



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, Iordan Liviu

Checked:

asist. univ. Nirca Dumitru,

Chişinău 2023

## **Topic: Mono-alphabetic Cipher**

### **Tasks:**

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 is assumed to be a text written in English. Bear in mind that only letters, the other characters remain unencrypted.

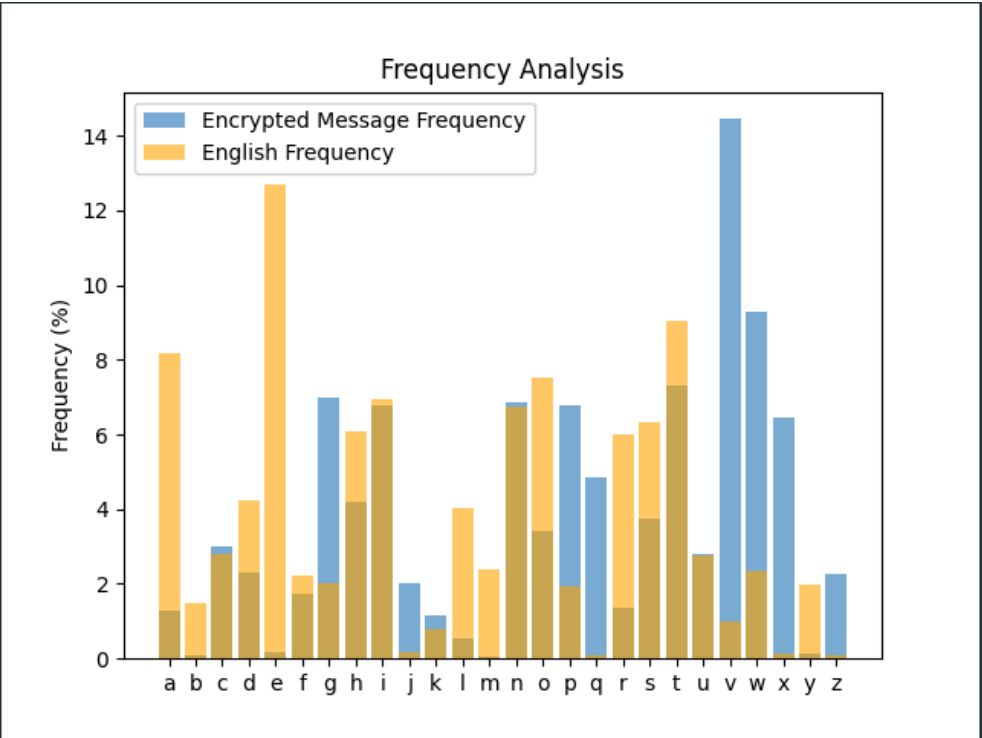
### **Theoretical notes:**

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.

### **Implementation(Var. Nr.14)**

Before explaining the process of obtaining the decrypted text, these are the data I have got from analyzing my cryptogram:



**Fig 3.** English letter frequency and encrypted message frequency according to my version of the code.

	Letter (Message)	ssage Frequency i	Letter (English)	glish Frequency ('
1	v	14.451	e	12.702
2	w	9.279	t	9.056
3	t	7.304	a	8.167
4	g	6.991	o	7.507
5	n	6.865	i	6.966
6	p	6.803	n	6.749
7	i	6.771	s	6.327

8	x	6.458	h	6.094
9	q	4.859	r	5.987
10	h	4.201	d	4.253
11	s	3.762	l	4.025
12	o	3.417	c	2.782
13	c	3.009	u	2.758
14	u	2.790	m	2.406
15	d	2.288	w	2.360
16	z	2.257	f	2.228
17	j	2.038	g	2.015
18	f	1.724	y	1.974
19	r	1.348	p	1.929
20	a	1.285	b	1.492
21	k	1.160	v	0.978
22	l	0.533	k	0.772
23	e	0.157	j	0.153
24	y	0.125	x	0.150
25	b	0.094	q	0.095
26	m	0.031	z	0.074

**Fig 2.** The sorted frequency table of the letters

1	a	b	8	h	c
2	b	q	9	i	r
3	c	f	10	j	g
4	d	u	11	k	v
5	e	j	12	l	k
6	f	y	13	m	z
7	g	n	14	n	o
15	o	d	21	u	p
16	p	s	22	v	e
17	q	h	23	w	t
18	r	h	24	x	i
19	s	l	25	y	x
20	t	a	26	z	m
21	u	p			

**Fig 3.** The substitution Letter mappings

**I have a cryptogram c** = *Pvhivw Nccxhv tgo wqvxi onzvpwxh ngvp cinz wqv Uixktwv - Nccxhv, anwqpdaoxkxpxngp nc wqv Unpw Nccxhv. Wqv Pvhivw Nccxhv rtp bdtiwvivo xg wqivvinnzp toenxgxgj wqv Cnivxjg Nccxhv tgo vgwvivo uixktwvsf cinz TahqdiqStgv. Cxiv tgo htgosvp adigvo hngpwtgwsf xg ngv innz; wqv pwtcc snojvo xgwqv nwqvip. Xw xghsdovo zvg rqn ztov wqvxi sxcv'p rnil wqv puvhxtswf ncdgpvtsxgj oxusnztwxh uthlvwp rxwq pdhq, ovcwgvpw wqtw wqv hndso avivpvtso rxwqndw vkxovghv nc wtzuvi xgj; ngv pdhq nuvgvi rtp E. V. Anov,ctwqvi nc Enqg Anov, Ei. Qv ivjdstisf puvgw wqivv qndip ng wqv oxputwhqvpnc wqv Lxgj nc Uidppxt, nuvgxgj wqvz tgo wqvg iv-pvtsxgj wqvz rxwqpuvhxts rty tgo htivcdssf hndgwvicvxwvo pvtsp. Uviqtup pdiui xpxgjsf xg tatpwxng nc qdztg ixjqwp, xwp xgwvihvuwxngp vgenfvo cdss svjtsxwf. Wqvpwtwdwv nc 1657 wqtw vpwtasxpqvo wqv unpwts pvikxhv ovhstivo ndwixjqw wqtw wqv ztxsp rviv wqv avpw zvtgp nc oxphnkvi xgj otgjvindp tgo rxhlvoovpxjgp tjtxgpw wqv hnzzngrvtswq. Svtpvp nc 1660 tgo 1663, hngcxizvoaf wqv Unpw Nccxhv Thw nc 1711, uvizxwwvo jnkvigzvgw nccxhtsp wn nuvgztxs dgovi rtiitgwp wqtw wqv wqvzpvskvp xppdvo.*

