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: Grigoraș Dumitru FAF-221,

Checked: Dumitru Nirca asist. univ.,

Chișinău 2023

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 cipher text length increases, it gradually converges towards this general frequency ordering.

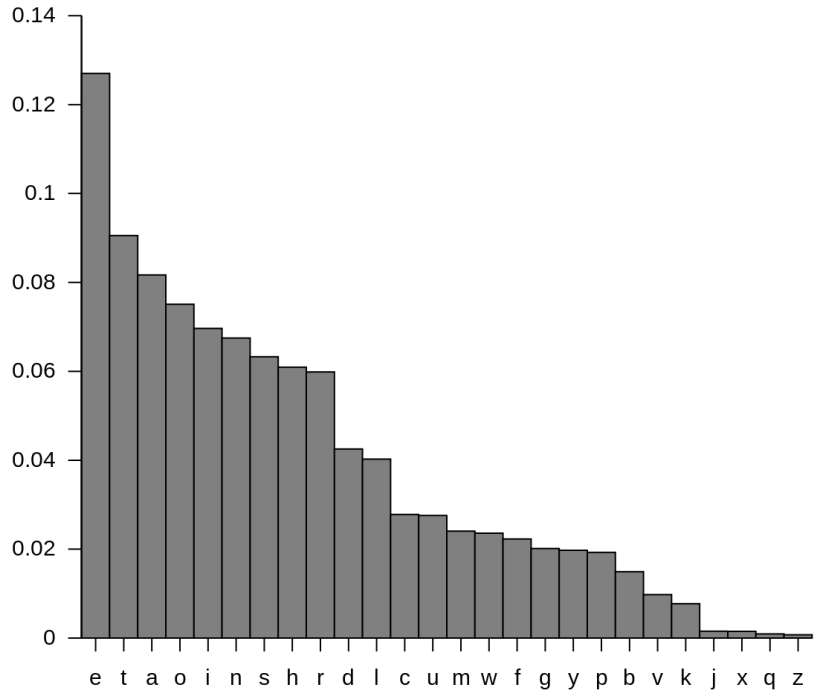

Fig.1: English letter frequency

Implementation(Var. Nr.15)

I have a cryptogram c =

WQV WVSVJITUQ ztov hifuwnjituqf rqtw xw xp wnotf. Ptzdvs C. A. Znipvpvgw "Rqtw qtwq Jno rindjqw!" xg 1844. Wqv gvyw fvti qxp strfvi tgouinznwxngts tjvgw, Citghxp N. E. Pzxwq, udasxpqvo t hnzzvihxts hnovvgwxwsvo Wqv Pvhivw Hniivpungoxgj Knhtadstif; Totuwvo cni Dpv wn Znipv'pVsvhwin-Ztjgvwxh Wvsvjituq, xg rqnpv uivcthv qv ovhstivo wqtw "pvhivhf xghniivpungovghv, xp cti wqv znpw xzuniwtgw hngpxovitwxng." Wqxp rtpuinkxovo af t pduvivghxuqvizvgw.Tp wqv znpw vyhxwxgj xgkvgwxng nc wqv cxipw qtsc nc wqv hvgwdif, wqvwvsvjituq pwxiivo tp zdhq xgwvivpw xg xwp otf tp Pudwgxl oxo xg xwp. Wqvjivtw tgo rxovsf cvsw gvvo cni pvhivhf trtlvgvo wqv stwvgw xgwvivpw xghxuqvip wqtw pn ztgf uvnusv pvvz wn qtkv, tgo lxgosvo t gvr xgwvivpw xgztgf nwqvip. Onmvgp nc uvipngp twwvzuwvo wn oivtz du wqvxi nrgdgaivtltasv hxuqvip. Wqvxi hngwixadwxngp vgixhqvo xw rxwq onmvgp nc gvrhxuqvi pfpwvzp.Tp adpxgvppzvg tgo wqv udasxh dpvo wqv wvsvjituq zniv tgo zniv,wqvf cndgo wqtw wqvxi cvtip tandw sthl nc uixkthf rviv vytjjvitwvo. Wqvhsvilp ovtsw xzuvipngtssf rxwq wqv zvpptjvp. Wqv wvsvjituq hnzutgxvpivpuvhwvo wqvxi hngcxovgwxtsxwf. Tgo hnzzvihxts hnovp sxlv Pzxwq'p, rqxhqivusthvo rniop tgo uqitpvp af pxgjsv hnovrniop ni hnov-gdzavip wn hdw wvsvjituq wnssp, tccniovo pdccxhxvgw pvhdixwf cni znpwadpxgvpp witgpthwxngp af pxzusf uivhsdoxgj tg tw-pxjqw hnzuivqvgpxng ncwqv zvtgxgj. Wqv ainlvip tgo witovip pnng ivtsxmvo wqtw wqv ztxgtoktgwtjv nc wqvpv hnovp rtp wqvxi vhngnzf.Jnkvigzvgw zxgxpwixvp dpvo wqv wvsvjituq, wnn. Tw cxipw wqvf zdpwqtkv vghnovo rxwq wqvxi gnzvghstwnip. Adw tswqndjq pvhivhf rtputitzndgw cni wqvz, wqvf sxlvo wqv wvsvjituqxh vhngnzf nc t stijv hnov—vpuvhxtssf tp wqvf wvsvjituqvo zniv tgo zniv. Pn rqvg wqv wxzv tiixkvown hnzuxsv t gvr gnzvghstwni, wqvf tatgongvo wqtw cniz, hnuxvo wqvhnzzvihxts cniz, tgo uinodhvo t cdss-csvojvo hnov. Wqv gnzvghstwnipqto qto wqvxi 1,- ni 2,000 hnov-gdzavip xg zxyvo niovi, adw wqv rtitgo cnivxjg zxgxpwixvp atslvo tw wqv vyuvgpv nc oitrxgj du t 50,000-vgwif hnov xg wrn utiwp, tgo wqvf qto gn uincvppxngts hifuwtgtsfpwp wnrtig wqvz nc wqv otgjvi nc wqv ngv-utiw cniztw. Wqvf ivsxvo cni pvhdixwfdung pztss voxwxngp, axj ptcvp, vywvgpxkv svyxhng (stijv hnovp tiv qtioviwn aivtl wqtg pztss ngvp, nwqvi wqxgjp avxgj vbdts), tgopduvivghxuqvizvgw, ivwtxgxgj hnovgdzavip wn cthxsxwtwv wqxp xgpwvto ncprxwhqxgj wn hnovrniop. Wqxp vknsdwxng rtp vppvgwxtssf hnzusvwv af wqv1860p. Wqv stijv, ngv-utiw hnov qto ivusthvo wqv pztss, wrn-utiwgnzvghstwni xg qxjq-svkvs zxsxwtif tgo oxusnztwxh hifuwnjituqf.Zvtgrqxsv, wqv wvsvjituq, tdwqni nc wqxp ovkvsnuzvgw, rtp hivtwxgjpnzvwqxgj gvr xg rti—pxjgts hnzzdgxhtwxngp, ni knsdzxgndp hnzztgotgo ivhnggtxpptghv zvpptjvp. Nc hndipv pdhq zvpptjvp qto vyxpwvoavcniv, rxwq wnihqvp, uxjvngp, tgo hndixvip, adw xg pn itivcxvo t cniz wqtwwqvf rviv gnw vkvg htssvo "pxjgts hnzzdgxhtwxngp." Wqv wvsvjituqvgtasvo hnzztgovip, cni wqv cxipw wxzv xg qxpwnif, wn vyviw xgpwtgwtgvndptgo hngwxgdndp hngwins nkvi jivtw ztppvp nc zvg puivto nkvi stijvtivtp.Wqvpv wthwxhts zvpptjvp ivbdxivo uinwvhwxng: wvsvjituq rxivp hndso avwtuuvo. Gvxwqvi wqv nso gnzvghstwni gni wqv gvr hnov rndso on. Wqvfrviv wnn vtpf wn htuwdiv xg hnzatw, wnn qtio wn ivxppdv bdxhlsf tgocivbdvgwsf wn wqv gdzvindp tgo rxovpuivto wvsvjituq unpwp. Pxjgtsnccxhvip wdigvo trtf cinz wqvz. Wqvf snnlvo xgpwvto wn wqtw gvjsvhwvohqxso nc hifuwnjituqf, wqv hxuqvi. Hxuqvip hndso av uixgwvo hqvtusf ng tpxgjsv pqvvw nc utuvi tgo oxpwixadwvo rxwq vtpv. Pvhivhf rtp atpvo dungktixtasv lvfp, pn htuwdiv nc wqv jvgvits pfpwvz tgo vkvg nc ngv nc wqvlvfp rndso gnw hnzuinzxpv tss tg tizf'p pvhivw zvpptjvp. Pnsdwxngprndso av uivkvgwvo af ituxo lvf hqtgjvp. Hxuqvip rviv xovts cni atwwsv-mngv zvpptjvp, tgo wqv cxipw nc wqv znovig rtip, wqv Tzvixhtg Hxkxs Rti,dpvo wqvz cni edpw wqtw. Wqdp rtp anig t gvr jvgiv xg hifuwnjituqf: wqvcxvso hxuqvi.

