiEthTdtssf dpEo, tgo pn TqE cxipT tTTEpTEo dpE ncTqtT jEgiE xg unsxTxhts tcctxip hnzE cinz TqEInztgp — tgo cinz TqE jiEtTEpT Inztg nc TqEz tss. EdsxdpHtEpti Tqdp xzuiEppEo qxp gtzEuEiztgEgTsf xgTn hifuTnsnjf.XT zdpT aE TqtT tp pnng tp t hdsTdiE qtp iEthqEo t hEiTtxgsEkEs,uinatasf zEtpdiEo stijEsf af xTp sxTEithf, hifuTnjituqf tuuEtippungTtgEndpsf — tp xTputiEgTp, stgjdtjE tgo rixTxgj, uinatasf tspn oxo.TqE zdsTxusE qdztg gEEop tgo oEpxiEp TqtT oEztgouixkthf tzngj Trnni zniE uEnusE xg TqE zxopT nc pnhxts sxcE zdpT xgEkxTtasf sEto TnhifuTnsnjfrqEiEkEi zEg TqixkE tgo rqEiEkEi TqEf rixTE. HdsTditsoxccdpxng pEEzp t sEpp sxlEsf EyustgtTxngcni xTp nhhdiiEghE xg. pn ztgftiEtp, ztgf nc TqEz oxpTtgT tgo xpnstTEo.TqE FEmxoxp, tg naphdiEpEhT nc tandT 25,000 uEnusE xg, gniTqEig Xitb,dpE t hifuTxh phixuT xg TqExi qnsf annlp aEhtdpETqEf cEti uEipEhdTxng afTqExi ZnpsEz gExjqanip. TxaETtgp dpE t lxgo nc hxuqEi htssEo "ixgpudgp"cni nccxhxts hniiEpungoEghE; xT xp gtzEo cni xTp xgkEgTni Ixg-h'(qqEg-)pudgp(-ut), rqnsxkEo xg TqE 1300p. TqE Gpxaxox pEhiET pnhxETf nc GxjEixtlEEup xTp uxhTnjituqxh phixuTcinz EdinuEtgp tp zdhq tp unppxasEaEhtdpE xT xp dpEo hqxEcsf Tn EyuiEpp snkE xg itTqEi oxiEhTxztjEif, tgoptzusEp tuuEti Tn aE tT sEtpT tp unignjituqxh tp TqEf tiE hifuTnjituqxh.TqE hifuTnjituqfnc Tqtxstgo oEkEsnuEo dgoEi Xgoxtg xgcsdEghE. TgEzaifngxh pTdof nc TqE pdaeEhT EkEg tuuEtipxg t jitzztTxhts rnilEgTxTsEo Unitgtktlft af Qsdtgj UitpnT TlptitgxTx (UqE). NgE pfpTEz,htssEo"TqE Eiixgj PxtzEpE," pdapTxTdTEp ngE oEsxhtTE PxtzEpE sETTEi cnitgnTqEi. Xg tgnTqEipfpTEz, hngpngtgTp tiE oxkxoEo xgTn pEkEg jindup nc cxkE sETTEip;t sETTEi xp xgoxhtTEo afrixTxgj TqE PxtzEpE gdzaEi nc xTp jindu tgousthxgj kEiTxhts onTp dgoEi xT Ebdts xg gdzaEi TnTqE sETTEi'p usthE xg xTpjindu. T pfpTEz htssEo "TqE qEizxT zETtzniuqnpxgj sETTEip" rixTEpTqETEyT athlrtiop.Xg TqE EdinuE nc TqE StTxg tsuqtaET—cinz rqxhq znoEig hifuTnsnjfrndsopuixgj—hifuTnjituqf csxhlEiEo rEtlsf. RxTq TqE hnsstupE nc TqEInztg EzuxiE, EdinuE qto usdgjEoxgTn TqE naphdixTf nc TqE Otil TjEp.SxTEithf qto tss adT oxptuuEtiEo. TiTp tgo phxEghEp rEiEcnijnTTEg, tgohifuTnjituqf rtp gnT EyhEuTEo. Ngsf odixgj TqE ZxoosE TjEpnhhtpxngtsztgdphixuTp, rxTq tg xgciEbdEgT pxjgtTdiE ni jsnpp ni "oEn jitTxtp" TqtT taniEo zngludT xgTn hxuqEi Tn tzdpE qxzpEsc, cxTcdssf xssdzxgtTE TqEhifuTnsnjxh otilgEpp, tgo, sxlE tpxgjsE htgosE jdTTEixgj xg t jiEtTzEoxEkts qtss, TqExi cEEasE cstixgjp ngsf EzuqtpxmE TqEjsnnz.TqE pfpTEzp dpEo rEiE pxzusE xg TqE EyTiEzE. UqitpEp rEiE rixTTEgkEiTxhtssf ni athlrtiop;onTp rEiE pdapTxTdTEo cni knrEsp;cniExjg tsuqtaETp, tp JiEEl, QEaiEr, tgo TizEgxtg, rEiE dpEo;EthqsETTEi nc TqE ustxgTEyT rtp iEusthEo af TqE ngE TqtT cnssnrp xT; xg TqE znpTtoktghEopfpTEz, puEhxts pxjgp pdapTxTdTEo cni sETTEip. Cni tsznpT tTqndptgo fEtip, cinz aEcniE 500Tn 1400, TqE hifuTnsnjf nc REpTEighxkxsxmtTxng pTtjgtTEo*

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 "t" word we could assume it is "a". So **T → A**

Unsfaxdp Ago nTHEip gEkEi pAxo rHETHEi Agf nc THE pdapTxTdTxnghxuHEip THEf oEphixaEo rEiEAhTdAssf dpEo, Ago pn THE cxipT ATTEpTEo dpE ncTHAT jEgiE xg

unsxTxhAs AccAxip hnzE cinz THEInzAgp — Ago cinz THE jiEATEpT InzAg nc THEz Ass. EdsxdpHAEpAi THdp xzuiEppEo Hxp gAzEuEizAgEgTsf xgTn hifuTnsnjf.XT zdpT aE THAT Ap pnng Ap A hdsTdiE HAp iEAhHEo A hEiTAxgsEkEs,uinaAasf zEApdiEo sAijEsf af xTp sxTEiAhf, hifuTnjiAuHf AuuEAippungTAgEndpsf — Ap xTpuAiEgTp, sAgjdAjE Ago rixTxgj, uinaAasf Aspn oxo.THE zdsTxusE HdzAg gEEop Ago oEpxiEp THAT oEzAgouixkAhf Azngj Trnni zniE uEnusE xg THE zxopT nc pnhxAs sxcE zdpT xgEkxTAasf sEAo TnhifuTnsnjfrHEiEkEi zEg THixkE Ago rHEiEkEi THEf rixTE. HdsTdiAsoxccdpxng pEEzp A sEpp sxlEsf EyusAgATxngcni xTp nhhdiiEghE xg. pn zAgfAiEAp, zAgf nc THEz oxpTAgT Ago xpnsATEo.THE FEmxoxp, Ag naphdiEpEhT nc AandT 25,000 uEnusE xg, gniTHEig XiAb,dpE A hifuTxh phixuT xg THExi Hnsf annlp aEhAdpETHEf cEAi uEipEhdTxng afTHExi ZnpsEz gExjHanip. TxaETAgp dpE A lxgo nc hxuHEi hAssEo "ixgpudgp"cni nccxhxAs hniiEpungoEghE; xT xp gAzEo cni xTp xgkEgTni Ixg-h'(HHEg-)pudgp(-uA), rHnsxkEo xg THE 1300p. THE Gpxaxox pEhiET pnhxETf nc GxjEixAlEEup xTp uxhTnjiAuHxh phixuTcinz EdinuEAgp Ap zdhH Ap unppxasEaEhAdpE xT xp dpEo hHxEcsf Tn EyuiEpp snkE xg iATHEi oxiEhTxzAjEif, AgopAzusEp AuuEAi Tn aE AT sEApT Ap unignjiAuHxh Ap THEf AiE hifuTnjiAuHxh.THE hifuTnjiAuHfnc THAxsAgo oEkEsnuEo dgoEi XgoxAg xgcsdEghE. AgEzaifngxh pTdof nc THE pdaeEhT EkEg AuuEAipxg A jiAzzATxhAs rnilEgTxTsEo