Wqvf pxovpwvuvo wqspanwqvipnzv uinhvodiv af uinzdsjtwxgj tss-xghsdpxkv  
jvgvits rtiitgwp.\*Wqv Pvhivw Nccxhv pvgw xgwvihvuwxngp vg hstxi wn wqv lxxgj  
tgo wqnpv xghxuqvi wn wqv hifuwtgtsfwp.Wqvf rviv lgnrg hnssvhwxkvsf tp wqv  
Ovhfuqvixgj Aitghq. Dgsxlv wqvPvhivw Nccxhv, wqv aitghq qto gn puvhxcxh  
snhtwxng. Xwp wxgf pwtcc nc vyuviwprnilvo stijvsf tw qnzv, ivhvxxkgj wqvxi  
ztwvixts af puvhxts zvppvgjvi.Gni qto xw tgf cnizts nijtgxmtwxng, wqv pvgxni  
Ovhfuqvivi avxgj zvivsfcxipw tzngj vbdtsf. Zniv pvhivw wqtg wqv Pvhivw Nccxhv,  
wqv aitghq'pcdgop htzv cinz pvhivw-pvikxhv zngvf xppdvo wn wqv Pvhivwtif nc  
wqv UnpwNccxhv cinz Utisxtzvgw'p pdiusdp ivkvgdv. Pvhdxwf rtp wxjqw—xg tss  
ncVgjstgo uinatasf ngsf 30 uvnusv lgyr rqtw oxusnztwxh hniivpungovghvrtf avxgj  
ivto tw tgf jxkvg znzvgw. Gvkviwqvsvpp, znpw zvg nc tcctxiopriv trtiv nc wqv  
uithwxhv nc nuvgxgj\*Wqxp thwxkxwf cnizp wqv svjts uivhvovgw cni wqv znovig  
wtuuxgj ncwvsvuqngvp, tw svtpw xg Aixwtxg. Pxjgxcxhtgwsf, qnrvkvi, wqv pndihv  
nc wqvunrvi wn xgwvihvuwx hnzdzgxtwxngp qtp gvkvi avvg ovwvizxgvo. WqvHinrg  
pxzusf vyvihxpvo xw tgo, ovpuwxv nhhtpxngts ovatwv, qtp hngwxgdown on pn,  
uivpdztasf rxwq wqv wthxw tuuinkts nc wqv udasxh tp gvhvpttifeni wqv ptcvxf nc  
wqv pwtwv.uixktwv svwwvip, tgo wqv ncwvg vghxuqvivo wqvxi hniivpungovghv  
nivgwidpwvo xw wn uixktwv zvppvgjvip rvg pvhivhf rtp vppvgwxts.Tcwvi wqv  
Vsvhwni nc Qtgnkvi pdhhvvovo wn wqv Vgjsxpq wqingv tpJvnijv X xg 1714,  
ivwtxgxgj wqv idsv nc wqv Jvitzg pwtwv, wqv OvhfuqvixgjAitghq hnsstanitwvo  
rxwq wqv asthl hqtzavi ztxgwtxgvo tw Gxvgadij afwqv Qtgnkvixtg jnkvigzvgw.  
Hifuwtgtsfwp Anov, Stzuv, tgo Gvdandijqto vkvg avvg xzuniwvo cinz wqviv—tg  
xingxh ovkvsnuzvgw xg kxvr nc tivcdpts nc Rtssxp wn oxkdsjv qxp wvhqgxbdv wn  
Qtgnkvi t cvr fvtip vtisxvi.Ztxs nuvgxgj avhtzv qtaxwds. Jvnijv tgo qxp pdhhvppnip  
wnnl thngpwtgw uvipngts xgwviwpw xg wqv rnil, ncwvg vghnditjxgj wtsvgw  
rxwqinfst andgw. Hniivpungovghv rtp hsnpsf rtwhqvo cni hixap wqtw rvivutppvo  
wn wqv Ovhfuqvixgj Aitghq.Odixgj wqv 1700p, wqv aitghq'p ndwudw tkvitjvo wrn  
ni wqivvoxputwhqvp t rvvl, tgo pnzvwxyzp ngv t of. Xwp hifuwtgtsfwp pnsko  
wqvoxputwhqvp nc Citghv, Tdpwixt, Ptyngf tgo nwqvi Jvitzg pwtwvp,  
Unstgo,Putxg, Uniwdjts, Qnsstgo, Ovgztal, Prvovg, Ptioxgxt, Gtusvp tgo  
nwqviXwtsxtg pwtwvp, Jivvhv, Wdilyf, Idppxt, tgo, stwvi, wqv Dgxwvo Pwtwvp.  
Wqvivhnio nc Civghq xgwvihvuwxngp hnkvip wrn hvgwdixvp tgo hnzuixpvp  
cxkvknsdzvp nc xgwvihvuwp wnwtsexgj 2,020 utjvp usdp wqivv knsdzvp nc  
lvfp.Uviqtup zniv wfluxts xp wqv Putgxpq onppxvi—wqivv knsdzvp nc  
xgwvihvuwpzin 1719 wn 1839 wnwtsexgj 872 utjvp. Gnw tss nc wqv zvptjvp

*rvivpnskvo tw wqv wxzv nc wqvxi xgwvihvuwxng. Ztgf rviv qvso vxwqvi dgwxsvgndjq qto thhdzdstwvo cni t pdhhvppcds twwthl ni dgwx s t gvvo tinpv cniwqvxi pnsdwxng.*

First we take a look at the frequencies for the letters in the tables:

	Letter (Message)	Message Frequency (%)	Letter (English)	English Frequency (%)
1	v	14.451	e	12.702
2	w	9.279	t	9.056
3	t	7.304	a	8.167
4	g	6.991	o	7.507
5	n	6.865	i	6.966
6	p	6.803	n	6.749
7	i	6.771	s	6.327

We see that the first three letters v, w, and t have similar appearance as e, t, and a in the english alphabet, therefore we substitute these letters:  $v \rightarrow e$ ,  $w \rightarrow t$ , and  $t \rightarrow a$ . So our text looks the following way:

*pEhiET nccxE Ago TqExi onzEpTxh ngEp cinz TqE uixkATE - nccxE, anTqpdaoxkxpxngp nc TqE unpT nccxE. TqE pEhiET nccxE rAp bdAiTEiEo xg TqiEEinnzp Aoengxgj TqE cniExgj nccxE Ago EgTEiEo uixkATESf cinz AahqdihqsAgE. cxiE Ago hAgosEp adigEo hngpTAgTsf xg ngE innz; TqE pTAcc snojEo xgTqE nTqEip. xT xghsdoEo zEg rqn zAoE TqExi sxE'p rnil TqE puEhxAsTf ncdgpEAsxgj oxusnzATxh uAhLEtp rxTq pdhq, oEcTgEpp TqAT TqEf hndso aEiEpEAsEo rxTqndT EkxoEghE nc TAzEixgj; ngE pdhq nuEgEi rAp e. E. anoE,cATqEi nc enqg anoE, ei. qE iEjdsAisf puEgT TqiEE qndip ng TqE oxpuATHqEpnc TqE lxgj nc uidppxA, nuEgxgj TqEz Ago TqEg iE-pEAsxgj TqEz rxTqpuEhxAs rAy Ago hAiEcdssf hndgTEicExTEo pEAsp. uEiqAup pdiuxpxgjsf xg AaApTxng nc qdzAg ixjqTp, xTp xgTEihEuTxngp EgenfEo cdss sEjAsxTf. TqEpTATdTE nc 1657 TqAT EpTAasxpqEo TqE unpTAs pEikxE oEhsAiEo ndTixjqT TqATTqE zAxsp rEiE TqE aEpT zEAgp nc oxphnkEixgj oAgjEindp Ago rxhlEooEpjgp AjAxgpT TqE hnzzngrEAsTq. sEApEp nc 1660 Ago 1663, hngcxizEoaf TqE unpT nccxE AhT nc 1711, uEizxTTEo jnkEigzEgT nccxhXasp Tn nuEgzAxs dgoEi rAiiAgTp TqAT TqEf TqEzpEskEp xppdEo. TqEf pxoEpTEuuEo TqxpantqEipnzE uinhEodiE af uinzdsjATxgj Ass-xghsdpxkE jEgEiAs rAiiAgTp.\*TqE pEhiET nccxE pEgT xgTEihEuTxngp Eg hsAxI Tn TqE lxgj Ago TqnpE xghxuqEi Tn TqE hifuTAGAsfpTp.TqEf rEiE Ignrg hnssEhTxkEsf Ap TqE oEhfuqEixgj aiAghq. dgsxE TqEpEhiET nccxE, TqE aiAghq qAo gn puEhxcxh snhATxng. xTp Txgf pTAcc nc EyuEiTpnilEo sAijEsf AT qnzE, iEhExkxgj TqExi zATEixAs af puEhxAs zEppEgjEi.gni qAo xT Agf cnizAs nijAgxmATxng, TqE pEgxni oEhfuqEiEi aExgj zEiEsfcxipT Azngj EbdAsp. zniE pEhiET TqAg TqE pEhiET nccxE, TqE aiAghq'pcdgop hAzE cinz pEhiET-pEikxE zngEf xppdEo Tn TqE pEhiETAif nc TqE unpTnccxE cinz uAisxAzEgT'p pdiusdp iEkEgdE. pEhdixTf rAp TxjqT—xg Ass ncEgjsAgo uinaAasf ngf 30 uEnusE IgEr rqAT oxusnzATxh*