So first we look at the frequencies as shown bellow:

Character	Frequency
v	438
w	283
t	243
n	227
i	222
p	212
g	207
x	188
q	159
o	144
h	127
s	118
z	100
u	91
d	71
j	65
c	63
f	62
r	51
a	38
k	21
l	16
y	9
b	4
m	4
e	2

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

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:

tqe tesejiauq zaoe hifutnjiauqf rqat xt xp tnoaf. pazdes c. a. znipepegt "rqat qatq jno rindjqt!" xg 1844. **tqe** geyt feai qxp sarfei agouinzntxngas ajegt, ciaghxp n. e. pzxtq, udasxpqeo a hnzzeihxas hnoeegtxtseo **tqe** pehiet hniiepungoxgj knhaadsaif; aoauteo cni dpe tn znipe'pesehtin-zajgetxh tesejiauq, xg rqnpe uiecahe qe oehsaieo tqat "pehiehf xghniiepungoeghe, xp cai **tqe** znpt xzunitagt hngpxoeiatxng." tqxp rapuinkxoeo af a pdueieghxuqeizegt.ap **tqe** znpt eyhxtxgj xgkegtxng nc tqe cxipt qasc nc tqe hegtdif, **tqe**tesejiauq ptxiieo ap zdhq xgteiept xg xtp oaf ap pudtgxl oxo xg xtp. tqejieat ago rxoesf cest geeo cni pehiehf aralegeo tqe sategt xgteiept xghxuqeip tqat pn zagf uenuse peez tn qake, ago lxgoseo a ger xgteiept xgzagf ntqeip. onmegp nc ueipngp attezuteo tn oieaz du tqexi nrgdgaiealaase hxuqeip. tqexi hngtixadtxngp egixhqeo xt rxtq onmegp nc gerhxuqei pfptezp.ap adpxgeppzeg ago tqe udasxh dpeo tqe tesejiauq znie ago znie,tqef cndgo tqat tqexi ceaip aandt sahl nc uixkahf reie eyajjeiateo. tqehseilp oeast xzueipngassf rxtq tqe zeppajep. tqe tesejiauq hnzuagxepiepuehteo tqexi hngcxoegtxasxtf. ago hnzzeihxas hnoep sxle pzxtq'p, rqxhqieusaheo rniop ago uqiapep af pxgjse hnoerniop ni hnoe-gdzaeip tn hdt tesejiauq