UniAgAkAlfA af HsdAgj UiApnT AlpAiAgxTx (UHE). NgE pfpTEz,hAssEo"THE Eiixgj PxAzEpE," pdapTxTdTEp ngE oEsxhATE PxAzEpE sETTEi cniAgnTHEi. Xg AgnTHEipfpTEz, hngpngAgTp AiE oxkxoEo xgTn pEkEg jindup nc cxkE sETTEip;A sETTEi xp xgoxhATEo afrixTxgj THE PxAzEpE gdzaEi nc xTp jindu AgousAhxgj kEiTxhAs onTp dgoEi xT EbdAs xg gdzaEi TnTHE sETTEi'p usAhE xg xTpjindu. A pfpTEz hAssEo "THE HEizxT zETAzniuHnpxgj sETTEip" rixTEpTHETEyT aAhlrAiop.Xg THE EdinuE nc THE SATxg AsuHAaET—cinz rHxhH znoEig hifuTnsnjfrndsopuixgj—hifuTnjiAuHf csxhlEiEo rEAlsf. RxTH THE hnssAupE nc THEInzAg EzuxiE, EdinuE HAo usdgjEoxgTn THE naphdixTf nc THE OAil AjEp.SxTEiAhf HAo Ass adT oxpAuuEAiEo. AiTp Ago phxEghEp rEiEcnijnTTEg, AgohifuTnjiAuHf rAp gnT EyhEuTEo. Ngsf odixgj THE ZxoosE AjEpnhhApxngAszAgdphixuTp, rxTH Ag xgciEbdEgT pxjgATdiE ni jsnpp ni "oEn jiATxAp" THAT AaniEo zngludT xgTn hxuHEi Tn AzdpE HxzpEsc, cxTcdssf xssdzxgATE THEhifuTnsnjxh oAilgEpp, Ago, sxlE ApxgjsE hAgosE jdTTEixgj xg A jiEATzEoxEkAs HAss, THExi cEEasE csAixgjp ngsf EzuHApxmE THEjsnnz.THE pfpTEzp dpEo rEiE pxzusE xg THE EyTiEzE. UHiApEp rEiE rixTTEgkEiTxhAssf ni aAhlrAiop;onTp rEiE pdapTxTdTEo cni knrEsp;cniExjg AsuHAaETp, Ap JiEEl, HEaiEr, Ago AizEgxAg, rEiE dpEo;EAhHsETTEi nc THE usAxgTEyT rAp iEusAhEo af THE ngE THAT cnssnrp xT; xg THE znpTAokAghEopfpTEz, puEhxAs pxjgp pdapTxTdTEo cni sETTEip. Cni AsznpT ATHndpAgo fEAip, cinz aEcniE 500Tn 1400, THE hifuTnsnjf nc REpTEighxkxsxmATxng pTAjgATEo

Next we have the “rHETHEi” word so I assume it’s wether, so **R → W and I → R.** Also I have THEf, which can be THEY, so **F → Y.** Another I have THEz. which can be THEM, so **Z → M.** Also I have Ass, which may be ALL, so **S → L.** Another what I have is Tn, which can be TO, so **N → O.**
Till now we have this:

UOLYaxdp Ago OTHERp gEkER pAxo WHETHER AgY Oc THE pdapTxTdTxOghxuHERp THEY oEphRxaEo WEREAhTdALLY dpEo, Ago pO THE cxRpT ATTEpTEo dpE OcTHAT jEgRE xg uOLxTxhAL AccAxRp hOME cROM THEROMAgp — Ago cROM THE jREATEpT ROMAg Oc THEM ALL. EdLxdpHAEpAR THdp xMuREppEo Hxp gAMEuERMAgEgTLY xgTO hRYuTOLOjY.XT MdpT aE THAT Ap pOOg Ap A hdLTdRE HAp REAhHEo A hERTAxgLEkEL,uROaAaLY MEApdREo LARjELY aY xTp LxTERAhY, hRYuTOjRAuHY AuuEARppuOgTAgEOdpLY — Ap xTpuAREgTp, LAgjdAjE