hniiEpungoEghErAp aExgj iEAo AT Agf jxkEg znzEgT. gEkEiTqEsEpp, znpT zEg nc AccAxiprEiE ArAiE nc TqE uiAhTxhE nc nuEgxgj\*Tqxp AhTxkxTf cnizp TqE sEjAs uiEhEoEgT cni TqE znoEig TAUuxgj nCTEsEuqngEp, AT sEApT xg aixTAXg. pxjgxcxhAgTsf, qnrEkEi, TqE pndihE nc TqEunrEi Tn xgTEihEuT hnzzdgxhATxngp qAp gEkEi aEEg oETEizxgEo. TqEhinrg pxzusf EyEihxpEo xT Ago, oEpuxTE nhhApxngAs oEaATE, qAp hngTxgdEoTn on pn, uiEpdzAasf rxTq TqE TAhxT AuuinkAs nc TqE udasxh Ap gEhEppAifcni TqE pAcETf nc TqE pTATE. uixkATE sETTEip, Ago TqEf nCTEg EghxuqEiEo TqExi hniiEpungoEghE niEgTidpTEo xT Tn uixkATE zEppEgjEip rqEg pEhiEhf rAp EppEgTxAs. AcTEi TqE EsEhTni nc qAgnkEi pdhhEEoEo Tn TqE Egjsxpq TqingE ApjEnijE x xg 1714, iETAxgxgj TqE idsE nc TqE jEizAg pTATE, TqE oEhfuqEixgjaiAghq hnssAaniATEo rxTq TqE asAhl hqAzaEi zAxgTAXgEo AT gxEgadij afTqE qAgnkEixAg jnkEigzEgT. hifuTAgAsfpTp anoE, sAzUE, Ago gEdandijqAo EkEg aEEg xzuniTEo cinz TqEiE—Ag xingxh oEkEsnuzEgT xg kxEr nc AiEcdpAs nc rAssxp Tn oxkdsjE qxp TEhqqxbdE Tn qAgnkEi A cEr fEAip EAisxEi. zAxs nuEgxgj aEhAzE qAaxTdAs. jEnijE Ago qxp pdhhEppnip Tnnl AhngpTAGT uEipngAs xgTEiEpT xg TqE rnil, nCTEg EghndiAjxgj TAsEgT rxTqinfAs andgTf. hniiEpungoEghE rAp hsnpEsf rATHqEo cni hixap TqAT rEiEuAppEo Tn TqE oEhfuqEixgj aiAghq. odixgj TqE 1700p, TqE aiAghq'p ndTudT AkEiAjEo Trn ni TqiEEoxpuATHqEp A rEEI, Ago pnzETxzEp ngE A oAf. xTp hifuTAgAsfpTp pnskEo TqEoxpuATHqEp nc ciAghE, AdpTixA, pAyngf Ago nTqEi jEizAg pTATEp, unsAgo, puAxp, uniTdjAs, qnssAgo, oEgzAil, prEoEg, pAioxgxA, gAusEp Ago nTqEixTAsxAg pTATEp, jiEEhE, TdilEf, idppxA, Ago, sATEi, TqE dgxTEo pTATEp. TqEiEhnio nc ciEghq xgTEihEuTxngp hnkEip Trn hEgTdixEp Ago hnzuixpEp cxEknsdzEp nc xgTEihEuTp TnTAsxgj 2,020 uAjEp usdp TqiEE knsdzEp nc lEfp. uEiqAup zniE TfuxhAs xp TqE puAgxpq onppxEi—TqiEE knsdzEp nc xgTEihEuTpcinz 1719 Tn 1839 TnTAsxgj 872 uAjEp. gnT Ass nc TqE zEppAjEp rEiEpnskEo AT TqE TxzE nc TqExi xgTEihEuTxng. zAgf rEiE qEso ExTqEi dgTxsEgndjq qAo AhhdzdsATEo cni A pdhhEppcds ATTAhl ni dgTxs A gEEo AinpE cniTqExi pnsdTxng.

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 now “THExi” since the only words that can follow are “there” and “their”, and since “there” cannot be, the word is “their”, therefore x -> i, i -> r. So, we have the following text:

pEhRET ncclhE Ago THEIR onzEpTih ngEp cRnz THE uRIkATE - ncclhE, anTHpdaolkplngp nc THE unpT ncclhE. THE pEhRET ncclhE rAp bdARTEREO Ig THREERnnzp Aoenlgjg THE cnREljg ncclhE Ago EgTEREO uRIkATESf cRnz AahHdRhHsAgE. cIRE Ago hAgosEp adRgEo hngpTAGTsf Ig ngE Rnnz; THE pTAcc snojEo IgTHE nTHERp. IT lghsdoEo zEg rHn zAoE THEIR slcE'p mRI THE puEhIAsTf ncdgpEAslgj olusnzATih uAhIETp rITH pdhH, oEcTgEpp THAT THEf hndso aEREPEAsEo rITHndT EkloEghE nc TAzUERlgj; ngE pdhH nuEgER rAp e. E. anoE, cATHER nc enHg anoE, eR. HE REjdsARsf puEgT THREE HndRp ng THE olpuATHHEpnc THE llgj nc uRdpplA, nuEglgj THEz Ago THEg RE-pEAslgj THEz rITHpuEhIAs rAy Ago hAREcdssf hndgTERcEITEo pEAsp. uERHAup pdRuRlplgjsf Ig AaApTIng nc HdzAg RIjHTp, ITp IgTERhEuTIngp EgenfEo cdss sEjAsITf. THEpTATdTE nc 1657 THAT