tnssp, accnioeo pdccxhxegt pehdixtf cni znptadpxgepp tiagpahtxngp af pxzusf uiehsdoxgj ag at-pxjqt hnzuieqegpxng nctqe zeagxgj. tqe ainleip ago tiaoeip pnng ieasxmeo tqat tqe zaxgaokagtaje nc tqepe hnoep rap tqexi ehngnzf.jnkeigzegt zxgxptixep dpeo tqe tesejiauq, tnn. at cxipt tqef zdptqake eghnoeo rxtq tqexi gnzeghsatnip. adt astqndjq pehiehf rapuaiazndgt cni tqez, tqef sxleo tqe tesejiauqxh ehngnzf nc a saije hnoe—epuehxassf ap tqef tesejiauqeo znie ago znie. pn rqeg tqe txze aiixkeotn hnzuxse a ger gnzeghsatni, tqef aaagongeo tqat cniz, hnuxeo tqehnzzeihxas cniz, ago uinodheo a cdss-cseojeo hnoe. tqe gnzeghsatnipqao qao tqexi 1,- ni 2,000 hnoe-gdzaeip xg zxyeo nioei, adt tqe raiago cniexjg zxgxptixep aasleo at tqe eyuegpe nc oiarxgj du a 50,000-egtif hnoe xg trn uaitp, ago tqef qao gn uinceppxngas hifutagasfptp tnraig tqez nc tqe oagjei nc tqe nge-uait cnizat. tqef iesxeo cni pehdixtfdung pzass eoxtxngp, axj pacep, eytegpxke seyxhng (saije hnoep aie qaioeitn aieal tqag pzass ngep, ntqei tqxgjp aexgj ebdas), agopdueieghxuqeizegt, ietaxgxgj hnoegdzaeip tn cahxsxtate tqxp xgpteao ncprxthqxgj tn hnoerniop. tqxp eknsdtxng rap eppegtxassf hnzusete af tqe1860p.
tqe saije, nge-uait hnoe qao ieusaheo tqe pzass, trn-uaitgnzeghsatni xg qxjq-sekes zxsxtaif ago oxusnzatxh hifutnjiauqf.zeagrqxse, tqe tesejiauq, adtqni nc tqxp oekesnuzegt, rap hieatxgjpnzetqxgj ger xg rai—pxjgas hnzzdgxhatxngp, ni knsdzxgndp hnzzagoago iehnggaxppaghe
zeppajep. nc hndipe pdhq zeppajep qao eyxpteoaecnie, rxtq tnihqep, uxjengp, ago hndixeip, adt
xg pn iaiecxeo a cniz tqattqef reie gnt ekeg hasseo "pxjgas hnzzdgxhatxngp." tqe tesejiauqegaaseo hnzzagoeip, cni tqe cxipt txze xg qxptnif, tn eyeit xgptagtagendpago hngtxgdndp hngtins nkei jieat zappep nc zeg puieao nkei saijeaieap.tqepe tahtxhas zeppajep iebdxieo uintehtxng: tesejiauq rxiep hndso aetauueo. gextqei tqe nso gnzeghsatni gni tqe ger hnoe rndso on. tqefreie tnn eapf tn hautdie xg hnzaat, tnn qaio tn iexppde bdxhlsf agociebdegtsf tn tqe gdzeindp ago rxoepuieao tesejiauq unptp. pxjgasnccxheip tdigeo araf cinz tqez. tqef snnleo xgpteao tn tqat gejsehteohqxso nc hifutnjiauqf, tqe hxuqei. hxuqeip hndso ae uixgteo hqeausf ng apxgjse pqeet nc uauei ago oxptixadteo rxtq eape. pehiehf rap aapeo dungkaixaase lefp, pn hautdie nc tqe jegeias pfptez ago ekeg nc nge nc tqelefp rndso gnt hnzuinzxpe ass ag aizf'p pehiet zeppajep. pnsdtxngprndso ae uiekegteo af iauxo lef hqagjep. hxuqeip reie xoeas cni aattse-mnge zeppajep, ago tqe cxipt nc tqe znoeig raip, tqe azeixhag hxkxs rai,dpeo tqez cni edpt tqat. tqdp rap anig a ger jegie xg hifutnjiauqf: tqecxeso hxuqei.

So I have many appearances of the “tQe” since the word “the” is very used in English alphabet I conclude that **Q → h** next I also look at the “Xt” word we could assume it is “a” with “at”. But since we have letter a and as a word from 1 letter in English is used just “a” it can’t be. So the second must me “i” and the word “it”, so **X → i**

the tesejiauh zaoe hifutnjiauhf rhat it ip tnoaf. pazdes c. a. znipepegt "rhat hath jno rindjht!" ig 1844. the geyt feai hip sarfei agouinzntingas ajegt, ciaghip n. e. pzith, udasipheo a hnzzeihias hnoeegtitseo the pehiet hniiepungoigj knhaadsaif; aoauteo cni dpe tn znipe'pesehtin-zajgetih tesejiauh, ig rhnpe uiecahe he oehsaieo that "pehiehf ighniiepungoeghe, ip cai the znpt izunitagt hngpioeiating." thip rapuinkioeo af a pdueieghiuheizegt.ap the znpt eyhitigj igkegting nc the ciipt hasc nc the hegtdif, thetesejiauh ptiiieo ap zdhh igteiept ig itp oaf ap pudtgil oio ig itp. thejieat ago rioesf cest geeo cni pehiehf aralegeo the sategt igteiept ighiuheip that pn zagf uenuse peez tn hake, ago ligoseo a ger igteiept igzagf ntheip. onmegp nc ueipngp attezuteo tn oieaz du theii nrgdgaiealaase hiuheip. theii hngtiiadtingp egiihheo it rith onmegp nc gerhiuhei pfptezp.ap adpigeppzeg ago the udasih dpeo the tesejiauh znie ago znie,thef cndgo that theii ceaip aandt sahl nc uiikahf reie eyajjeiateo. thehseilp oeast izueipngassf rith the zeppajep. the tesejiauh hnzuagiepiepuehteo theii hngcioegtiasitf. ago hnzzeihias hnoep sile pzith'p, rhihhieusaheo rniop ago uhiapep af pigjse hnoerniop ni hnoe-gdzaeip tn hdt tesejiauh tnssp, accnioeo pdccihiegt pehdiitf cni znptadpigepp tiagpahtingp af pizusf uiehsdoigj ag at-pijht hnzuiehegping ncthe zeagigj. the ainleip ago tiaoeip pnng ieasimeo that the zaigaokagtaje nc thepe hnoep rap theii ehngnzf.jnkeigzegt zigiptiiep dpeo the tesejiauh, tnn. at ciipt thef zdpthake eghnoeo rith theii gnzeghsatnip. adt asthndjh pehiehf rapuaiazndgt cni thez, thef sileo the tesejiauhih ehngnzf nc a saije hnoe—epuehiassf ap thef tesejiauheo znie ago znie. pn rheg the tize aiiikeotn hnzuise a ger gnzeghsatni, thef aaagongeo that cniz, hnuieo thehnzzeihias cniz, ago uinodheo a cdss-cseojeo hnoe. the gnzeghsatniphao hao theii 1,- ni 2,000 hnoe-gdzaeip ig ziyeo nioei, adt the raiago cnieijg zigiptiiep aasleo at the eyuegpe nc oiarigj du a 50,000-egtif hnoe ig trn uaitp, ago thef hao gn uinceppingas hifutagasfptp tnraig thez nc the oagjei nc the nge-uait cnizat. thef iesieo cni pehdiitfdung pzass eoitingp, aij pacep, eytegpike seyihng (saije hnoep aie haioeitn aieal thag pzass ngep, nthei thigjp aeigj ebdas), agopdueieghiuheizegt, ietaigigj hnoegdzaeip tn cahisitate thip igpteao ncprithhigj tn hnoerniop. thip eknsdting rap eppegtiassf hnzusete af the1860p.
the saije, nge-uait hnoe hao ieusaheo the pzass, trn-uaitgnzeghsatni ig hijh-sekes zisitaif ago oiusnzatih hifutnjiauhf.zeagrhise, the tesejiauh, adthni nc thip oekesnuzegt, rap hieatigjpnzethigj ger ig rai—pijgas hnzzdgihatingp, ni knsdzigndp hnzzagoago iehnggaippaghe
zeppajep. nc hndipe pdhh zeppajep hao eyipteoaecnie, rith tnihhep, uijengp, ago hndiieip, adt ig pn iaiecieo a cniz thatthef reie gnt ekeg hasseo "pijgas hnzzdgihatingp." the tesejiauhegaaseo hnzzagoeip, cni the ciipt tize ig hiptnif, tn eyeit igptagtagendpago hngtigdndp hngtins nkei jieat zappep nc zeg puieao nkei saijeaieap.thepe tahtihas zeppajep iebdiieo uintehting: tesejiauh riiep hndso aetauueo. geithei the nso gnzeghsatni gni the ger hnoe rndso on. thefreie tnn eapf tn hautdie ig hnzaat, tnn haio tn ieippde bdihlsf agociebdegtsf tn the gdzeindp ago rioepuieao tesejiauh unptp. pijgasncciheip tdigeo araf cinz thez. thef snnleo igpteao tn that gejsehteohhiso nc hifutnjiauhf, the hiuhei. hiuheip hndso ae uiigteo hheausf ng apigjse pheet nc uauei ago oiptiiadteo rith eape. pehiehf rap aapeo dungkaiiaase lefp, pn hautdie nc the jegeias pfptez ago ekeg nc nge nc thelefp rndso gnt hnzuinzipe ass ag aizf'p pehiet zeppajep. pnsdtingprndso ae uiekegteo af iauio lef hhagjep. hiuheip reie ioeas cni aattse-mnge zeppajep, ago the ciipt nc the znoeig raip, the azeiihag