Ago WRxTxgj, uROaAaLY ALpO oxo.THE MdLTxuLE HdMAg gEEop Ago oEpxREp THAT oEMAgouRxkAhY AMOgj TWOOR MORE uEOuLE xg THE MxopT Oc pOhxAL LxcE MdpT xgEkxTAaLY LEAo TOhRYuTOLOjYWHEREkER MEg THRxkE Ago WHEREkER THEY WRxTE. HdLTdRALoxccdpxOg pEEMp A LEpp LxlELY EyuLAgATxOgcOR xTp OhhdRREghE xg. pO MAgYAREAp, MAgY Oc THEM oxpTAgT Ago xpOLATEo.THE YEmxoxp, Ag OaphdREpEhT Oc AaOdT 25,000 uEOuLE xg, gORTHERg XRAb,dpE A hRYuTxh phRxuT xg THExR HOLY aOOlp aEhAdpETHEY cEAR uERpEhdTxOg aYTHExR MOpLEM gExjHaORp. TxaETAgp dpE A lxgo Oc hxuHER hALLEo "RxgpudgpcOR OccxhxAL hORREpuOgoEghE; xT xp gAMEo cOR xTp xgkEgTOR Rxg-h'(HHEg-)pudgp(-uA), WHOLxkEo xg THE 1300p. THE Gpxaxox pEhRET pOhxETY Oc GxjERxAlEEup xTp uxhTOjRAuHxh phRxuTcROM EdROuEAgp Ap MdhH Ap uOppxaLEaEhAdpE xT xp dpEo hHxEcLY TO EyuREpp LOkE xg RATHER oxREhTxMAjERY, AgopAMuLEp AuuEAR TO aE AT LEApT Ap uORgOjRAuHxh Ap THEY ARE hRYuTOjRAuHxh.THE hRYuTOjRAuHYOc THAxLAgo oEkELOuEo dgoER XgoxAg xgcLdEghE. AgEMaRYOgxh pTdoY Oc THE pdaeEhT EkEg AuuEARpxg A jRAMMATxhAL WORlEgTxTLEo UORAgAkAlYA aY HLdAgj URApOT AlpARAgxTx (UHE). OgE pYpTEM,hALLEo"THE ERRxgj PxAMEpE," pdapTxTdTEp OgE oELxhATE PxAMEpE LETTER cORAgOTHER. Xg AgOTHERpYpTEM, hOgpOgAgTp ARE oxkxoEo xgTO pEkEg jROdup Oc cxkE LETTERp;A LETTER xp xgoxhATEo aYWRxTxgj THE PxAMEpE gdMaER Oc xTp jROdu AgouLAhxgj kERTxhAL oOTp dgoER xT EbdAL xg gdMaER TOTHE LETTER'p uLAhE xg xTpjROdu. A pYpTEM hALLEo "THE HERMxT METAMORuHOpxgj LETTERp" WRxTEpTHETEyT aAhlWARop.Xg THE EdROuE Oc THE LATxg ALuHAaET—cROM WHxhH MOoERg hRYuTOLOjYWOdLopuRxgj—hRYuTOjRAuHY cLxhlEREo WEAlLY. WxTH THE hOLLAupE Oc THEROMAg EMuxRE, EdROuE HAo uLdgjEoxgTO THE OaphdRxTY Oc THE OARl AjEp.LxTERAhY HAo ALL adT oxpAuuEAREo. ARTp Ago phxEghEp WEREcORjOTTEg, AgohRYuTOjRAuHY WAp gOT EyhEuTEo. OgLY odRxgj THE MxooLE AjEpOhhApxOgALMAgdphRxuTp, WxTH Ag xgcREbdEgT pxjgATdRE OR jLOpp OR "oEO jRATxAp" THAT AaOREo MOgludT xgTO hxuHER TO AMdpE HxMpELc, cxTcdLLY xLLdMxgATE THEhRYuTOLOjxh oARlgEpp, Ago, LxlE ApxgjLE hAgoLE jdTTERxgj xg A jREATMEoxEkAL HALL, THExR cEEaLE cLARxgjp OgLY EMuHApxmE THEjLOOM.THE pYpTEMp dpEo WERE pxMuLE xg THE EyTREME. UHRApEp WERE WRxTTEgkERTxhALLY OR aAhlWARop;oOTp WERE pdapTxTdTEo cOR kOWELp;cORExjg ALuHAaETp, Ap JREEl, HEaREW, Ago ARMEgxAg, WERE dpEo;EAhHLETTER Oc THE uLAxgTEyT WAp REuLAhEo aY THE OgE THAT cOLLOWp xT; xg THE MOpTAokAghEopYpTEM, puEhxAL pxjgp pdapTxTdTEo cOR LETTERp. COR ALMOpT ATHOdpAgo YEARp, cROM aEcORE 500TO 1400, THE hRYuTOLOjY Oc WEpTERghxkxLxmATxOg pTAjgATEo