EpTAaslpHEo THE unpTAs pERklhE oEhsAREo ndTRljHT THATTHE zAlsp rERE THE aEpT  
zEAgp nc olphnkERlgj oAgjERndp Ago rhlEooEpljgp AjAlgpT THE hnzzngrEAsTH. sEApEp nc  
1660 Ago 1663, hngclRzEoaf THE unpT ncclhE AhT nc 1711, uERzITTEo jnkERgzEgT  
ncclhIAsp Tn nuEgzAls dgoER rARRAgTp THAT THEf THEzpEskEp lppdEo. THEf  
ploEpTEuuEo THlpanTHERpnzE uRnhEodRE af uRnzdsjATlgj Ass-lghsdplkE jEGERAs  
rARRAgTp.\*THE pEhRET ncclhE pEgT lgTERhEuTIngp Eg hsAIR Tn THE llgj Ago THnpE  
lghluHER Tn THE hRfuTAGAsfpTp.THEf rERE lgnrg hnssEhTlKEsf Ap THE oEhfuHERlgj  
aRAghH. dgsllE THEpEhRET ncclhE, THE aRAghH HAo gn puEhlclh snhATIng. ITp Tlgf pTAcc  
nc EyuERTprnRIEo sARJEsf AT HnzE, REhElklgj THEIR zATERIAs af puEhIAs zEppEgJER.gnR  
HAo IT Agf cnRzAs nRjAgImATIng, THE pEglnR oEhfuHERER aElgj zERESfclRpT Azngj  
EbdAsp. znRE pEhRET THAg THE pEhRET ncclhE, THE aRAghH'pcdgop hAzE cRnz  
pEhRET-pERklhE zngEf lppdEo Tn THE pEhRETARf nc THE unpTncclhE cRnz uARslAzEgT'p  
pdRusdp REkEgdE. pEhdRITf rAp TljHT—lg Ass ncEgjsAgo uRnaAasf ngsf 30 uEnusE lgEr  
rHAT olusnzATlh hnRREPungoEghErAp aElgj REAo AT Agf jlkEg znzEgT. gEkERTHEsEpp,  
znpt zEg nc AccAIRprERE ArARE nc THE uRAhTIhE nc nuEglgj\*THlp AhTlKITf cnRzp THE  
sEjAs uREhEoEgT cnR THE znoERg TAuulgj ncTEsEuHngEp, AT sEApT lg aRITAlg.  
pljglclhAgTsf, HnrEKER, THE pndRhE nc THEunrER Tn lgTERhEuT hnzzdglhATIngp HAp  
gEkER aEEg oETERzlgEo. THEhRnrg plzusf EyERhlpEo IT Ago, oEpulTE nhhApIngAs  
oEaATE, HAp hngTlgdEoTn on pn, uREpdzAasf rITH THE TAhIT AuuRnkAs nc THE udaslh Ap  
gEhEppARfcnr THE pAcETf nc THE pTATE.uRIkATE sETTERp, Ago THEf ncTEg  
EghluHEREo THEIR hnRREPungoEghE nREgTRdpTEo IT Tn uRIkATE zEppEgJERp rHEg  
pEhREhf rAp EppEgTlAs.AcTER THE EsEhTnR nc HAgnKER pdhhEEoEo Tn THE EgjslpH  
THRngE ApjEnRjE I lg 1714, RETAlglgj THE RdsE nc THE jERzAg pTATE, THE  
oEhfuHERlgjaRAghH hnssAanRATEo rITH THE asAhI hHAzaER zAlgTAlgEo AT glEgadRj  
afTHE HAgnKERIAG jnkERgzEgT. hRfuTAGAsfpTp anoE, sAzUE, Ago gEdandRjHAo EkEg  
aEEg lzunRTEo cRnz THERE—Ag lRnglh oEkEsnuzEgT lg klEr nc AREcdpAs nc rAsslp Tn  
olkdsjE Hlp TEhHglbdE Tn HAgnKER A cEr fEARp EARslER.zAls nuEglgj aEhAzE HAalTdAs.  
jEnRjE Ago Hlp pdhhEppnRp Tnnl AhngpTAGT uERpngAs lgTEREpT lg THE rnRI, ncTEg  
EghndRAJlgj TAsEgT rITHRnfAs andgTf. hnRREPungoEghE rAp hsnpEsf rATHHEo cnR hRIap  
THAT rEREuAppEo Tn THE oEhfuHERlgj aRAghH.odRlgj THE 1700p, THE aRAghH'p ndTudT  
AkERAjEo Trn nR THREEolpuATHHEp A rEEI, Ago pnzETlZEp ngE A oAf. ITp hRfuTAGAsfpTp  
pnskEo THEolpuATHHEp nc cRAghE, AdpTRIA, pAyngf Ago nTHER jERzAg pTATEp,  
unsAgo,puAlg, unRTdjAs, HnssAgo, oEgzARI, prEoEg, pARolglA, gAusEp Ago nTHERITAsIAG  
pTATEp, jREEhE, TdRIEf, RdppIA, Ago, sATER, THE dglTEo pTATEp. THEREhnRo nc  
cREghH lgTERhEuTIngp hnkERp Trn hEgTdRIEp Ago hnzuRlpEp clkEknsdzEp nc  
lgTERhEuTp TnTAslgj 2,020 uAjEp usdp THREE knsdzEp nc lEfp.uERHAup znRE TfulhAs lp  
THE puAgIpH onpplER—THREE knsdzEp nc lgTERhEuTpcRnz 1719 Tn 1839 TnTAslgj 872  
uAjEp. gnT Ass nc THE zEppAjEp rEREpnskEo AT THE TlZE nc THEIR lgTERhEuTIng. zAgf  
rERE HEso EITHER dgTIsEgndjH HAo AhhdzdsATEo cnR A pdhhEppcds ATTAhI nR dgTIs A  
gEEo ARnpE cnRTHEIR pnsdTIng.

So I have many appearances of the “ITp” since the word “its” is very used in English alphabet I conclude that p -> s, and “THE SEhRET” which has to be the word “The secret”, therefore h -> c, and finally for this part the word “RijHTS” has to be the english word “rights”, so we conclude j -> g. So, the text now looks the following:

SECRET ncclCE Ago THEIR onzESTIC ngES cRnz THE uRIkATE - ncclCE,  
anTHSdaolkISIngS nc THE unST ncclCE. THE SECRET ncclCE rAS bdARTEREO Ig  
THREERnnzS AoenlgIgG THE cnREIGg ncclCE Ago EgTEREO uRIkATEsf cRnz  
AaCHdRCHsAgE. clRE Ago CAgosES adRgEO CngSTAgTsf Ig ngE Rnnz; THE STAcc snoGEO  
IgTHE nTHERS. IT IgCsdoEO zEg rHn zAoE THEIR slcE'S rnRI THE SuECIASf ncdgSEAslgG  
olusnzATIC uACIETS rITH SdCH, oEcTgESS THAT THEf Cndso aERESEAsEO rITHndT  
EkloEgCE nc TAzUERlgG; ngE SdCH nuEgER rAS e. E. anoE,cATHER nc enHg anoE, eR. HE  
REGdsARsf SuEgT THREE HndRS ng THE oISuATCHESnc THE llgG nc uRdSSIA, nuEglgG  
THEz Ago THEg RE-SEAslgG THEz rITHSuECIAS rAy Ago CAREcdssf CndgTERcEITEo  
SEAsS. uERHAuS SdRuRISlgGsf Ig AaASTIng nc HdzAg RIGHTS, ITS IgTERCEuTIngS  
EgenfEO cdss sEGAsITf. THESTATdTE nc 1657 THAT ESTAAsISHEo THE unSTAs SERkICE  
oECsAREo ndTRIGHT THATTHE zAISs rERE THE aEST zEAgS nc oISCnkERlgG  
oAgGERndS Ago rICIEooESIGgS AGAlgST THE CnzzngrEAsTH. sEASES nc 1660 Ago 1663,  
CngclRzEOaf THE unST ncclCE ACT nc 1711, uERzITTEo GnKERgzEgT ncclCIASs Tn  
nuEgzAls dgoER rARRAgTS THAT THEf THEzSEskES ISSdEO. THEf SloESTEuuEO  
THISanTHERSnzE uRnCEodRE af uRnzdsGATlgG Ass-IgCsdSlkE GEgERAS  
rARRAgTS.\*THE SECRET ncclCE SEgT IgTERCEuTIngS Eg CsAIR Tn THE llgG Ago THnSE  
IgCluHER Tn THE CRfuTAGAsfSTS.THEf rERE Ignrg CnssECTIkEsf AS THE oECfuHERlgG  
aRagCH. dgsllE THESECRET ncclCE, THE aRagCH HAo gn SuECIclC snCATIng. ITS Tlgf  
STAcc nc EyuERTSmRIEO sARGESf AT HnzE, RECEIklgG THEIR zATERIAS af SuECIAS  
zESSEgGER.gnR HAo IT Agf cnRzAs nRGAgImATIng, THE SEglnR oECfuHERER aElgG  
zERESfclRST AzngG EbdAsS. znRE SECRET THAg THE SECRET ncclCE, THE  
aRagCH'ScdgoS CAzE cRnz SECRET-SERkICE zngEf ISSdEO Tn THE SECRETARf nc THE  
unSTncclCE cRnz uARsIAzEgT'S SdRusdS REkEgdE. SECdRITf rAS TIGHT—Ig Ass  
ncEgGsAgo uRnaAasf ngf 30 uEnusE IgEr rHAT olusnzATIC CnRRESungoEgCErAS aElgG  
REAO AT Agf GlkEg znzEgT. gEkERTHEsESS, znST zEg nc AccAIRSrERE ArARE nc THE  
uRACTICE nc nuEglgG\*THIS ACTIkITf cnRzS THE sEGAs uRECEoEgT cnR THE znoERg  
TAuulgG ncTEsEuHngES, AT sEAST Ig aRITAlg. SIGglclCAGTsf, HnrEkER, THE SndRCE nc  
THEunrER Tn IgTERCEuT CnzzdglCATIngS HAS gEkER aEEg oETERzlgEO. THECRnrg  
Slzsf EyERCISEo IT Ago, oESuITE nCCASIngAs oEaATE, HAS CngTlgdEOtn on Sn,  
uRESdzAasf rITH THE TACIT AuuRnkAs nc THE udasIC AS gECESsARfcnR THE SAcETf nc  
THE STATE.uRIkATE sETTERS, Ago THEf ncTEg EgCluHEREo THEIR CnRRESungoEgCE  
nREgTRdSTEO IT Tn uRIkATE zESSEgGERS rHEg SECRECF rAS ESSEgTIAs.AcTER THE  
EsECTnR nc HAgnkER SdCCEEOEO Tn THE EgGsISH THRngE ASGENRGE I Ig 1714,  
RETAIglgG THE RdsE nc THE GERzAg STATE, THE oECfuHERlgGaRagCH CnssAanRATEo  
rITH THE asACI CHAZaER zAlgTAlgEO AT gIEgadRG afTHE HAgnkERIAg GnKERgzEgT.  
CRfuTAGAsfSTS anoE, sAzUE, Ago gEdandRGHAo EkEg aEEg IzunRTEo cRnz THERE—Ag  
IRnglC oEkEsnuzEgT Ig kIEr nc AREcdSAs nc rAssIS Tn olkdsGE HIS TECHglbdE Tn