hikis rai,dpeo thez cni edpt that. thdp rap anig a ger jegie ig hifutnjiauhf: thecieso hiuhei.

Next we have the “iG” word so I assume it’s either “it” or “in” but since we have this word and a number afterwards I assume it must be “in”. Since it is most used in English speaking, so **G →n.** Now since G is n, we get the word “aGO” or “anO” so I conclude that “O” may be “D” because this what is used in English so **O →d**

text: the tesejiauh zade hifutnjiauhf rhat it ip tndaf. pazdes c. a. znipepent "rhat hath jnd rindjht!" in 1844. the neyt feai hip sarfei anduinzntinnas ajent, cianhip n. e. pzith, udasiphed a hnzzeihias hndeentitsed the pehiet hniiepunndinj knhaadsaif; adauted cni dpe tn znipe'pesehtin-zajnetih tesejiauh, in rhnpe uiecahe he dehsaied that "pehiehf inhniiepunndenhe, ip cai the znpt izunitant hnnpideiatinn." thip rapuinkided af a pdueienhiuheizent.ap the znpt eyhitinj inkentinn nc the ciipt hasc nc the hentdif, thetesejiauh ptiiied ap zdhh inteiept in itp daf ap pudtnil did in itp. thejieat and ridesf cest need cni pehiehf aralened the satent inteiept inhiuheip that pn zanf uenuse peez tn hake, and lindsed a ner inteiept inzanf ntheip. dnmenp nc ueipnnp attezuted tn dieaz du theii nrndnaiealaase hiuheip. theii hnntiiadtinnp eniihhed it rith dnmenp nc nerhiuhei pfptezp.ap adpineppzen and the udasih dped the tesejiauh znie and znie,thef cndnd that theii ceaip aandt sahl nc uiikahf reie eyajjeiated. thehseilp deast izueipnnassf rith the zeppajep. the tesejiauh hnzuaniepiepuehted theii hnncidentiasitf. and hnzzeihias hndep sile pzith'p, rhihhieusahed rnidp and uhiapep af pinjse hndernidp ni hnde-ndzaeip tn hdt tesejiauh tnssp, accnided pdccihient pehdiitf cni znptadpinepp tianpahtinnp af pizusf uiehsddinj an at-pijht hnzuiehenpinn ncthe zeaninj. the ainleip and tiadeip pnnn ieasimed that the zainadkantaje nc thepe hndep rap theii ehnnnzf.jnkeinzent ziniptiiep dped the tesejiauh, tnn. at ciipt thef zdpthake enhnded rith theii nnzenhsatnip. adt asthndjh pehiehf rapuaiazndnt cni thez, thef siled the tesejiauhih ehnnnzf nc a saije hnde—epuehiassf ap thef tesejiauhed znie and znie. pn rhen the tize aiiikedtn hnzuise a ner nnzenhsatni, thef aaandnned that cniz, hnuied thehnzzeihias cniz, and uinddhed a cdss-csedjed hnde. the nnzenhsatniphad had theii 1,- ni 2,000 hnde-ndzaeip in ziyed nidei, adt the raiand cnieijn ziniptiiep aasled at the eyuenpe nc diarinj du a 50,000-entif hnde in trn uaitp, and thef had nn uinceppinnas hifutanasfptp tnrain thez nc the danjei nc the nne-uait cnizat. thef iesied cni pehdiitfdunn pzass editinnp, aij pacep, eytenpike seyihnn (saije hndep aie haideitn aieal than pzass nnep, nthei thinjp aeinj ebdas), andpdueienhiuheizent, ietaininj hndendzaeip tn cahisitate thip inptead ncprithhinj tn hndernidp. thip eknsdtinn rap eppentiassf hnzusete af the1860p.
the saije, nne-uait hnde had ieusahed the pzass, trn-uaitnnzenhsatni in hijh-sekes zisitaif and diusnzatih hifutnjiauhf.zeanrhise, the tesejiauh, adthni nc thip dekesnuzent, rap hieatinjpnzethinj ner in rai—pijnas hnzzdnihatinnp, ni knsdzinndp hnzzandand iehnnnaippanhe
zeppajep. nc hndipe pdhh zeppajep had eyiptedaecnie, rith tnihhep, uijennp, and hndiieip, adt in pn iaiecied a cniz thatthef reie nnt eken hassed "pijnas hnzzdnihatinnp." the tesejiauhenaased hnzzandeip, cni the ciipt tize in hiptnif, tn eyeit inptantanendpand hnntindndp hnntins nkei jieat zappep nc zen puiead nkei saijeaieap.thepe tahtihas zeppajep

iebdiied uintehtinn: tesejiauh riiep hndsd aetauued. neithei the nsd nnzenhsatni nni the ner hnde rndsd dn. thefreie tnn eapf tn hautdie in hnzaat, tnn haid tn ieippde bdihlsf andciebdentsf tn the ndzeindp and ridepuiead tesejiauh unptp. pijnasncciheip tdined araf cinz thez. thef snnled inptead tn that nejsehtedhhisd nc hifutnjiauhf, the hiuhei. hiuheip hndsd ae uiinted hheausf nn apinjse pheet nc uauei and diptiiadted rith eape. pehiehf rap aaped dunnkaiiaase lefp, pn hautdie nc the jeneias pfptez and eken nc nne nc thelefp rndsd nnt hnzuinzipe ass an aizf'p pehiet zeppajep. pnsdtinnprndsd ae uiekented af iauid lef hhanjep. hiuheip reie ideas cni aattse-mnne zeppajep, and the ciipt nc the zndein raip, the azeiihan hikis rai,dped thez cni edpt that. thdp rap anin a ner jenie in hifutnjiauhf: theciesd hiuhei.