Now above I have the word “OTHERp” so I conclude it must be “OTHERS” so **P → S**. Also I have the word “gEkER ” so it could be “NEVER”, so **G → N and K → V.** “xT” may be “IT”, so **X → I.** “REAhHEo” may be ”REACHED”, so **H → C and O → D.** “WEAlLY” may be “WEAKLY”, so **L → K**

After we apply it:

UOLYaIdS AND OTHERS NEVER SAID WHETHER ANY Oc THE SdaSTITdTIONCIuHERS THEY DESCRIaED WEREACTdALLY dSED, AND SO THE cIRST ATTESTED dSE OcTHAT jENRE IN uOLITICAL AccAIRS COME cROM THEROMANS — AND cROM THE jREATEST ROMAN Oc THEM ALL. EdLIdSCAESAR THdS IMuRESSED HIS NAMEuERMANENTLY INTO CRYuTOLOjY.IT MdST aE THAT AS SOON AS A CdLTdRE HAS REACHED A CERTAINLEVEL,uROaAaLY MEASdRED LARjELY aY ITS LITERACY, CRYuTOjRAuHY AuuEARSSuONTANEOdSLY — AS ITSuARENTS, LANjdAjE AND WRITINj, uROaAaLY ALSO DID.THE MdLTIuLE HdMAN NEEDS AND DESIRES THAT DEMANDuRIVACY AMONj TWOOR MORE uEOuLE IN THE MIDST Oc SOCIAL LIcE MdST INEVITAaLY LEAD TOCRYuTOLOjYWHEREVER MEN THRIVE AND WHEREVER THEY WRITE. CdLTdRALDIccdSION SEEMS A LESS LIKELY EyuLANATIONcOR ITS OCCdRRENCE IN. SO MANYAREAS, MANY Oc THEM DISTANT AND ISOLATED.THE YEmIDIS, AN OaSCdRESECT Oc AaOdT 25,000 uEOuLE IN, NORTHERN IRAb,dSE A CRYuTIC SCRIuT IN THEIR HOLY aOOKS aECAdSETHEY cEAR uERSECdTION aYTHEIR MOSLEM NEIjHaORS. TIaETANS dSE A KIND Oc CIuHER CALLED "RINSudNS"cOR OccICIAL CORRESuONDENCE; IT IS NAMED cOR ITS INVENTOR RIN-C'(HHEN-)SudNS(-uA), WHOLIVED IN THE 1300S. THE NSIaIDI SECRET SOCIETY Oc NIjERIAKEEuS ITS uICTOjRAuHIC SCRIuTcROM EdROuEANS AS MdCH AS uOSSIaLEaECAdSE IT IS dSED CHIEcLY TO EyuRESS LOVE IN RATHER DIRECTIMAjERY, ANDSAMuLES AuuEAR TO aE AT LEAST AS uORNOjRAuHIC AS THEY ARE CRYuTOjRAuHIC.THE CRYuTOjRAuHYOc THAILAND DEVELOuED dNDER INDIAN INcLdENCE. ANEMaRYONIC STdDY Oc THE SdaeECT EVEN AuuEARSIN A jRAMMATICAL WORKENTITLED UORANAVAKYA aY HLdANj URASOT AKSARANITI (UHE). ONE SYSTEM,CALLED"THE ERRINj SIAMESE," SdaSTITdTES ONE DELICATE SIAMESE LETTER cORANOTHER. IN ANOTHERSYSTEM, CONSONANTS ARE