HAgNkER A cEr fEARS EARsIER.zAls nuEglgG aECAzE HAaITdAs. GEnRGE Ago HIS SdCCCESSnRS Tnnl ACngSTAgT uERSngAs IgTEREST Ig THE mRI, ncTEg EgCndRAGlgG TAsEgT rITHRnfAs andgTf. CnRRESungoEgCE rAS CsnSEsf rATCHEo cnR CRlaS THAT rEREuASSEo Tn THE oECfuHERlgG aRAgCH.odRIgG THE 1700S, THE aRAgCH'S ndTudT AkERAGEo Trn nR THREEoISuATCHES A rEEI, Ago SnzETIzES ngE A oAf. ITS CRfuTAGAsfSTS SnskEo THEoISuATCHES nc cRAgCE, AdSTRIA, SAyngf Ago nTHER GERzAg STATES, unsAgo,SuAlg, unRTdGAs, HnssAgo, oEgzARI, SrEoEg, SARoIglA, gAusES Ago nTHERITAsIag STATES, GREECE, TdRIEf, RdSSIA, Ago, sATER, THE dgITeo STATES. THERECnRo nc cREgCH IgTERCEuTIngS CnkERS Trn CEgTdRIES Ago CnzURISES clkEknsdzES nc IgTERCEuTS TnTAslgG 2,020 uAGES usdS THREE knsdzES nc IEfS.uERHAuS znRE TfulCAs IS THE SuAgISH onSSIER—THREE knsdzES nc IgTERCEuTScRnz 1719 Tn 1839 TnTAslgG 872 uAGES. gnT Ass nc THE zESSAGES rERESnskEo AT THE TIzE nc THEIR IgTERCEuTIng. zAgf rERE HEso EITHER dgTIsEgndGH HAo ACCdzdsATEo cnR A SdCCCESScds ATTACI nR dgTIs A gEEo ARnSE cnRTHEIR SnsdTIng.

Now we can see more and more discovered letters forming words. WE can observe the following: “ATTACI” meaning ‘attack’, so I -> k, “SdCCCESSnRS” must be “successors”, meaning d -> u, n -> o. The occurrences of “THE SECRET OccICE rAS” and “SECRET OccICE” in general help us draw the conclusion: c -> f, r -> h. So, the text now is the following:

SECRET OFFICE Ago THEIR oOzESTIC OgES FROz THE uRIkATE - OFFICE, aOTHsUaolkISIOgS OF THE uOST OFFICE. THE SECRET OFFICE HAS bUARTEREo Ig THREEROOzS AoEoIglgG THE FOREIGg OFFICE Ago EgTEREo uRIkATEsf FROz AaCHURCHsAgE. FIRE Ago CAgosES aURgEo COgSTAgTsf Ig OgE ROOz; THE STAFF sOoGEo IgTHE OTHERS. IT IgCsUoEo zEg HHO zAoE THEIR sIFE'S HORK THE SuECIAS Tf OFUgSEAslgG olusOzATIC uACKETS HITH SUCH, oEFTgESS THAT THEf COUso aERESEAsEo HITHOUT EkloEgCE OF TAzuERlgG; OgE SUCH OuEgER HAS e. E. aOoE,FATHER OF eOHg aOoE, eR. HE REGUsARsf SuEgT THREE HOURS Og THE oISuATCHESOF THE KIgG OF uRUSSIA, OuEglgG THEz Ago THEg RE-SEAslgG THEz HITHSuECIAS HAY Ago CAREFUssf COUgTERFEITEo SEAsS. uERHAuS SURuRISlgGsf Ig AaASTIOg OF HUzAg RIGHTS, ITS IgTERCEuTIOgS EgeOfEo FUss sEGAsITf. THESTATUTE OF 1657 THAT ESTAasISHEo THE uOSTAs SERKICE oECsAREo OUTRIGHT THATTHE zAlsS HERE THE aEST zEAgS OF oISCOKERlgG oAgGEROUS Ago HICKEooESIGgS AGAIgST THE COzzOgHEAsTH. sEASES OF 1660 Ago 1663, COgFIRzEoaf THE uOST OFFICE ACT OF 1711, uERzITTEo GOKERgzEgT OFFICIASs TO OuEgzAls UgoER HARRAgTS THAT THEf THEzSEskES ISSUEo. THEf SloESTEuuEo THISaOTHERSOzE uROCEoURE af uROzUsGATlgG Ass-IgCsUSIke GEgERAs HARRAgTS.\*THE SECRET OFFICE SEgT IgTERCEuTIOgS Eg CsAIR TO THE KIgG Ago THOSE IgCluHER TO THE CRfuTAGAsfSTS.THEf HERE KgOHg COssECTIkEsf AS THE oECfuHERlgG aRAgCH. UgsIKE THESECRET OFFICE, THE aRAgCH HAo gO SuECIFIC sOCATIOg. ITS TIgf STAFF OF EyuERTSHORKEo sARGEsf AT HOzE, RECEIklgG THEIR zATERIAS af SuECIAS