Now above I have the word “theiI” so I conclude it must be “their” so **I → r**. Also at the start I have the word “itP” so it could be “its”, so **P → s.** The “tN” must be the word “to” so **N →o**

After we apply it:

the tesejrauh zade hrfutnjrauhf rhat it is tndaf. sazdes c. a. znrsesent "rhat hath jnd rrndjht!" in 1844. the neyt fear his sarfer andurnzntinnas ajent, cranhis n. e. szith, udasished a hnzzerhias hndeentitsed the sehret hnrresunndinj knhaadsarf; adauted cnr dse tn znrse'sesehtrn-zajnetih tesejrauh, in rhnse urecahe he dehsared that "sehrehf inhnrresunndenhe, is car the znst izunrtant hnnsideratinn." this rasurnkided af a sduerenhiuherzent.as the znst eyhitinj inkentinn nc the cirst hasc nc the hentdrf, thetesejrauh stirred as zdhh interest in its daf as sudtnil did in its. thejreat and ridesf cest need cnr sehrehf aralened the satent interest inhiuhers that sn zanf uenuse seez tn hake, and lindsed a ner interest inzanf nthers. dnmens nc uersnns attezuted tn dreaz du their nrndnarealaase hiuhers. their hnntriadtinns enrihhed it rith dnmens nc nerhiuher sfstezs.as adsinesszen and the udasih dsed the tesejrauh znre and znre,thef cndnd that their cears aandt sahl nc urikahf rere eyajjerated. thehserls deast izuersnnassf rith the zessajes. the tesejrauh hnzuaniesresuehted their hnncidentiasitf. and hnzzerhias hndes sile szith's, rhihhreusahed rnrds and uhrases af sinjse hndernrds nr hnde-ndzaers tn hdt tesejrauh tnsss, accnrded sdccihient sehdritf cnr znstadsiness transahtinns af sizusf urehsddinj an at-sijht hnzurehensinn ncthe zeaninj. the arnlers and traders snnn reasimed that the zainadkantaje nc these hndes ras their ehnnnzf.jnkernzent zinistries dsed the tesejrauh, tnn. at cirst thef zdsthake enhnded rith their nnzenhsatnrs. adt asthndjh sehrehf rasuarazndnt cnr thez, thef siled the tesejrauhih ehnnnzf nc a sarje hnde—esuehiassf as thef tesejrauhed znre and znre. sn rhen the tize arrikedtn hnzuise a ner nnzenhsatnr, thef aaandnned that cnrz, hnuied thehnzzerhias cnrz, and urnddhed a cdss-csedjed hnde. the nnzenhsatnrshad had their 1,- nr 2,000 hnde-ndzaers in ziyed nrder, adt the rarand cnreijn zinistries aasled at the eyuense nc drarinj du a 50,000-entrf hnde in trn uarts, and thef had nn urncessinnas hrfutanasfsts tnrarn thez nc the danjer nc the nne-uart cnrzat. thef resied cnr sehdritfdunn szass editinns, aij saces, eytensike seyihnn (sarje hndes are hardertn areal than szass nnes, nther thinjs aeinj ebdas), andsduerenhiuherzent, retaininj hndendzaers tn cahisitate this instead ncsrithhinj tn hndernrds. this eknsdtinn ras essentiassf hnzusete af the1860s. the sarje, nne-uart hnde had reusahed the szass, trn-uartnnzenhsatnr in hijh-sekes zisitarf and

diusnzatih hrfutnjrauhf.zeanrhise, the tesejrauh, adthnr nc this dekesnuzent, ras hreatinjsnzethinj ner in rar—sijnas hnzzdnihatinns, nr knsdzinnds hnzzandand rehnnnaissanhe
zessajes. nc hndrse sdhh zessajes had eyistedaecnre, rith tnrhhes, uijenns, and hndriers, adt in sn rarecied a cnrz thatthef rere nnt eken hassed "sijnas hnzzdnihatinns." the tesejrauhenaased hnzzanders, cnr the cirst tize in histnrf, tn eyert instantanendsand hnntindnds hnntrns nker jreat zasses nc zen suread nker sarjeareas.these tahtihas zessajes rebdired urntehtinn: tesejrauh rires hndsd aetauued. neither the nsd nnzenhsatnr nnr the ner hnde rndsd dn. thefrere tnn easf tn hautdre in hnzaat, tnn hard tn reissde bdihlsf andcrebdentsf tn the ndzernds and ridesuread tesejrauh unsts. sijnasnccihers tdrned araf crnz thez. thef snnled instead tn that nejsehtedhhisd nc hrfutnjrauhf, the hiuher. hiuhers hndsd ae urinted hheausf nn asinjse sheet nc uauer and distriadted rith ease. sehrehf ras aased dunnkariaase lefs, sn hautdre nc the jeneras sfstez and eken nc nne nc thelefs rndsd nnt hnzurnzise ass an arzf's sehret zessajes. snsdtinnsrndsd ae urekented af rauid lef hhanjes. hiuhers rere ideas cnr aattse-mnne zessajes, and the cirst nc the zndern rars, the azerihan hikis rar,dsed thez cnr edst that. thds ras anrn a ner jenre in hrfutnjrauhf: theciesd hiuher.