DIVIDED INTO SEVEN jROduS Oc cIVE LETTERS;A LETTER IS INDICATED aYWRITINj THE SIAMESE NdMaER Oc ITS jROdu ANDuLACINj VERTICAL DOTS dNDER IT EbdAL IN NdMaER TOTHE LETTER'S uLACE IN ITSjROdu. A SYSTEM CALLED "THE HERMIT METAMORuHOSINj LETTERS" WRITESTHETEyT aACKWARDS.IN THE EdROuE Oc THE LATIN ALuHAaET—cROM WHICH MODERN CRYuTOLOjYWOdLDSuRINj—CRYuTOjRAuHY cLICKERED WEAKLY. WITH THE COLLAuSE Oc THEROMAN EMuIRE, EdROuE HAD uLdNjEDINTO THE OaSCdRITY Oc THE DARK AjES.LITERACY HAD ALL adT DISAuuEARED. ARTS AND SCIENCES WEREcORjOTTEN, ANDCRYuTOjRAuHY WAS NOT EyCEuTED. ONLY DdRINj THE MIDDLE AjESOCCASIONALMANdSCRIuTS, WITH AN INcREbdENT SIjNATdRE OR jLOSS OR "DEO jRATIAS" THAT AaORED MONKudT INTO CIuHER TO AMdSE HIMSELc, cITcdLLY ILLdMINATE THECRYuTOLOjIC DARKNESS, AND, LIKE ASINjLE CANDLE jdTTERINj IN A jREATMEDIEVAL HALL,

THEIR cEEaLE cLARINjS ONLY EMuHASImE THEjLOOM.THE SYSTEMS dSED WERE SIMuLE IN THE EyTREME. UHRASES WERE WRITTENVERTICALLY OR aACKWARDS;DOTS WERE SdaSTITdTED cOR VOWELS;cOREIjN ALuHAaETS, AS JREEK, HEaREW, AND ARMENIAN, WERE dSED;EACHLETTER Oc THE uLAINTEyT WAS REuLACED aY THE ONE THAT cOLLOWS IT; IN THE MOSTADVANCEDSYSTEM, SuECIAL SIjNS SdaSTITdTED cOR LETTERS. COR ALMOST ATHOdSAND YEARS, cROM aEcORE 500TO 1400, THE CRYuTOLOjY Oc WESTERNCIVILImATION STAjNATED

After we apply it we see the 'Oc' appearance could be "on" or 'of' since 'n' we already have it must be of. So **C → F.** Also I have the "DESCRIaED" so the best word for it is "DESCRIBED", so **A → B.** "dSE" can be "USE", so **D → U.** "CRYuTOLOjY" may be "CRYPTOLOGY", so **U → P and J → G. "**CIVILImATION" may be "CIVILIZATION", so **M → Z.** "EyuRESS" may be "EXPRESS", so **Y → X.** "EbdAL" may be "EQUAL", so **B → Q.**

POLYBIUS AND OTHERS NEVER SAID WHETHER ANY OF THE SUBSTITUTIONCIPHERS THEY DESCRIBED WEREACTUALLY USED, AND SO THE FIRST ATTESTED USE OFTHAT GENRE IN POLITICAL AFFAIRS COME FROM THEROMANS — AND FROM THE GREATEST ROMAN OF THEM ALL. EULIUSCAESAR THUS IMPRESSED HIS NAMEPERMANENTLY INTO CRYPTOLOGY.IT MUST BE THAT AS SOON AS A CULTURE HAS REACHED A CERTAINLEVEL,PROBABLY MEASURED LARGELY BY ITS LITERACY, CRYPTOGRAPHY APPEARSSPONTANEOUSLY — AS ITSPARENTS, LANGUAGE AND WRITING, PROBABLY ALSO DID.THE MULTIPLE HUMAN NEEDS AND DESIRES THAT DEMANDPRIVACY AMONG TWOOR MORE PEOPLE IN THE MIDST OF SOCIAL LIFE MUST INEVITABLY LEAD TOCRYPTOLOGYWHEREVER MEN THRIVE AND WHEREVER THEY WRITE. CULTURALDIFFUSION SEEMS A LESS LIKELY EXPLANATIONFOR ITS OCCURRENCE IN. SO MANYAREAS, MANY OF THEM DISTANT AND ISOLATED.THE YEZIDIS, AN OBSCURESECT OF ABOUT 25,000 PEOPLE IN, NORTHERN IRAQ,USE A CRYPTIC SCRIPT IN THEIR HOLY BOOKS BECAUSETHEY FEAR PERSECUTION BYTHEIR MOSLEM NEIGHBORS. TIBETANS USE A KIND OF CIPHER CALLED "RINSPUNS"FOR OFFICIAL CORRESPONDENCE; IT IS NAMED FOR ITS INVENTOR RIN-C'(HHEN-)SPUNS(-PA), WHOLIVED IN THE 1300S. THE NSIBIDI SECRET SOCIETY OF NIGERIAKEEPS ITS PICTOGRAPHIC SCRIPTFROM EUROPEANS AS MUCH AS POSSIBLEBECAUSE IT IS USED CHIEFLY TO EXPRESS LOVE IN RATHER DIRECTIMAGERY, ANDSAMPLES APPEAR TO BE AT LEAST AS PORNOGRAPHIC AS THEY ARE CRYPTOGRAPHIC.THE CRYPTOGRAPHYOF THAILAND DEVELOPED UNDER INDIAN INFLUENCE. ANEMBRYONIC STUDY OF THE SUBeECT EVEN APPEARSIN A GRAMMATICAL WORKENTITLED PORANAVAKYA BY HLUANG PRASOT AKSARANITI (PHE). ONE SYSTEM,CALLED"THE ERRING SIAMESE," SUBSTITUTES ONE DELICATE SIAMESE LETTER FORANOTHER. IN ANOTHERSYSTEM, CONSONANTS ARE DIVIDED INTO SEVEN GROUPS OF FIVE LETTERS;A LETTER IS INDICATED BYWRITING THE SIAMESE NUMBER OF ITS GROUP ANDPLACING VERTICAL DOTS UNDER IT EQUAL IN NUMBER TOTHE LETTER'S PLACE IN

ITSGROUP. A SYSTEM CALLED "THE HERMIT METAMORPHOSING LETTERS" WRITESTHETEXT BACKWARDS.IN THE EUROPE OF THE LATIN ALPHABET—FROM WHICH MODERN CRYPTOLOGYWOULDSPRING—CRYPTOGRAPHY FLICKERED WEAKLY. WITH THE COLLAPSE OF THEROMAN EMPIRE, EUROPE HAD PLUNGEDINTO THE OBSCURITY OF THE DARK AGES.LITERACY HAD ALL BUT DISAPPEARED. ARTS AND SCIENCES WEREFORGOTTEN, ANDCRYPTOGRAPHY WAS NOT EXCEPTED. ONLY DURING THE MIDDLE AGESOCCASIONALMANUSCRIPTS, WITH AN INFREQUENT SIGNATURE OR GLOSS OR "DEO GRATIAS" THAT ABORED MONKPUT INTO CIPHER TO AMUSE HIMSELF, FITFULLY ILLUMINATE THECRYPTOLOGIC DARKNESS, AND, LIKE ASINGLE CANDLE GUTTERING IN A GREATMEDIEVAL HALL, THEIR FEEBLE FLARINGS ONLY EMPHASIZE THEGLOOM.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 MOSTADVANCEDSYSTEM, SPECIAL SIGNS SUBSTITUTED FOR LETTERS. FOR ALMOST ATHOUSAND YEARS, FROM BEFORE 500TO 1400, THE CRYPTOLOGY OF WESTERNCIVILIZATION STAGNATED.