zESSEgGER.gOR HAO IT Agf FORzAs ORGAgImATIOg, THE SEgIOR oECfuHERER aElgG  
zERESfFIRST AzOgG EbUAsS. zORE SECRET THAg THE SECRET OFFICE, THE  
aRAgCH'SFUgoS CAzE FROz SECRET-SERkICE zOgEf ISSUEo TO THE SECRETARf OF  
THE uOSTOFFICE FROz uARsIAzEgT'S SURusUS REkEgUE. SECURITf HAS TIGHT—Ig Ass  
OFEGGsAgO uROaAasf Ogsf 30 uEOusE KgEH HHAT olusOzATIC CORRESuOgoEgCEHAS  
aElgG REAO AT Agf GIkEg zOzEgT. gEkERTHEsESS, zOST zEg OF AFFAIRSHERE AHARE  
OF THE uRACTICE OF OuEglgG\*THIS ACTIkITf FORzS THE sEGAs uRECEoEgT FOR THE  
zOoERg TAuulgG OFTEsEuHOgES, AT sEAST Ig aRITAlg. SIGgIfICAgTsf, HOHEKER, THE  
SOURCE OF THEuOHER TO IgTERCEuT COzzUgICATIOgS HAS gEkER aEEg oETERzlgEo.  
THECROHg Slzusr EyERCISEo IT Ago, oESuITE OCCASIOgAs oEaATE, HAS COgTlgUEoTO  
oO SO, uRESUzAasf HITH THE TACIT AuuROkAs OF THE uUasIC AS gECESSARfFOR THE  
SAFETf OF THE STATE.uRIkATE sETTERS, Ago THEf OFTEg EgCluHEREo THEIR  
CORRESuOgoEgCE OREgTRUSTEo IT TO uRIkATE zESSEgGERS HHEg SECREcf HAS  
ESSEgTIAs.AFTER THE EsECTOR OF HAgOkER SUCCEEOEO TO THE EgGsISH THROgE  
ASGEORGE I Ig 1714, RETAlglgG THE RUSe OF THE GERzAg STATE, THE  
oECfuHERIgGaRAgCH COssAaORATEo HITH THE asACK CHAZaER zAlgTAlgEO AT  
glEgaURG afTHE HAgOkERIAg GOkERgzEgT. CRfuTAGAsfSTS aOoE, sAzUE, Ago  
gEUaOURGHAo EkEg aEEg IzuORTEo FROz THERE—Ag IROgIC oEkEsOuzEgT Ig kIEH OF  
AREFUSAs OF HAssIS TO oIkUsGE HIS TECHgIbUE TO HAgOkER A FEH fEARS  
EARsIER.zAls OuEglgG aECAzE HAaITUAs. GEORGE Ago HIS SUCCESSORS TOOK  
ACOGSTAgT uERSOgAs IgTEREST Ig THE HORK, OFTEg EgCOURAGlgG TAsEgT  
HITHROfAs aOUgTf. CORRESuOgoEgCE HAS CsOSEsf HATCHEo FOR CRlAs THAT  
HEREuASSEo TO THE oECfuHERIgG aRAgCH.oURlgG THE 1700S, THE aRAgCH'S  
OUTuUT AkERAGEo THO OR THREEoISuATCHES A HEEK, Ago SOzETizES OgE A oAf. ITS  
CRfuTAGAsfSTS SOskEO THEoISuATCHES OF FRAgCE, AUSTRIA, SAyOgf Ago OTHER  
GERzAg STATES, uOsAgo,SuAlg, uORTUGAs, HOssAgo, oEgzARK, SHEoEg, SARolglA,  
gAusES Ago OTHERITAsIAg STATES, GREECE, TURKEf, RUSSIA, Ago, sATER, THE UgITEo  
STATES. THERECORo OF FREgCH IgTERCEuTIOgS COkERS THO CEgTURIES Ago  
COzuRISES FIKEkOsUZES OF IgTERCEuTS TOTAslgG 2,020 uAGES usUS THREE  
kOsUZES OF KEfS.uERHAuS zORE TfuICAs IS THE SuAgISH oOSSIER—THREE kOsUZES  
OF IgTERCEuTSFROz 1719 TO 1839 TOTAslgG 872 uAGES. gOT Ass OF THE zESSAGES  
HERESOsKEo AT THE TizE OF THEIR IgTERCEuTIOg. zAgf HERE HESo EITHER  
UgTIsEgOUGH HAO ACCUzUsATEo FOR A SUCCESSFUUs ATTACK OR UgTIs A gEEo  
AROSE FORTHEIR SOsUTIOg.

Next, we have the following “THE FOREIGN OFFICE” meaning “foreign”, therefore g -> n, from the context “SECRET OFFICE AND THEIR”, “AND” has to be “And”, therefore o -> d, “DOMESTIC” means “domestic”, therefore z -> m. also from the context “CONSTANTLY IN ONE ROOM”, there should be “constantly” meaning s -> l, and f -> y, so the text looks the following way:

SECRET OFFICE AND THEIR DOMESTIC ONES FROM THE OFFICE, aOTHSUADIVISIONS OF THE POST OFFICE. THE SECRET OFFICE HAS QUARTERED IN THREE ROOMS ADJOINING THE FOREIGN OFFICE AND ENTERED PRIVATELY FROM A CHURCH LANE. FIRE AND CANDLES BURNED CONSTANTLY IN ONE ROOM; THE STAFF LODGED IN THE OTHERS. IT INCLUDED MEN WHO MADE THEIR LIFE'S WORK THE SPECIALTY OF UNSEALING DIPLOMATIC PACKETS WITH SUCH, DEFTNESS THAT THEY COULD RESEAL THEM WITHOUT EVIDENCE OF TAMpering; ONE SUCH OFFICER HAS E. E. AODE, FATHER OF JOHN AODE, ESQ. HE REGULARLY SENT THREE HOURS ON THE DISPATCHES OF THE KING OF RUSSIA, OPENING THEM AND THEN RE-SEALING THEM WITH SPECIAL HAND AND CAREFULLY COUNTERFEITED SEALS. HOWEVER, SURPRISINGLY IN A STATE OF HUMAN RIGHTS, ITS INTERCEPTIONS ENJOYED FULL LEGALITY. THE STATUTE OF 1657 THAT ESTABLISHED THE POSTAL SERVICE DECLARED OUTRIGHT THAT THE MAILS HERE THE BEST MEANS OF DISCOVERING DANGEROUS AND HIDDEN DESIGNS AGAINST THE COMMONWEALTH. LEASES OF 1660 AND 1663, CONFIRMED BY THE POST OFFICE ACT OF 1711, PERMITTED GOVERNMENT OFFICIALS TO OPEN MAIL UNDER WARRANTS THAT THEY THEMSELVES ISSUED. THEY SIDESTEPPED THIS OTHERWISE PROCEDURE BY PROMULGATING ALL-INCLUSIVE GENERAL WARRANTS. \*THE SECRET OFFICE SENT INTERCEPTIONS EN CLAIR TO THE KING AND THOSE INCIPIENT TO THE CRYPTANALYSTS. THEY HERE KNOW COLLECTIVELY AS THE DECRYPTING BRANCH. UNLIKE THE SECRET OFFICE, THE BRANCH HAD NO SPECIFIC LOCATION. ITS TINY STAFF OF EYE-TESTERS LARGELY AT HOME, RECEIVING THEIR MATERIAL BY SPECIAL MESSENGER. NOR HAD IT ANY FORMAL ORGANIZATION, THE SENIOR DECRYPTER BEING MERELY FIRST AMONG EQUALS. MORE SECRET THAN THE SECRET OFFICE, THE BRANCH'S FUNDS CAME FROM SECRET-SERVICE MONEY ISSUED TO THE SECRETARY OF THE POST OFFICE FROM PARLIAMENT'S SURPLUS REVENUE. SECURITY WAS TIGHT—IN ALL OF ENGLAND AND ROYALTY ONLY 30 PEOPLE KNEW THAT DIPLOMATIC CORRESPONDENCE WAS BEING READ AT ANY GIVEN MOMENT. NEVERTHELESS, MOST MEN OF AFFAIRS HERE AWARE OF THE PRACTICE OF OPENING \*THIS ACTIVITY FORMS THE LEGAL PRECEDENT FOR THE MODERN TAPPING OF TELEPHONES, AT LEAST IN BRITAIN. SIGNIFICANTLY, HOWEVER, THE SOURCE OF THE OTHER TO INTERCEPT COMMUNICATIONS HAS NEVER BEEN DETERMINED. THE CROWN SIMPLY EXERCISED IT AND, DESPITE OCCASIONAL DEBATE, HAS CONTINUED TO DO SO, RESUMINGLY WITH THE TACIT APPROVAL OF THE PUBLIC AS NECESSARY FOR THE SAFETY OF THE STATE. PRIVATE LETTERS, AND THEY OFTEN ENCIPIERED THEIR CORRESPONDENCE OR ENTRUSTED IT TO PRIVATE MESSENGERS WHEN SECRECY WAS ESSENTIAL. AFTER THE ELECTOR OF HANOVER