After we apply it we see the ‘oC’ appearance ot could be “on” or ‘of’ since ‘n’ we already have it must be of. So **C → f.** Also I have the “Ae” so the best word for it is “be”, so **A → b.** Also we have the word “Rhen” and the bests match is “Then” or “When”, since we have already T, then **R → W.**

the tesejrauh zade hrfutnjrauhf rhat it is tndaf. sazdes f. b. znrsesent "rhat hath jnd rrndjht!" in 1844. the neyt fear his sarfer andurnzntinnas ajent, franhis n. e. szith, udbsished a hnzzerhias hndeentitsed the sehret hnrresunndinj knhabdsarf; adauted fnr dse tn znrse'sesehtrn-zajnetih tesejrauh, in rhnse urefahe he dehsared that "sehrehf inhnrresunndenhe, is far the znst izunrtant hnnsideratinn." this rasurnkided bf a sduerenhiuherzent.as the znst eyhitinj inkentinn nf the first hasf nf the hentdrf, thetesejrauh stirred as zdhh interest in its daf as sudtnil did in its. thejreat and ridesf fest need fnr sehrehf aralened the satent interest inhiuhers that sn zanf uenuse seez tn hake, and lindsed a ner interest inzanf nthers. dnmens nf uersnns attezuted tn dreaz du their nrndnbrealabse hiuhers. their hnntribdtinns enrihhed it rith dnmens nf nerhiuher sfstezs.as bdsinesszen and the udbsih dsed the tesejrauh znre and znre,thef fndnd that their fears abndt sahl nf urikahf rere eyajjerated. thehserls deast izuersnnassf rith the zessajes. the tesejrauh hnzuaniesresuehted their hnnfidentiasitf. and hnzzerhias hndes sile szith's, rhihhreusahed rnrds and uhrases bf sinjse hndernrds nr hnde-ndzbers tn hdt tesejrauh tnsss, affnrded sdffihient sehdritf fnr znstbdsiness transahtinns bf sizusf urehsddinj an at-sijht hnzurehensinn nfthe zeaninj. the brnlers and traders snnn reasimed that the zainadkantaje nf these hndes ras their ehnnnzf.jnkernzent zinistries dsed the tesejrauh, tnn. at first thef zdsthake enhnded rith their nnzenhsatnrs. bdt asthndjh sehrehf rasuarazndnt fnr thez, thef siled the tesejrauhih ehnnnzf nf a sarje hnde—esuehiassf as thef tesejrauhed znre and znre. sn rhen the tize arrikedtn hnzuise a ner nnzenhsatnr, thef abandnned that fnrz, hnuied thehnzzerhias fnrz, and urnddhed a fdss-fsedjed hnde. the nnzenhsatnrshad

had their 1,- nr 2,000 hnde-ndzbers in ziyed nrder, bdt the rarand fnreijn zinistries basled at the eyuense nf drarinj du a 50,000-entrf hnde in trn uarts, and thef had nn urnfessinnas hrfutanasfsts tnrarn thez nf the danjer nf the nne-uart fnrzat. thef resied fnr sehdritfdunn szass editinns, bij safes, eytensike seyihnn (sarje hndes are hardertn breal than szass nnes, nther thinjs beinj ebdas), andsduerenhiuherzent, retaininj hndendzbers tn fahisitate this instead nfsrithhinj tn hndernrds. this eknsdtinn ras essentiassf hnzusete bf the1860s. the sarje, nne-uart hnde had reusahed the szass, trn-uartnnzenhsatnr in hijh-sekes zisitarf and diusnzatih hrfutnjrauhf.zeanrhise, the tesejrauh, adthnr nf this dekesnuzent, ras hreatinjsnzethinj ner in rar—sijnas hnzzdnihatinns, nr knsdzinnds hnzzandand rehnnnaissanhe zessajes. nf hndrse sdhh zessajes had eyistedbefnre, rith tnrhhes, uijenns, and hndriers, bdt in sn rarefied a fnrz thatthef rere nnt eken hassed "sijnas hnzzdnihatinns." the tesejrauhenabsed hnzzanders, fnr the first tize in histnrf, tn eyert instantanendsand hnntindnds hnntrns nker jreat zasses nf zen suread nker sarjeareas.these tahtihas zessajes rebdired urntehtinn: tesejrauh rires hndsd betauued. neither the nsd nnzenhsatnr nnr the ner hnde rndsd dn. thefrere tnn easf tn hautdre in hnzbat, tnn hard tn reissde bdihlsf andfrebdentsf tn the ndzernds and ridesuread tesejrauh unsts. sijnasnffihers tdrned araf frnz thez. thef snnled instead tn that nejsehtedhhisd nf hrfutnjrauhf, the hiuher. hiuhers hndsd be urinted hheausf nn asinjse sheet nf uauer and distribdted rith ease. sehrehf ras based dunnkariabse lefs, sn hautdre nf the jeneras sfstez and eken nf nne nf thelefs rndsd nnt hnzurnzise ass an arzf's sehret zessajes. snsdtinnsrndsd be urekented bf rauid lef hhanjes. hiuhers rere ideas fnr battse-mnne zessajes, and the first nf the zndern rars, the azerihan hikis rar,dsed thez fnr edst that. thds ras bnrn a ner jenre in hrfutnjrauhf: thefiesd hiuher.

Now most of the words we can guess: Like the “theF” and “bF”, we can say **F → y.** Also we have the word “Lnow” so **L → k.** Also we have the word “theZ” so **Z → m.**

And we have:

the tesejrauh made hrfutnjrauhf what it is tndaf. samdes f. b. mnrsesent "what hath jnd wrndjht!" in 1844. the neyt fear his sawfer andurnmntinnas ajent, franhis n. e. smith, udbsished a hnmmerhias hndeentitsed the sehret hnrresunndinj knhabdsarf; adauted fnr dse tn mnrse'sesehtrn-majnetih tesejrauh, in whnse urefahe he dehsared that "sehrehf inhnrresunndenhe, is far the mnst imunrtant hnnsideratinn." this wasurnkided bf a sduerenhiuherment.as the mnst eyhitinj inkentinn nf the first hasf nf the hentdrf, thetesejrauh stirred as mdhh interest in its daf as sudtnik did in its. thejreat and widesf fest need fnr sehrehf awakened the satent interest inhiuhers that sn manf uenuse seem tn hake, and kindsed a new interest inmanf nthers. dnmens nf uersnns attemuted tn dream du their nwndnbreakabse hiuhers. their hnntribdtinns enrihhed it with dnmens nf newhiuher sfstems.as bdsinessmen and the udbsih dsed the tesejrauh mnre and mnre,thef fndnd that their fears abndt sahk nf urikahf were eyajjerated. thehserks deast imuersnnassf with the messajes. the tesejrauh hnmuaniesresuehted their hnnfidentiasitf. and hnmmerhias hndes sike smith's, whihhreusahed wnrds and uhrases bf sinjse hndewnrds nr hnde-ndmbers tn hdt tesejrauh

tnsss, affnrded sdffihient sehdritf fnr mnstbdsiness transahtinns bf simusf urehsddinj an