SUCCEEDED TO THE ENGLISH THRONE AS GEORGE I IN 1714, RETAINING THE RULE OF THE GERMAN STATE, THE DECYHERING RANCH COLLABORATED WITH THE LACK CHAMBER MAINTAINED AT NIENBURG AND THE HANOVERIAN GOVERNMENT. CRYPTANALYSTS BODE, LAMUE, AND NEUBOURGHAD BEEN IMPORTED FROM THERE—AN IRONIC DEVELOPMENT IN VIEW OF REFUSAL OF HALLIS TO DISCLOSE HIS TECHNIQUE TO HANOVER A FEW YEARS EARLIER. MAIL OPENING BECAME HABITUAL. GEORGE AND HIS SUCCESSORS TOOK A CONSTANT PERSONAL INTEREST IN THE WORK, OFTEN ENCOURAGING TALENT WITH ROYAL AID. CORRESPONDENCE HAS CLOSELY WATCHED FOR CRIMES THAT HEREIN LED TO THE DECYHERING RANCH. DURING THE 1700S, THE RANCH'S OUTPUT AVERAGED TWO OR THREE DISPATCHES A WEEK, AND SOMETIMES ONE A DAY. ITS CRYPTANALYSTS SOLVED THE DISPATCHES OF FRANCE, AUSTRIA, SPAIN AND OTHER GERMAN STATES, HOLLAND, SWEDEN, PORTUGAL, HOLLAND, DENMARK, SHEDEN, SARDINIA, NAPLES AND OTHER ITALIAN STATES, GREECE, TURKEY, RUSSIA, AND, LATER, THE UNITED STATES. THE RECORD OF FRENCH INTERCEPTIONS COVERS TWO CENTURIES AND COMPRISES FIVE VOLUMES OF INTERCEPTS TOTALING 2,020 PAGES PLUS THREE VOLUMES OF KEYS. PERHAPS MORE TYPICAL IS THE SPANISH DOSSIER—THREE VOLUMES OF INTERCEPTS FROM 1719 TO 1839 TOTALING 872 PAGES. NOT ALL OF THE MESSAGES WERE SOLVED AT THE TIME OF THEIR INTERCEPTION. MANY WERE HELD EITHER UNTIL ENOUGH HAD ACCUMULATED FOR A SUCCESSFUL ATTACK OR UNTIL A NEED AROSE FOR THEIR SOLUTION.

Next we see this: “ FIRE AND CANDLES BURNED”, from the context we deduct the word “burned”, meaning a -> b, from “THE POSTAL SERVICE DECLARED” we deduct the “postal service”, therefore u -> p, and k -> v, “ENJOYED FULL”, from “enjoyed”, e -> j, so the text looks like:

SECRET OFFICE AND THEIR DOMESTIC ONES FROM THE PRIVATE - OFFICE, BOTH SUBDIVISIONS OF THE POST OFFICE. THE SECRET OFFICE WAS QUARTERED IN THREE ROOMS ADJOINING THE FOREIGN OFFICE AND ENTERED PRIVATELY FROM ABCHURCH LANE. FIRE AND CANDLES BURNED CONSTANTLY IN ONE ROOM; THE STAFF LODGED IN THE OTHERS. IT INCLUDED MEN WHO MADE THEIR LIFE'S WORK THE SPECIALTY OF UNSEALING DIPLOMATIC PACKETS WITH SUCH DEFTNESS THAT THEY COULD BE RESEALED WITHOUT EVIDENCE OF TAMPERING; ONE SUCH OPENER WAS J. E. BODE, FATHER OF JOHN BODE, JR. HE REGULARLY SPENT THREE HOURS ON THE DISPATCHES OF THE KING OF PRUSSIA, OPENING THEM AND THEN RE-SEALING THEM WITH SPECIAL WAY AND CAREFULLY COUNTERFEITED SEALS. PERHAPS SURPRISINGLY IN ABSTENTION OF HUMAN RIGHTS, ITS INTERCEPTIONS ENJOYED FULL LEGALITY. THE STATUTE OF 1657 THAT ESTABLISHED THE POSTAL SERVICE DECLARED OUTRIGHT THAT THE MAILS WERE THE BEST MEANS OF DISCOVERING DANGEROUS AND WICKED DESIGNS AGAINST THE COMMONWEALTH. LEASES OF 1660 AND 1663, CONFIRMED BY THE POST OFFICE ACT OF 1711, PERMITTED GOVERNMENT OFFICIALS TO OPEN MAIL UNDER WARRANTS THAT THEY THEMSELVES ISSUED. THEY SIDESTEPED THIS BOTHERSOME PROCEDURE BY PROMULGATING ALL-INCLUSIVE

GENERAL WARRANTS.\*THE SECRET OFFICE SENT INTERCEPTIONS EN CLAIR TO THE KING AND THOSE INCIPHER TO THE CRYPTANALYSTS.THEY WERE KNOWN COLLECTIVELY AS THE DECYPHERING BRANCH. UNLIKE THESECRET OFFICE, THE BRANCH HAD NO SPECIFIC LOCATION. ITS TINY STAFF OF EyPERTSWORKED LARGELY AT HOME, RECEIVING THEIR MATERIAL BY SPECIAL MESSENGER.NOR HAD IT ANY FORMAL ORGANImATION, THE SENIOR DECYPHERER BEING MERELYFIRST AMONG EbUALS. MORE SECRET THAN THE SECRET OFFICE, THE BRANCH'SFUNDS CAME FROM SECRET-SERVICE MONEY ISSUED TO THE SECRETARY OF THE POSTOFFICE FROM PARLIAMENT'S SURPLUS REVENUE. SECURITY WAS TIGHT—IN ALL OFENGLAND PROBABLY ONLY 30 PEOPLE KNEW WHAT DIPLOMATIC CORRESPONDENCEWAS BEING READ AT ANY GIVEN MOMENT. NEVERTHELESS, MOST MEN OF AFFAIRSWERE AWARE OF THE PRACTICE OF OPENING\*THIS ACTIVITY FORMS THE LEGAL PRECEDENT FOR THE MODERN TAPPING OFTELEPHONES, AT LEAST IN BRITAIN. SIGNIFICANTLY, HOWEVER, THE SOURCE OF THEPOWER TO INTERCEPT COMMUNICATIONS HAS NEVER BEEN DETERMINED. THECROWN SIMPLY EyERCISED IT AND, DESPITE OCCASIONAL DEBATE, HAS CONTINUEDTO DO SO, PRESUMABLY WITH THE TACIT APPROVAL OF THE PUBLIC AS NECESSARYFOR THE SAFETY OF THE STATE.PRIVATE LETTERS, AND THEY OFTEN ENCIPHERED THEIR CORRESPONDENCE ORENTRUSTED IT TO PRIVATE MESSENGERS WHEN SECRECY WAS ESSENTIAL.AFTER THE ELECTOR OF HANOVER SUCCEEDED TO THE ENGLISH THRONE ASGEORGE I IN 1714, RETAINING THE RULE OF THE GERMAN STATE, THE DECYPHERINGBRANCH COLLABORATED WITH THE BLACK CHAMBER MAINTAINED AT NIENBURG BYTHE HANOVERIAN GOVERNMENT. CRYPTANALYSTS BODE, LAMPE, AND NEUBOURGHAD EVEN BEEN IMPORTED FROM THERE—AN IRONIC DEVELOPMENT IN VIEW OF AREFUSAL OF WALLIS TO DIVULGE HIS TECHNIbUE TO HANOVER A FEW YEARS EARLIER.MAIL OPENING BECAME HABITUAL. GEORGE AND HIS SUCCESSORS TOOK ACONSTANT PERSONAL INTEREST IN THE WORK, OFTEN ENCOURAGING TALENT WITHROYAL BOUNTY. CORRESPONDENCE WAS CLOSELY WATCHED FOR CRIBS THAT WEREPASED TO THE DECYPHERING BRANCH.DURING THE 1700S, THE BRANCH'S OUTPUT AVERAGED TWO OR THREEDISPATCHES A WEEK, AND SOMETIMES ONE A DAY. ITS CRYPTANALYSTS SOLVED THEDISPATCHES OF FRANCE, AUSTRIA, SAYONY AND OTHER GERMAN STATES, POLAND,SPAIN, PORTUGAL, HOLLAND, DENMARK, SWEDEN, SARDINIA, NAPLES AND OTHERITALIAN STATES, GREECE, TURKEY, RUSSIA, AND, LATER, THE UNITED STATES. THERECORD OF FRENCH INTERCEPTIONS COVERS TWO CENTURIES AND COMPRISES FIVEVOLUMES OF INTERCEPTS TOTALING 2,020 PAGES PLUS THREE VOLUMES OF KEYS.PERHAPS MORE TYPICAL IS THE SPANISH DOSSIER—THREE VOLUMES OF INTERCEPTSFROM 1719 TO 1839 TOTALING 872 PAGES. NOT ALL OF THE MESSAGES WERESOLVED AT THE TIME OF THEIR INTERCEPTION. MANY WERE HELD EITHER UNTILENOUGH HAD ACCUMULATED FOR A SUCCESSFUL ATTACK OR UNTIL A NEED AROSE FORTHEIR SOLUTION.