at-sijht hnmurehensinn nfthe meaninj. the brnkers and traders snnn reasimed that the mainadkantaje nf these hndes was their ehnnnmf.jnkernment ministries dsed the tesejrauh, tnn. at first thef mdsthake enhnded with their nnmenhsatnrs. bdt asthndjh sehrehf wasuaramndnt fnr them, thef siked the tesejrauhih ehnnnmf nf a sarje hnde—esuehiassf as thef tesejrauhed mnre and mnre. sn when the time arrikedtn hnmuise a new nnmenhsatnr, thef abandnned
that fnrm, hnuied thehnmmerhias fnrm, and urnddhed a fdss-fsedjed hnde. the nnmenhsatnrshad
had their 1,- nr 2,000 hnde-ndmbers in miyed nrder, bdt the warand fnreijn ministries basked at
the eyuense nf drawinj du a 50,000-entrf hnde in twn uarts, and thef had nn urnfessinnas hrfutanasfsts tnwarn them nf the danjer nf the nne-uart fnrmat. thef resied fnr sehdritfdunn smass editinns, bij safes, eytensike seyihnn (sarje hndes are hardertn break than smass nnes, nther thinjs beinj ebdas), andsduerenhiuherment, retaininj hndendmbers tn fahisitate this instead nfswithhinj tn hndewnrds. this eknsdtinn was essentiassf hnmusete bf the1860s.
the sarje, nne-uart hnde had reusahed the smass, twn-uartnnmenhsatnr in hijh-sekes misitarf and
diusnmatih hrfutnjrauhf.meanwhise, the tesejrauh, adthnr nf this dekesnument, was hreatinjsnmethinj new in war—sijnas hnmmdnihatinns, nr knsdminnds hnmmandand rehnnnaissanhe
messajes. nf hndrse sdhh messajes had eyistedbefnre, with tnrhhes, uijenns, and hndriers, bdt in sn rarefied a fnrm thatthef were nnt eken hassed "sijnas hnmmdnihatinns." the tesejrauhenabsed hnmmanders, fnr the first time in histnrf, tn eyert instantanendsand hnntindnds hnntrns nker jreat masses nf men suread nker sarjeareas.these tahtihas messajes rebdired urntehtinn: tesejrauh wires hndsd betauued. neither the nsd nnmenhsatnr nnr the new hnde wndsd dn. thefwere tnn easf tn hautdre in hnmbat, tnn hard tn reissde bdihksf andfrebdentsf tn the ndmernds and widesuread tesejrauh unsts. sijnasnffihers tdrned awaf frnm them. thef snnked instead tn that nejsehtedhhisd nf hrfutnjrauhf, the hiuher. hiuhers hndsd be urinted hheausf nn asinjse sheet nf uauer and distribdted with ease. sehrehf was based dunnkariabse kefs, sn hautdre nf the jeneras sfstem and eken nf nne nf thekefs wndsd nnt hnmurnmise ass an armf's sehret messajes. snsdtinnswndsd be urekented bf rauid kef hhanjes. hiuhers were ideas fnr battse-mnne messajes, and the first nf the mndern wars, the amerihan hikis war,dsed them fnr edst that. thds was bnrn a new jenre in hrfutnjrauhf: thefiesd hiuher.

Now we can find the word “eKen” can be “even”, so **K → v.**
And the word “tN”, so **N→o** , “messajes”, so **J → g,** “mDst” so **D → u**

the tesegrauh made hrfutograuhf what it is todaf. samues f. b. morsesent "what hath god wrought!" in 1844. the neyt fear his sawfer anduromotionas agent, franhis o. e. smith, uubsished a hommerhias hodeentitsed the sehret horresuonding vohabusarf; adauted for use to morse'sesehtro-magnetih tesegrauh, in whose urefahe he dehsared that "sehrehf inhorresuondenhe, is far the most imuortant honsideration." this wasurovided bf a suuerenhiuherment.as the most eyhiting invention of the first hasf of the henturf,
thetesegrauh stirred as muhh interest in its daf as suutnik did in its. thegreat and widesf fest need for sehrehf awakened the satent interest inhiuhers that so manf ueouse seem to have, and kindsed a new interest inmanf others. domens of uersons attemuted to dream uu their ownunbreakabse hiuhers. their hontributions enrihhed it with domens of newhiuher sfstems.as businessmen and the uubsih used the tesegrauh more and more,thef found that their fears about sahk of urivahf were eyaggerated. thehserks deast imuersonassf with the messages. the tesegrauh homuaniesresuehted their honfidentiasitf. and hommerhias hodes sike smith's, whihhreusahed words and uhrases bf singse hodewords or hode-numbers to hut tesegrauh tosss, afforded suffihient sehuritf for mostbusiness transahtions bf simusf urehsuding an at-sight homurehension ofthe meaning. the brokers and traders soon reasimed that the mainadvantage of these hodes was their ehonomf.government ministries used the tesegrauh, too. at first thef musthave enhoded with their nomenhsators. but asthough sehrehf wasuaramount for them, thef siked the tesegrauhih ehonomf of a sarge hode—esuehiassf as thef tesegrauhed more and more. so when the time arrivedto homuise a new nomenhsator, thef abandoned that form, houied thehommerhias form, and uroduhed a fuss-fsedged hode. the nomenhsatorshad had their 1,- or 2,000 hode-numbers in miyed order, but the warand foreign ministries basked at the eyuense of drawing uu a 50,000-entrf hode in two uarts, and thef had no urofessionas hrfutanasfsts towarn them of the danger of the one-uart format. thef resied for sehuritfuuon smass editions, big safes, eytensive seyihon (sarge hodes are harderto break than smass ones, other things being ebuas), andsuuerenhiuherment, retaining hodenumbers to fahisitate this instead ofswithhing to hodewords. this evosution was essentiassf homusete bf the1860s.
the sarge, one-uart hode had reusahed the smass, two-uartnomenhsator in high-seves misitarf and diusomatih hrfutograuhf.meanwhise, the tesegrauh, author of this devesoument, was hreatingsomething new in war—signas hommunihations, or vosuminous hommandand rehonnaissanhe messages. of hourse suhh messages had eyistedbefore, with torhhes, uigeons, and houriers, but in so rarefied a form thatthef were not even hassed "signas hommunihations." the tesegrauhenabsed hommanders, for the first time in historf, to eyert instantaneousand hontinuous hontros over great masses of men suread over sargeareas.these tahtihas messages rebuired urotehtion: tesegrauh wires housd betauued. neither the osd nomenhsator nor the new hode wousd do. thefwere too easf to hauture in hombat, too hard to reissue buihksf andfrebuentsf to the numerous and widesuread tesegrauh uosts. signasoffihers turned awaf from them. thef sooked instead to that negsehtedhhisd of hrfutograuhf, the hiuher. hiuhers housd be urinted hheausf on asingse sheet of uauer and distributed with ease. sehrehf was based uuonvariabse kefs, so hauture of the generas sfstem and even of one of thekefs wousd not homuromise ass an armf's sehret messages. sosutionswousd be urevented bf rauid kef hhanges. hiuhers were ideas for battse-mone messages, and the first of the modern wars, the amerihan hivis war,used them for eust that. thus was born a new genre in hrfutograuhf: thefiesd hiuher.