We can see from “ORGANImATION” the word “organization,” therefore m -> z, “TECHNIbUE” as in “technique”, meaning b -> q, and “RE-SEALING THEM WITH SPECIAL WAy”, talking about diplomatic packets, we reffer “wax”, meaning y -> x. And the final, decyphthered text is:

SECRET OFFICE AND THEIR DOMESTIC ONES FROM THE PRIVATE - OFFICE, BOTH SUBDIVISIONS OF THE POST OFFICE. THE SECRET OFFICE WAS QUARTERED IN THREE ROOMS ADJOINING THE FOREIGN OFFICE AND ENTERED PRIVATELY FROM ABCHURCH LANE. FIRE AND CANDLES BURNED CONSTANTLY IN ONE ROOM; THE STAFF LODGED IN THE OTHERS. IT INCLUDED MEN WHO MADE THEIR LIFE'S WORK THE SPECIALTY OF UNSEALING DIPLOMATIC PACKETS WITH SUCH, DEFTNESS THAT THEY COULD BE RESEALED WITHOUT EVIDENCE OF TAMPERING; ONE SUCH OPENER WAS J. E. BODE, FATHER OF JOHN BODE, JR. HE REGULARLY SPENT THREE HOURS ON THE DISPATCHES OF THE KING OF PRUSSIA, OPENING THEM AND THEN RE-SEALING THEM WITH SPECIAL WAX AND CAREFULLY COUNTERFEITED SEALS. PERHAPS SURPRISINGLY IN A BASTION OF HUMAN RIGHTS, ITS INTERCEPTIONS ENJOYED FULL LEGALITY. THE STATUTE OF 1657 THAT ESTABLISHED THE POSTAL SERVICE DECLARED OUTRIGHT THAT THE MAILS WERE THE BEST MEANS OF DISCOVERING DANGEROUS AND WICKED DESIGNS AGAINST THE COMMONWEALTH. LEASES OF 1660 AND 1663, CONFIRMED BY THE POST OFFICE ACT OF 1711, PERMITTED GOVERNMENT OFFICIALS TO OPEN MAIL UNDER WARRANTS THAT THEY THEMSELVES ISSUED. THEY SIDESTEPED THE BOTHERSOME PROCEDURE BY PROMULGATING ALL-INCLUSIVE GENERAL WARRANTS. \*THE SECRET OFFICE SENT INTERCEPTIONS EN CLAIR TO THE KING AND THOSE INCIPHER TO THE CRYPTANALYSTS. THEY WERE KNOWN COLLECTIVELY AS THE DECIPHERING BRANCH. UNLIKE THE SECRET OFFICE, THE BRANCH HAD NO SPECIFIC LOCATION. ITS TINY STAFF OF EXPERTS WORKED LARGELY AT HOME, RECEIVING THEIR MATERIAL BY SPECIAL MESSENGER. NOR HAD IT ANY FORMAL ORGANIZATION, THE SENIOR DECIPHERER BEING MERELY FIRST AMONG EQUALS. MORE SECRET THAN THE SECRET OFFICE, THE BRANCH'S FUNDS CAME FROM SECRET-SERVICE MONEY ISSUED TO THE SECRETARY OF THE POST OFFICE FROM PARLIAMENT'S SURPLUS REVENUE. SECURITY WAS TIGHT—IN ALL OF ENGLAND PROBABLY ONLY 30 PEOPLE KNEW WHAT DIPLOMATIC CORRESPONDENCE WAS BEING READ AT ANY GIVEN MOMENT. NEVERTHELESS, MOST MEN OF AFFAIRS WERE AWARE OF THE PRACTICE OF OPENING \*THIS ACTIVITY FORMS THE LEGAL PRECEDENT FOR THE MODERN TAPPING OF TELEPHONES, AT LEAST IN BRITAIN. SIGNIFICANTLY, HOWEVER, THE SOURCE OF THE POWER TO INTERCEPT COMMUNICATIONS HAS NEVER BEEN DETERMINED. THE CROWN SIMPLY EXERCISED IT AND, DESPITE OCCASIONAL DEBATE, HAS CONTINUED TO DO SO, PRESUMABLY WITH THE TACIT APPROVAL OF THE PUBLIC AS NECESSARY FOR THE SAFETY OF THE STATE. PRIVATE LETTERS, AND THEY OFTEN ENCIPHERED THEIR CORRESPONDENCE OR ENTRUSTED IT TO PRIVATE MESSENGERS WHEN SECRECY WAS ESSENTIAL. AFTER THE ELECTOR OF HANOVER SUCCEEDED TO THE ENGLISH THRONE AS GEORGE I IN 1714, RETAINING THE RULE OF THE GERMAN STATE, THE DECIPHERING BRANCH COLLABORATED WITH THE BLACK CHAMBER MAINTAINED AT



NIENBURG BY THE HANOVERIAN GOVERNMENT. CRYPTANALYSTS BODE, LAMPE, AND NEUBOURG HAS EVEN BEEN IMPORTED FROM THERE—AN IRONIC DEVELOPMENT IN VIEW OF REFUSAL OF WALLIS TO DIVULGE HIS TECHNIQUE TO HANOVER A FEW YEARS EARLIER. MAIL OPENING BECAME HABITUAL. GEORGE AND HIS SUCCESSORS TOOK A CONSTANT PERSONAL INTEREST IN THE WORK, OFTEN ENCOURAGING TALENT WITH ROYAL BOUNTY. CORRESPONDENCE WAS CLOSELY WATCHED FOR CRIBS THAT WERE PASSED TO THE DECIPHERING BRANCH. DURING THE 1700S, THE BRANCH'S OUTPUT AVERAGED TWO OR THREE DISPATCHES A WEEK, AND SOMETIMES ONE A DAY. IT'S CRYPTANALYSTS SOLVED THE DISPATCHES OF FRANCE, AUSTRIA, SAXONY AND OTHER GERMAN STATES, POLAND, SPAIN, PORTUGAL, HOLLAND, DENMARK, SWEDEN, SARDINIA, NAPLES AND OTHER ITALIAN STATES, GREECE, TURKEY, RUSSIA, AND, LATER, THE UNITED STATES. THE RECORD OF FRENCH INTERCEPTIONS COVERS TWO CENTURIES AND COMPRISES FIVE VOLUMES OF INTERCEPTS TOTALING 2,020 PAGES PLUS THREE VOLUMES OF KEYS. PERHAPS MORE TYPICAL IS THE SPANISH DOSSIER—THREE VOLUMES OF INTERCEPTS FROM 1719 TO 1839 TOTALING 872 PAGES. NOT ALL OF THE MESSAGES WERE SOLVED AT THE TIME OF THEIR INTERCEPTION. MANY WERE HELD EITHER UNTIL ENOUGH HAD ACCUMULATED FOR A SUCCESSFUL ATTACK OR UNTIL A NEED AROSE FOR THEIR SOLUTION.