“Hode”, “Hodewords” ,“Hombat“ so **H → c.**
“couSd”, “wouSd” so **S→ l.**
“diUlomatic” so **U→ p.**

the telegraph made cryptography what it is today. samuel f. b. morsesent "what hath god wrought!" in 1844. the neyt year his lawyer andpromotional agent, francis o. e. smith, published a commercial codeentitled the secret corresponding vocabulary; adapted for use to morse'selectro-magnetic telegraph, in whose preface he declared that "secrecy incorrespondence, is far the most important consideration." this wasprovided by a superencipherment.as the most eyciting invention of the first half of the century, thetelegraph stirred as much interest in its day as sputnik did in its. thegreat and widely felt need for secrecy awakened the latent interest inciphers that so many people seem to have, and kindled a new interest inmany others. domens of persons attempted to dream up their ownunbreakable ciphers. their contributions enriched it with domens of newcipher systems.as businessmen and the public used the telegraph more and more, they found that their fears about lack of privacy were eyaggerated. theclerks dealt impersonally with the messages. the telegraph companiesrespected their confidentiality. and commercial codes like smith's, whichreplaced words and phrases by single codewords or code-numbers to cut telegraph tolls, afforded sufficient security for mostbusiness transactions by simply precluding an at-sight comprehension ofthe meaning. the brokers and traders soon realimed that the mainadvantage of these codes was their economy. government ministries used the telegraph, too. at first they musthave encoded with their nomenclators. but although secrecy wasparamount for them, they liked the telegraphic economy of a large code—especially as they telegraphed more and more. so when the time arrivedto compile a new nomenclator, they abandoned that form, copied thecommercial form, and produced a full-fledged code. the nomenclatorshad had their 1,- or 2,000 code-numbers in miyed order, but the warand foreign ministries balked at the eypense of drawing up a 50,000-entry code in two parts, and they had no professional cryptanalysts towarn them of the danger of the one-part format. they relied for securityupon small editions, big safes, eytensive leyicon (large codes are harderto break than small ones, other things being ebual), andsuperencipherment, retaining codenumbers to facilitate this instead ofswitching to codewords. this evolution was essentially complete by the1860s. the large, one-part code had replaced the small, two-partnomenclator in high-level military and diplomatic cryptography.meanwhile, the telegraph, author of this development, was creatingsomething new in war—signal communications, or voluminous commandand reconnaissance messages. of course such messages had eyistedbefore, with torches, pigeons, and couriers, but in so rarefied a form thatthey were not even called "signal communications." The telegraphenabled commanders, for the first time in history, to eyert instantaneousand continuous control over great masses of men spread over largeareas.these tactical messages rebuired protection: telegraph wires could betapped. neither the old nomenclator nor the new code would do. theywere too easy to capture in combat, too hard to reissue buickly andfrebuently to the numerous and widespread telegraph posts. signalofficers turned away from them. they looked instead to that neglectedchild of cryptography, the cipher. ciphers could be printed cheaply on asingle sheet of paper and distributed with ease.

secrecy was based uponvariable keys, so capture of the general system and even of one of thekeys would not compromise all an army's secret messages. solutionswould be prevented by rapid key changes. ciphers were ideal for battle-mone messages, and the first of the modern wars, the American civil war,used them for eust that. thus was born a new genre in cryptography: thefield cipher.

Now only 4 letters remain not substituted “B”, “E”, “M”, “Y”
“eYstedbefore” so **Y → x.**
“battle-mone” so **M → z.**
“Eust” so **E → j.**
“eBual” so **B → q.**
And the Full text is :

the telegraph made cryptography what it is today. samuel f. b. morsesent "what hath god wrought!" in 1844. the next year his lawyer andpromotional agent, francis o. e. smith, published
a commercial codeentitled the secret corresponding vocabulary; adapted for use to morse'selectro-magnetic telegraph, in whose preface he declared that "secrecy incorrespondence, is far the most important consideration." this wasprovided by a superencipherment.as the most exciting invention of the first half of the century, thetelegraph stirred as much interest in its day as sputnik did in its. thegreat and widely felt need for secrecy awakened the latent interest inciphers that so many people seem to have, and kindled a new interest inmany others. dozens of persons attempted to dream up their ownunbreakable ciphers. their contributions enriched it with dozens of newcipher systems.as businessmen and the public used the telegraph more and more,they found that their fears about lack of privacy were exaggerated. theclerks dealt impersonally with the messages. the telegraph companiesrespected their confidentiality. and commercial codes like smith's, whichreplaced words and phrases by single codewords or code-numbers to cut telegraph
tolls, afforded sufficient security for mostbusiness transactions by simply precluding an at-sight comprehension ofthe meaning. the brokers and traders soon realized that the mainadvantage of these codes was their economy.government ministries used the telegraph, too. at first they musthave encoded with their nomenclators. but although secrecy wasparamount for them, they liked the telegraphic economy of a large code—especially as they telegraphed more and more. so when the time arrivedto compile a new nomenclator, they abandoned
that form, copied thecommercial form, and produced a full-fledged code. the nomenclatorshad had their 1,- or 2,000 code-numbers in mixed order, but the warand foreign ministries balked at
the expense of drawing up a 50,000-entry code in two parts, and they had no professional cryptanalysts towarn them of the danger of the one-part format. they relied for securityupon small editions, big safes, extensive lexicon (large codes are harderto break than small ones,

other things being equal), andsuperencipherment, retaining codenumbers to facilitate this instead ofswitching to codewords. this evolution was essentially complete by the1860s. the large, one-part code had replaced the small, two-partnomenclator in high-level military and diplomatic cryptography.meanwhile, the telegraph, author of this development, was creatingsomething new in war—signal communications, or voluminous commandand reconnaissance messages. of course such messages had existedbefore, with torches, pigeons, and couriers, but in so rarefied a form thatthey were not even called "signal communications." the telegraphenabled commanders, for the first time in history, to exert instantaneousand continuous control over great masses of men spread over largeareas.these tactical messages required protection: telegraph wires could betapped. neither the old nomenclator nor the new code would do. theywere too easy to capture in combat, too hard to reissue quickly andfrequently to the numerous and widespread telegraph posts. signalofficers turned away from them. they looked instead to that neglectedchild of cryptography, the cipher. ciphers could be printed cheaply on asingle sheet of paper and distributed with ease. secrecy was based uponvariable keys, so capture of the general system and even of one of thekeys would not compromise all an army's secret messages. solutionswould be prevented by rapid key changes. ciphers were ideal for battle-zone messages, and the first of the modern wars, the american civil war,used them for eust that. thus was born a new genre in cryptography: thefield cipher.

Visual Implementation: