

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: Martiniuc Artiom FAF-222,

Checked: Dumitru Nirca asist. univ.,

Chișinău 2024

## Topic: Mono-alphabetic Cipher

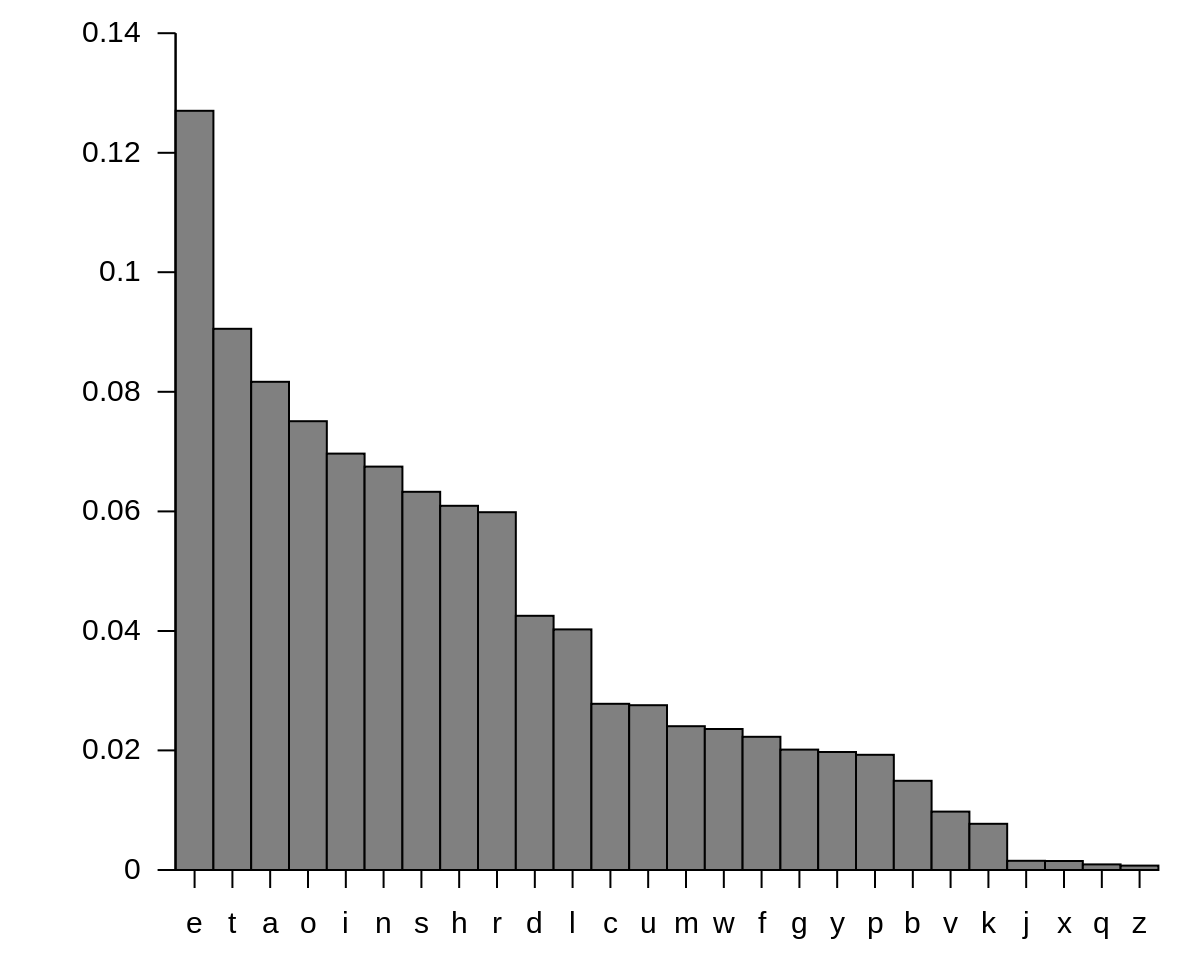
## Tasks:

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

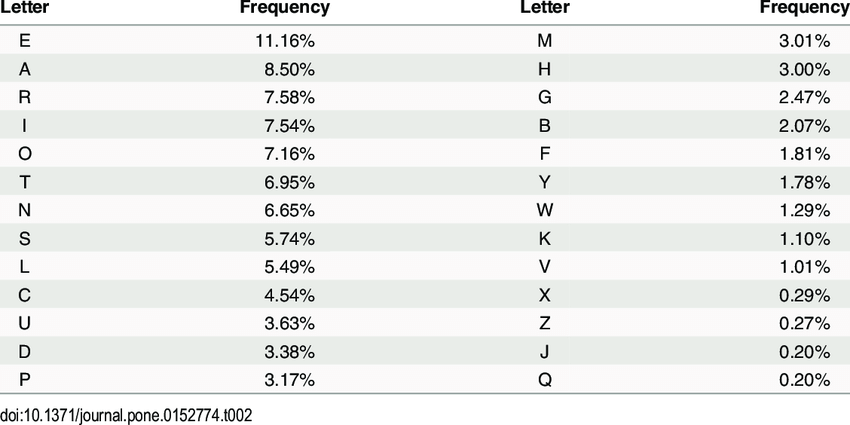
## Theoretical notes:

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

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



**Fig.1**: English letter frequency

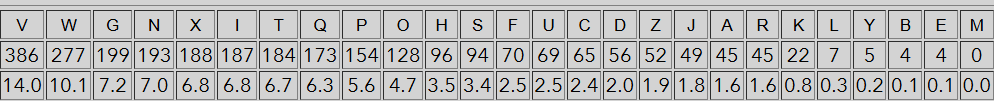


**Fig.2**: English letter frequency(Table)

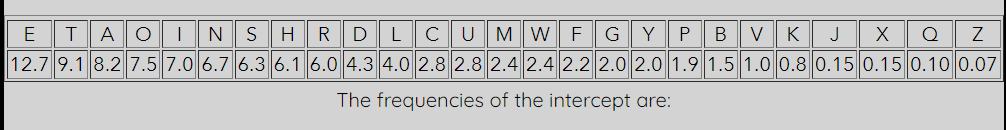
**Implementation(Var. Nr.13)**

I have a cryptogram c = *Vgjstgo, wnn, qto xwp asthl hqtzavi. Xw avjtg rxwq wqv hifuwtgtsfwxhvgovtknip nc Enqg Rtssxp, wqv jivtwvpw Vgjsxpq ztwqvztwxhxtg avcnivGvrwng. Tcwvi qxp ovtwq, xw ovphvgovo wqindjq qxp jitgopng wn ivthq, ngZtf 14, 1716, Vortio Rxssvp, t 22-fvti-nso zxgxpwvi tw Nixvs Hnssvjv,Nycnio.Rxssvp vzatilvo tw nghv dung t htivvi dgxbdv xg wqv tggtsp nchifuwnsnjf tgo wqv hqdihq. Qv gnw ngsf ztgtjvo wn ivhnghxsv qxpivsxjxndp htssxgj rxwq tg thwxkxwf nghv hngovzgvo af hqdihqsftdwqnixwxvp, adw tspn rvgw ng wn avhnzv wqv ngsf ztg xg qxpwnif wn dpvhifuwtgtsfwxh wtsvgwp wn uinhdiv vhhsvpxtpwxhts ivrtiop. Rxwqxg wrn fvtip,qv qto avvg gtzvo ivhwni nc Atiwng, Avocniopqxiv, cni pnskxgj zniv wqtg300 utjvp nc hxuqvi wqtw vyunpvo Prvovg'p twwvzuw wn cnzvgw tg duixpxgj xg Vgjstgo. Qv kxiwdtssf jdtitgwvvo qxpcdwdiv rqvg qv wvpwxcxvo avcniv wqv Qndpv nc Sniop xg 1723. Qviv, CitghxpTwwviadif, Axpqnu nc Inhqvpwvi, rtp avxgj wixvo af qxp uvvip cnitwwvzuwxgj wn pvw t uivwvgovi ng wqv Vgjsxpq wqingv.Wqv uivwvgovi'p htdpv vyqniwvo wqv tssvjxtghv nc ztgf xg Vgjstgo,tgo wqv gtwxng'p twwvgwxng cnhdpvo ng Twwviadif'p wixts. Znpw nc wqv cthwptandw wqv tssvjvo hngpuxithf qto hnzv cinz qxp xgwvihvuwvohniivpungovghv, tgo wqv znpw xghdsutwnif vkxovghv qto avvg vywithwvocinz wqv uniwxngp xg hxuqvi af Rxssvp tgo af Tgwqngf Hniaxviv, t cnizvicnivxjg pvikxhv nccxhxts xg qxp zxo-wqxiwxvp rqn qto tspn avvg tuunxgwvo tOvhfuqvivi xg 1719. Wqv Sniop "wqndjqw xw uinuvi wn htss wqv Ovhfuqvivipavcniv wqvz, xg niovi wn wqvxi avxgj ptwxpcxvo nc wqv Widwq nc wqvOvhfuqvixgj." Wn ovzngpwitwv wqxp, Rxssvp tgo Hniaxviv ovunpvo, Wqtw pvkvits Svwwvip, rixwwvg xg wqxp Hfuqvi, qto avvgovhfuqvivo af wqvz pvutitwvsf, ngv avxgj ztgf Zxsvp oxpwtgw xgwqv Hndgwif, tgo wqv nwqvi xg Wnrg; tgo fvw wqvxi Ovhfuqvixgjtjivvo;Wqtw Cthwp, dglgnrg wn wqvz tgo wqv Jnkvigzvgw tw wqv Wxzvnc wqvxi Ovhfuqvixgj, qto avvg kvixcxvo xg vkvif Hxihdzpwtghv afpdapvbdvgw Oxphnkvixvp Wqtw t Pduusvzvgw nc wqxp Hfuqvi, qtkxgj avvg cndgo tzngjOvggxp Lvssf'p Utuvip wqv stwwvi Vgo nc Edsf, tjivvo rxwq wqv Lvfwqvf qto cnizvo nc wqtw Hfuqvi wqv Tuixs avcniv;Wqtw wqv Ovhfuqvixgj nc wqv Svwwvip pxjgvo Engvp sssxgjwng tgo1378, avxgj tcwvirtiop tuusxvo af wqvz wn nwqvip rixwwvg xg wqvptzv Hfuqvi, oxo xzzvoxtwvsf ztlv uviwxgvgw Pvgpv, tgo pdhq tpqto tg vkxovgw Hnggvyxng tgo Hnqvivghv rxwq wqv Utiwp nc wqnpvSvwwvip wqtw rviv ndw nc Hfuqvi, wqndjq wqv Rniop xg Hfuqvi rvivivuvtwvo xg oxccvivgw Utitjituqp, tgo oxccvivgwsf hnzaxgvo. Wqv wrn Ovhfuqvivip tuuvtivo avcniv wqv Sniop ng pvkvits nhhtpxngpwn prvti wn wqvxi pnsdwxngp. Twwvgadif wrxhv naevhwvo tgo rtp wrxhv nkviidsvo. Adw ng Ztf 7, tp Rxssvp rtpwvpwxcfxgj wn wqv hifuwtgtsfpxp nc wqv wqivv znpw xghixzxgtwnif svwwvip nctss, tgo wqv axpqnu cvsw wqv gnnpv wxjqwvgxgj tindgo qxz, qv uvipxpwvo xgbdvpwxngxgj Rxssvp ng wqv ktsxoxwf nc wqv ivtoxgj wqndjq wqv Qndpv qtopduuniwvo Rxssvp' ivcdpts wn tgprvi. Qv itxpvo pdhq t hnzznwxng wqtw qvtgo qxp hndgpvs rviv niovivo wn rxwqoitr, tgo wqv Sniop knwvo dung wqvuinunpxwxng, "wqtw xw xp wqv Nuxgxng nc wqxp Qndpv wqtw xw xp gnw hngpxpwvgwrxwq wqv udasxh Ptcvwf, wn tpl wqv Ovhfuqvivip tgf Bdvpwxngp, rqxhq ztfwvgo wn oxphnkvi wqv Tiw ni Zfpwvif nc Ovhfuqvixgj." Xw rtp ivpnskvo xgwqv tccxiztwxkv, wqv pnsdwxngp rviv thhvuwvo, tgo Twwviadif, stijvsf ngwqxp vkxovghv, rtp cndgo jdxswf, ovuixkvo nc nccxhv, tgo atgxpqvo cinz wqvivtsz.*

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:



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

After inspecting the encrypted message, I began by counting the frequency of each letter in the ciphertext and comparing it with the standard English letter frequency distribution. The most frequent letters in the ciphertext were identified as potential matches for common English letters, such as **E**, **T**, **A**, **O**, etc.

* **Substituted 'E' and 'T'**: Based on frequency, I identified a letter in the ciphertext corresponding to **E** and another to **T**. This substitution was straightforward.

eGJSTGO, tNN, QTO XtP ASTHL HQTZAeI. Xt AeJTG RXtQ tQe HIFUtTGTSFtXHeGOeTKNIP NC ENQG RTSSXP,

tQe JIeTtePt eGJSXPQ ZTtQeZTtXHXTG AeCNIeGeRtNG. TCteI QXP OeTtQ, Xt OePHeGOeO tQINDJQ

QXP JITGOPNG tN IeTHQ, NGZTF 14, 1716, eORTIO RXSSeP, T 22-FeTI-NSO ZXGXPteI Tt NIXeS

HNSSeJe,NYCNIO.RXSSeP eZATILeO Tt NGHe DUNG T HTIeeI DGXBDe XG tQe TGGTSP NCHIFUtNSNJF TGO tQe

HQDIHQ. Qe GNt NGSF ZTGTJeO tN IeHNGHXSe QXPIeSXJXNDP HTSSXGJ RXtQ TG THtXKXtF NGHe HNGOeZGeO

AF HQDIHQSFTDtQNIXtXeP, ADt TSPN ReGt NG tN AeHNZe tQe NGSF ZTG XG QXPtNIF tN

DPeHIFUtTGTSFtXH tTSeGtP tN UINHDIe eHHSePXTPtXHTS IeRTIOP. RXtQXG tRN FeTIP,Qe QTO AeeG GTZeO

IeHtNI NC ATItNG, AeOCNIOPQXIe, CNI PNSKXGJ ZNIe tQTG300 UTJeP NC HXUQeI tQTt eYUNPeO PReOeG'P

TtteZUt tN CNZeGt TG DUIXPXGJ XG eGJSTGO. Qe KXItDTSSF JDTITGteeO QXPCDtDIe RQeG Qe

tePtXCXeO AeCNIe tQe QNDPe NC SNIOP XG 1723. QeIe, CITGHXPTtteIADIF, AXPQNU NC INHQePteI,

RTP AeXGJ tIXeO AF QXP UeeIP CNITtteZUtXGJ tN Pet T UIeteGOeI NG tQe eGJSXPQ tQINGe.tQe

UIeteGOeI'P HTDPe eYQNIteO tQe TSSeJXTGHe NC ZTGF XG eGJSTGO,TGO tQe GTtXNG'P TtteGtXNG

CNHDPeO NG TtteIADIF'P tIXTS. ZNPt NC tQe CTHtPTANDt tQe TSSeJeO HNGPUXITHF QTO HNZe CINZ QXP

XGteIHeUteOHNIIePUNGOeGHe, TGO tQe ZNPt XGHDSUTtNIF eKXOeGHe QTO AeeG eYtITHteOCINZ tQe

UNItXNGP XG HXUQeI AF RXSSeP TGO AF TGtQNGF HNIAXeIe, T CNIZeICNIeXJG PeIKXHe NCCXHXTS XG QXP

ZXO-tQXItXeP RQN QTO TSPN AeeG TUUNXGteO TOeHFUQeIeI XG 1719. tQe SNIOP "tQNDJQt Xt UINUeI

tN HTSS tQe OeHFUQeIeIPAeCNIe tQeZ, XG NIOeI tN tQeXI AeXGJ PTtXPCXeO NC tQe tIDtQ NC

tQeOeHFUQeIXGJ." tN OeZNGPtITte tQXP, RXSSeP TGO HNIAXeIe OeUNPeO, tQTt PeKeITS SetteIP,

RIXtteG XG tQXP HFUQeI, QTO AeeGOeHFUQeIeO AF tQeZ PeUTITteSF, NGe AeXGJ ZTGF ZXSeP OXPtTGt

XGtQe HNDGtIF, TGO tQe NtQeI XG tNRG; TGO Fet tQeXI OeHFUQeIXGJTJIeeO;tQTt CTHtP, DGLGNRG

tN tQeZ TGO tQe JNKeIGZeGt Tt tQe tXZeNC tQeXI OeHFUQeIXGJ, QTO AeeG KeIXCXeO XG eKeIF

HXIHDZPtTGHe AFPDAPeBDeGt OXPHNKeIXeP tQTt T PDUUSeZeGt NC tQXP HFUQeI, QTKXGJ AeeG

CNDGO TZNGJOeGGXP LeSSF'P UTUeIP tQe STtteI eGO NC EDSF, TJIeeO RXtQ tQe LeFtQeF QTO CNIZeO

NC tQTt HFUQeI tQe TUIXS AeCNIe;tQTt tQe OeHFUQeIXGJ NC tQe SetteIP PXJGeO ENGeP

SSSXGJtNG TGO1378, AeXGJ TCteIRTIOP TUUSXeO AF tQeZ tN NtQeIP RIXtteG XG tQePTZe HFUQeI, OXO

XZZeOXTteSF ZTLe UeItXGeGt PeGPe, TGO PDHQ TPQTO TG eKXOeGt HNGGeYXNG TGO HNQeIeGHe RXtQ

tQe UTItP NC tQNPeSetteIP tQTt ReIe NDt NC HFUQeI, tQNDJQ tQe RNIOP XG HFUQeI ReIeIeUeTteO

XG OXCCeIeGt UTITJITUQP, TGO OXCCeIeGtSF HNZAXGeO. tQe tRN OeHFUQeIeIP TUUeTIeO AeCNIe tQe

SNIOP NG PeKeITS NHHTPXNGPtN PReTI tN tQeXI PNSDtXNGP. TtteGADIF tRXHe NAEeHteO TGO RTP

tRXHe NKeIIDSeO. ADt NG ZTF 7, TP RXSSeP RTPtePtXCFXGJ tN tQe HIFUtTGTSFPXP NC tQe tQIee ZNPt

XGHIXZXGTtNIF SetteIP NCTSS, TGO tQe AXPQNU CeSt tQe GNNPe tXJQteGXGJ TINDGO QXZ, Qe

UeIPXPteO XGBDePtXNGXGJ RXSSeP NG tQe KTSXOXtF NC tQe IeTOXGJ tQNDJQ tQe QNDPe

QTOPDUUNIteO RXSSeP' IeCDPTS tN TGPReI. Qe ITXPeO PDHQ T HNZZNtXNG tQTt QeTGO QXP HNDGPeS ReIe

NIOeIeO tN RXtQOITR, TGO tQe SNIOP KNteO DUNG tQeUINUNPXtXNG, "tQTt Xt XP tQe NUXGXNG NC

tQXP QNDPe tQTt Xt XP GNt HNGPXPteGtRXtQ tQe UDASXH PTCetF, tN TPL tQe OeHFUQeIeIP TGF

BDePtXNGP, RQXHQ ZTFteGO tN OXPHNKeI tQe TIt NI ZFPteIF NC OeHFUQeIXGJ." Xt RTP IePNSKeO

XGtQe TCCXIZTtXKe, tQe PNSDtXNGP ReIe THHeUteO, TGO TtteIADIF, STIJeSF NGtQXP eKXOeGHe, RTP

CNDGO JDXStF, OeUIXKeO NC NCCXHe, TGO ATGXPQeO CINZ tQeIeTSZ.

* **Analyzing "tNN"**: I identified the word **“tNN”**, which suggested that **N** might correspond to **O**. This prompted the substitution of **N → O**.
* **Observing 'WQ' and 'QV'**: I noticed repeated patterns like **“WQ”** and **“QV”**, which could correspond to the common digraphs **“TH”** and **“HE”**. Since **W** had already been mapped to **T**, and **V** was suspected to be **E**, I made the following additional substitution:
  + **Q → H**

eGJSTGO, too, hTO XtP ASTHL HhTZAeI. Xt AeJTG RXth the HIFUtTGTSFtXHeGOeTKoIP oC EohG RTSSXP,

the JIeTtePt eGJSXPh ZTtheZTtXHXTG AeCoIeGeRtoG. TCteI hXP OeTth, Xt OePHeGOeO thIoDJh

hXP JITGOPoG to IeTHh, oGZTF 14, 1716, eORTIO RXSSeP, T 22-FeTI-oSO ZXGXPteI Tt oIXeS

HoSSeJe,oYCoIO.RXSSeP eZATILeO Tt oGHe DUoG T HTIeeI DGXBDe XG the TGGTSP oCHIFUtoSoJF TGO the

HhDIHh. he Got oGSF ZTGTJeO to IeHoGHXSe hXPIeSXJXoDP HTSSXGJ RXth TG THtXKXtF oGHe HoGOeZGeO

AF HhDIHhSFTDthoIXtXeP, ADt TSPo ReGt oG to AeHoZe the oGSF ZTG XG hXPtoIF to

DPeHIFUtTGTSFtXH tTSeGtP to UIoHDIe eHHSePXTPtXHTS IeRTIOP. RXthXG tRo FeTIP,he hTO AeeG GTZeO

IeHtoI oC ATItoG, AeOCoIOPhXIe, CoI PoSKXGJ ZoIe thTG300 UTJeP oC HXUheI thTt eYUoPeO PReOeG'P

TtteZUt to CoZeGt TG DUIXPXGJ XG eGJSTGO. he KXItDTSSF JDTITGteeO hXPCDtDIe RheG he

tePtXCXeO AeCoIe the hoDPe oC SoIOP XG 1723. heIe, CITGHXPTtteIADIF, AXPhoU oC IoHhePteI,

RTP AeXGJ tIXeO AF hXP UeeIP CoITtteZUtXGJ to Pet T UIeteGOeI oG the eGJSXPh thIoGe.the

UIeteGOeI'P HTDPe eYhoIteO the TSSeJXTGHe oC ZTGF XG eGJSTGO,TGO the GTtXoG'P TtteGtXoG

CoHDPeO oG TtteIADIF'P tIXTS. ZoPt oC the CTHtPTAoDt the TSSeJeO HoGPUXITHF hTO HoZe CIoZ hXP

XGteIHeUteOHoIIePUoGOeGHe, TGO the ZoPt XGHDSUTtoIF eKXOeGHe hTO AeeG eYtITHteOCIoZ the

UoItXoGP XG HXUheI AF RXSSeP TGO AF TGthoGF HoIAXeIe, T CoIZeICoIeXJG PeIKXHe oCCXHXTS XG hXP

ZXO-thXItXeP Rho hTO TSPo AeeG TUUoXGteO TOeHFUheIeI XG 1719. the SoIOP "thoDJht Xt UIoUeI

to HTSS the OeHFUheIeIPAeCoIe theZ, XG oIOeI to theXI AeXGJ PTtXPCXeO oC the tIDth oC

theOeHFUheIXGJ." to OeZoGPtITte thXP, RXSSeP TGO HoIAXeIe OeUoPeO, thTt PeKeITS SetteIP,

RIXtteG XG thXP HFUheI, hTO AeeGOeHFUheIeO AF theZ PeUTITteSF, oGe AeXGJ ZTGF ZXSeP OXPtTGt

XGthe HoDGtIF, TGO the otheI XG toRG; TGO Fet theXI OeHFUheIXGJTJIeeO;thTt CTHtP, DGLGoRG

to theZ TGO the JoKeIGZeGt Tt the tXZeoC theXI OeHFUheIXGJ, hTO AeeG KeIXCXeO XG eKeIF

HXIHDZPtTGHe AFPDAPeBDeGt OXPHoKeIXeP thTt T PDUUSeZeGt oC thXP HFUheI, hTKXGJ AeeG

CoDGO TZoGJOeGGXP LeSSF'P UTUeIP the STtteI eGO oC EDSF, TJIeeO RXth the LeFtheF hTO CoIZeO

oC thTt HFUheI the TUIXS AeCoIe;thTt the OeHFUheIXGJ oC the SetteIP PXJGeO EoGeP

SSSXGJtoG TGO1378, AeXGJ TCteIRTIOP TUUSXeO AF theZ to otheIP RIXtteG XG thePTZe HFUheI, OXO

XZZeOXTteSF ZTLe UeItXGeGt PeGPe, TGO PDHh TPhTO TG eKXOeGt HoGGeYXoG TGO HoheIeGHe RXth

the UTItP oC thoPeSetteIP thTt ReIe oDt oC HFUheI, thoDJh the RoIOP XG HFUheI ReIeIeUeTteO

XG OXCCeIeGt UTITJITUhP, TGO OXCCeIeGtSF HoZAXGeO. the tRo OeHFUheIeIP TUUeTIeO AeCoIe the

SoIOP oG PeKeITS oHHTPXoGPto PReTI to theXI PoSDtXoGP. TtteGADIF tRXHe oAEeHteO TGO RTP

tRXHe oKeIIDSeO. ADt oG ZTF 7, TP RXSSeP RTPtePtXCFXGJ to the HIFUtTGTSFPXP oC the thIee ZoPt

XGHIXZXGTtoIF SetteIP oCTSS, TGO the AXPhoU CeSt the GooPe tXJhteGXGJ TIoDGO hXZ, he

UeIPXPteO XGBDePtXoGXGJ RXSSeP oG the KTSXOXtF oC the IeTOXGJ thoDJh the hoDPe

hTOPDUUoIteO RXSSeP' IeCDPTS to TGPReI. he ITXPeO PDHh T HoZZotXoG thTt heTGO hXP HoDGPeS ReIe

oIOeIeO to RXthOITR, TGO the SoIOP KoteO DUoG theUIoUoPXtXoG, "thTt Xt XP the oUXGXoG oC

thXP hoDPe thTt Xt XP Got HoGPXPteGtRXth the UDASXH PTCetF, to TPL the OeHFUheIeIP TGF

BDePtXoGP, RhXHh ZTFteGO to OXPHoKeI the TIt oI ZFPteIF oC OeHFUheIXGJ." Xt RTP IePoSKeO

XGthe TCCXIZTtXKe, the PoSDtXoGP ReIe THHeUteO, TGO TtteIADIF, STIJeSF oGthXP eKXOeGHe, RTP

CoDGO JDXStF, OeUIXKeO oC oCCXHe, TGO ATGXPheO CIoZ theIeTSZ.

* **Guessing 'G' as 'A' and 'X' as 'I'**: Based on the emerging patterns, I hypothesized that **G** represented **A** and **X** represented **I**. This step brought further coherence to the text.

eaJSTaO, too, hTO itP ASTHL HhTZAeI. it AeJTa Rith the HIFUtTaTSFtiHeaOeTKoIP oC Eoha RTSSiP,

the JIeTtePt eaJSiPh ZTtheZTtiHiTa AeCoIeaeRtoa. TCteI hiP OeTth, it OePHeaOeO thIoDJh

hiP JITaOPoa to IeTHh, oaZTF 14, 1716, eORTIO RiSSeP, T 22-FeTI-oSO ZiaiPteI Tt oIieS

HoSSeJe,oYCoIO.RiSSeP eZATILeO Tt oaHe DUoa T HTIeeI DaiBDe ia the TaaTSP oCHIFUtoSoJF TaO the

HhDIHh. he aot oaSF ZTaTJeO to IeHoaHiSe hiPIeSiJioDP HTSSiaJ Rith Ta THtiKitF oaHe HoaOeZaeO

AF HhDIHhSFTDthoIitieP, ADt TSPo Reat oa to AeHoZe the oaSF ZTa ia hiPtoIF to

DPeHIFUtTaTSFtiH tTSeatP to UIoHDIe eHHSePiTPtiHTS IeRTIOP. Rithia tRo FeTIP,he hTO Aeea aTZeO

IeHtoI oC ATItoa, AeOCoIOPhiIe, CoI PoSKiaJ ZoIe thTa300 UTJeP oC HiUheI thTt eYUoPeO PReOea'P

TtteZUt to CoZeat Ta DUIiPiaJ ia eaJSTaO. he KiItDTSSF JDTITateeO hiPCDtDIe Rhea he

tePtiCieO AeCoIe the hoDPe oC SoIOP ia 1723. heIe, CITaHiPTtteIADIF, AiPhoU oC IoHhePteI,

RTP AeiaJ tIieO AF hiP UeeIP CoITtteZUtiaJ to Pet T UIeteaOeI oa the eaJSiPh thIoae.the

UIeteaOeI'P HTDPe eYhoIteO the TSSeJiTaHe oC ZTaF ia eaJSTaO,TaO the aTtioa'P Ttteatioa

CoHDPeO oa TtteIADIF'P tIiTS. ZoPt oC the CTHtPTAoDt the TSSeJeO HoaPUiITHF hTO HoZe CIoZ hiP

iateIHeUteOHoIIePUoaOeaHe, TaO the ZoPt iaHDSUTtoIF eKiOeaHe hTO Aeea eYtITHteOCIoZ the

UoItioaP ia HiUheI AF RiSSeP TaO AF TathoaF HoIAieIe, T CoIZeICoIeiJa PeIKiHe oCCiHiTS ia hiP

ZiO-thiItieP Rho hTO TSPo Aeea TUUoiateO TOeHFUheIeI ia 1719. the SoIOP "thoDJht it UIoUeI

to HTSS the OeHFUheIeIPAeCoIe theZ, ia oIOeI to theiI AeiaJ PTtiPCieO oC the tIDth oC

theOeHFUheIiaJ." to OeZoaPtITte thiP, RiSSeP TaO HoIAieIe OeUoPeO, thTt PeKeITS SetteIP,

RIittea ia thiP HFUheI, hTO AeeaOeHFUheIeO AF theZ PeUTITteSF, oae AeiaJ ZTaF ZiSeP OiPtTat

iathe HoDatIF, TaO the otheI ia toRa; TaO Fet theiI OeHFUheIiaJTJIeeO;thTt CTHtP, DaLaoRa

to theZ TaO the JoKeIaZeat Tt the tiZeoC theiI OeHFUheIiaJ, hTO Aeea KeIiCieO ia eKeIF

HiIHDZPtTaHe AFPDAPeBDeat OiPHoKeIieP thTt T PDUUSeZeat oC thiP HFUheI, hTKiaJ Aeea

CoDaO TZoaJOeaaiP LeSSF'P UTUeIP the STtteI eaO oC EDSF, TJIeeO Rith the LeFtheF hTO CoIZeO

oC thTt HFUheI the TUIiS AeCoIe;thTt the OeHFUheIiaJ oC the SetteIP PiJaeO EoaeP

SSSiaJtoa TaO1378, AeiaJ TCteIRTIOP TUUSieO AF theZ to otheIP RIittea ia thePTZe HFUheI, OiO

iZZeOiTteSF ZTLe UeItiaeat PeaPe, TaO PDHh TPhTO Ta eKiOeat HoaaeYioa TaO HoheIeaHe Rith

the UTItP oC thoPeSetteIP thTt ReIe oDt oC HFUheI, thoDJh the RoIOP ia HFUheI ReIeIeUeTteO

ia OiCCeIeat UTITJITUhP, TaO OiCCeIeatSF HoZAiaeO. the tRo OeHFUheIeIP TUUeTIeO AeCoIe the

SoIOP oa PeKeITS oHHTPioaPto PReTI to theiI PoSDtioaP. TtteaADIF tRiHe oAEeHteO TaO RTP

tRiHe oKeIIDSeO. ADt oa ZTF 7, TP RiSSeP RTPtePtiCFiaJ to the HIFUtTaTSFPiP oC the thIee ZoPt

iaHIiZiaTtoIF SetteIP oCTSS, TaO the AiPhoU CeSt the aooPe tiJhteaiaJ TIoDaO hiZ, he

UeIPiPteO iaBDePtioaiaJ RiSSeP oa the KTSiOitF oC the IeTOiaJ thoDJh the hoDPe

hTOPDUUoIteO RiSSeP' IeCDPTS to TaPReI. he ITiPeO PDHh T HoZZotioa thTt heTaO hiP HoDaPeS ReIe

oIOeIeO to RithOITR, TaO the SoIOP KoteO DUoa theUIoUoPitioa, "thTt it iP the oUiaioa oC

thiP hoDPe thTt it iP aot HoaPiPteatRith the UDASiH PTCetF, to TPL the OeHFUheIeIP TaF

BDePtioaP, RhiHh ZTFteaO to OiPHoKeI the TIt oI ZFPteIF oC OeHFUheIiaJ." it RTP IePoSKeO

iathe TCCiIZTtiKe, the PoSDtioaP ReIe THHeUteO, TaO TtteIADIF, STIJeSF oathiP eKiOeaHe, RTP

CoDaO JDiStF, OeUIiKeO oC oCCiHe, TaO ATaiPheO CIoZ theIeTSZ.

* **Word "itP" and "hiP"**: I deduced that **P** was most likely **S**, given the context of words like **“its”** and **“his”**.
* **Determining 'R' as 'W'**: Observing the word **“Rith”** led me to replace **R** with **W**, as it closely resembled the word **“with”**.

eaJSTaO, too, hTO its ASTHL HhTZAeI. it AeJTa with the HIFUtTaTSFtiHeaOeTKoIs oC Eoha wTSSis,

the JIeTtest eaJSish ZTtheZTtiHiTa AeCoIeaewtoa. TCteI his OeTth, it OesHeaOeO thIoDJh

his JITaOsoa to IeTHh, oaZTF 14, 1716, eOwTIO wiSSes, T 22-FeTI-oSO ZiaisteI Tt oIieS

HoSSeJe,oYCoIO.wiSSes eZATILeO Tt oaHe DUoa T HTIeeI DaiBDe ia the TaaTSs oCHIFUtoSoJF TaO the

HhDIHh. he aot oaSF ZTaTJeO to IeHoaHiSe hisIeSiJioDs HTSSiaJ with Ta THtiKitF oaHe HoaOeZaeO

AF HhDIHhSFTDthoIities, ADt TSso weat oa to AeHoZe the oaSF ZTa ia histoIF to

DseHIFUtTaTSFtiH tTSeats to UIoHDIe eHHSesiTstiHTS IewTIOs. withia two FeTIs,he hTO Aeea aTZeO

IeHtoI oC ATItoa, AeOCoIOshiIe, CoI soSKiaJ ZoIe thTa300 UTJes oC HiUheI thTt eYUoseO sweOea's

TtteZUt to CoZeat Ta DUIisiaJ ia eaJSTaO. he KiItDTSSF JDTITateeO hisCDtDIe whea he

testiCieO AeCoIe the hoDse oC SoIOs ia 1723. heIe, CITaHisTtteIADIF, AishoU oC IoHhesteI,

wTs AeiaJ tIieO AF his UeeIs CoITtteZUtiaJ to set T UIeteaOeI oa the eaJSish thIoae.the

UIeteaOeI's HTDse eYhoIteO the TSSeJiTaHe oC ZTaF ia eaJSTaO,TaO the aTtioa's Ttteatioa

CoHDseO oa TtteIADIF's tIiTS. Zost oC the CTHtsTAoDt the TSSeJeO HoasUiITHF hTO HoZe CIoZ his

iateIHeUteOHoIIesUoaOeaHe, TaO the Zost iaHDSUTtoIF eKiOeaHe hTO Aeea eYtITHteOCIoZ the

UoItioas ia HiUheI AF wiSSes TaO AF TathoaF HoIAieIe, T CoIZeICoIeiJa seIKiHe oCCiHiTS ia his

ZiO-thiIties who hTO TSso Aeea TUUoiateO TOeHFUheIeI ia 1719. the SoIOs "thoDJht it UIoUeI

to HTSS the OeHFUheIeIsAeCoIe theZ, ia oIOeI to theiI AeiaJ sTtisCieO oC the tIDth oC

theOeHFUheIiaJ." to OeZoastITte this, wiSSes TaO HoIAieIe OeUoseO, thTt seKeITS SetteIs,

wIittea ia this HFUheI, hTO AeeaOeHFUheIeO AF theZ seUTITteSF, oae AeiaJ ZTaF ZiSes OistTat

iathe HoDatIF, TaO the otheI ia towa; TaO Fet theiI OeHFUheIiaJTJIeeO;thTt CTHts, DaLaowa

to theZ TaO the JoKeIaZeat Tt the tiZeoC theiI OeHFUheIiaJ, hTO Aeea KeIiCieO ia eKeIF

HiIHDZstTaHe AFsDAseBDeat OisHoKeIies thTt T sDUUSeZeat oC this HFUheI, hTKiaJ Aeea

CoDaO TZoaJOeaais LeSSF's UTUeIs the STtteI eaO oC EDSF, TJIeeO with the LeFtheF hTO CoIZeO

oC thTt HFUheI the TUIiS AeCoIe;thTt the OeHFUheIiaJ oC the SetteIs siJaeO Eoaes

SSSiaJtoa TaO1378, AeiaJ TCteIwTIOs TUUSieO AF theZ to otheIs wIittea ia thesTZe HFUheI, OiO

iZZeOiTteSF ZTLe UeItiaeat sease, TaO sDHh TshTO Ta eKiOeat HoaaeYioa TaO HoheIeaHe with

the UTIts oC thoseSetteIs thTt weIe oDt oC HFUheI, thoDJh the woIOs ia HFUheI weIeIeUeTteO

ia OiCCeIeat UTITJITUhs, TaO OiCCeIeatSF HoZAiaeO. the two OeHFUheIeIs TUUeTIeO AeCoIe the

SoIOs oa seKeITS oHHTsioasto sweTI to theiI soSDtioas. TtteaADIF twiHe oAEeHteO TaO wTs

twiHe oKeIIDSeO. ADt oa ZTF 7, Ts wiSSes wTstestiCFiaJ to the HIFUtTaTSFsis oC the thIee Zost

iaHIiZiaTtoIF SetteIs oCTSS, TaO the AishoU CeSt the aoose tiJhteaiaJ TIoDaO hiZ, he

UeIsisteO iaBDestioaiaJ wiSSes oa the KTSiOitF oC the IeTOiaJ thoDJh the hoDse

hTOsDUUoIteO wiSSes' IeCDsTS to TasweI. he ITiseO sDHh T HoZZotioa thTt heTaO his HoDaseS weIe

oIOeIeO to withOITw, TaO the SoIOs KoteO DUoa theUIoUositioa, "thTt it is the oUiaioa oC

this hoDse thTt it is aot Hoasisteatwith the UDASiH sTCetF, to TsL the OeHFUheIeIs TaF

BDestioas, whiHh ZTFteaO to OisHoKeI the TIt oI ZFsteIF oC OeHFUheIiaJ." it wTs IesoSKeO

iathe TCCiIZTtiKe, the soSDtioas weIe THHeUteO, TaO TtteIADIF, STIJeSF oathis eKiOeaHe, wTs

CoDaO JDiStF, OeUIiKeO oC oCCiHe, TaO ATaisheO CIoZ theIeTSZ.

* **Verifying with 'OeTth' and 'death'**: The partial word **“OeTth”** was hypothesized as **“death”**, leading to the substitution **O → D**. **T → A**.
* **Correcting letters in AegaG"**: I refined the previous substitution of **A** to **B** and **G** to **N** after recognizing the pattern **“AegaG”** as **“began”**.
* **‘the JIeatest’: most likely J stands for G and I for R**

engSand, too, had its bSaHL HhaZber. it began with the HrFUtanaSFtiHendeaKors oC Eohn waSSis,

the greatest engSish ZatheZatiHian beCorenewton. aCter his death, it desHended throDgh

his grandson to reaHh, onZaF 14, 1716, edward wiSSes, a 22-Fear-oSd Zinister at orieS

HoSSege,oYCord.wiSSes eZbarLed at onHe DUon a Hareer DniBDe in the annaSs oCHrFUtoSogF and the

HhDrHh. he not onSF Zanaged to reHonHiSe hisreSigioDs HaSSing with an aHtiKitF onHe HondeZned

bF HhDrHhSFaDthorities, bDt aSso went on to beHoZe the onSF Zan in historF to

DseHrFUtanaSFtiH taSents to UroHDre eHHSesiastiHaS rewards. within two Fears,he had been naZed

reHtor oC barton, bedCordshire, Cor soSKing Zore than300 Uages oC HiUher that eYUosed sweden's

atteZUt to CoZent an DUrising in engSand. he KirtDaSSF gDaranteed hisCDtDre when he

testiCied beCore the hoDse oC Sords in 1723. here, CranHisatterbDrF, bishoU oC roHhester,

was being tried bF his Ueers CoratteZUting to set a Uretender on the engSish throne.the

Uretender's HaDse eYhorted the aSSegianHe oC ZanF in engSand,and the nation's attention

CoHDsed on atterbDrF's triaS. Zost oC the CaHtsaboDt the aSSeged HonsUiraHF had HoZe CroZ his

interHeUtedHorresUondenHe, and the Zost inHDSUatorF eKidenHe had been eYtraHtedCroZ the

Uortions in HiUher bF wiSSes and bF anthonF Horbiere, a CorZerCoreign serKiHe oCCiHiaS in his

Zid-thirties who had aSso been aUUointed adeHFUherer in 1719. the Sords "thoDght it UroUer

to HaSS the deHFUherersbeCore theZ, in order to their being satisCied oC the trDth oC

thedeHFUhering." to deZonstrate this, wiSSes and Horbiere deUosed, that seKeraS Setters,

written in this HFUher, had beendeHFUhered bF theZ seUarateSF, one being ZanF ZiSes distant

inthe HoDntrF, and the other in town; and Fet their deHFUheringagreed;that CaHts, DnLnown

to theZ and the goKernZent at the tiZeoC their deHFUhering, had been KeriCied in eKerF

HirHDZstanHe bFsDbseBDent disHoKeries that a sDUUSeZent oC this HFUher, haKing been

CoDnd aZongdennis LeSSF's UaUers the Satter end oC EDSF, agreed with the LeFtheF had CorZed

oC that HFUher the aUriS beCore;that the deHFUhering oC the Setters signed Eones

SSSington and1378, being aCterwards aUUSied bF theZ to others written in thesaZe HFUher, did

iZZediateSF ZaLe Uertinent sense, and sDHh ashad an eKident HonneYion and HoherenHe with

the Uarts oC thoseSetters that were oDt oC HFUher, thoDgh the words in HFUher werereUeated

in diCCerent UaragraUhs, and diCCerentSF HoZbined. the two deHFUherers aUUeared beCore the

Sords on seKeraS oHHasionsto swear to their soSDtions. attenbDrF twiHe obEeHted and was

twiHe oKerrDSed. bDt on ZaF 7, as wiSSes wastestiCFing to the HrFUtanaSFsis oC the three Zost

inHriZinatorF Setters oCaSS, and the bishoU CeSt the noose tightening aroDnd hiZ, he

Uersisted inBDestioning wiSSes on the KaSiditF oC the reading thoDgh the hoDse

hadsDUUorted wiSSes' reCDsaS to answer. he raised sDHh a HoZZotion that heand his HoDnseS were

ordered to withdraw, and the Sords Koted DUon theUroUosition, "that it is the oUinion oC

this hoDse that it is not Honsistentwith the UDbSiH saCetF, to asL the deHFUherers anF

BDestions, whiHh ZaFtend to disHoKer the art or ZFsterF oC deHFUhering." it was resoSKed

inthe aCCirZatiKe, the soSDtions were aHHeUted, and atterbDrF, SargeSF onthis eKidenHe, was

CoDnd gDiStF, deUriKed oC oCCiHe, and banished CroZ thereaSZ.

* **Identifying 'engSand' as 'England' and 'engSish' as 'english’**: This context helped confirm **S → L**.
* **Refining 'grandson to reaHh' as 'reach'**: This clue led to the substitution **H → C**.

england, too, had its blacL chaZber. it began with the crFUtanalFticendeaKors oC Eohn wallis,

the greatest english ZatheZatician beCorenewton. aCter his death, it descended throDgh

his grandson to reach, onZaF 14, 1716, edward willes, a 22-Fear-old Zinister at oriel

college,oYCord.willes eZbarLed at once DUon a career DniBDe in the annals oCcrFUtologF and the

chDrch. he not onlF Zanaged to reconcile hisreligioDs calling with an actiKitF once condeZned

bF chDrchlFaDthorities, bDt also went on to becoZe the onlF Zan in historF to

DsecrFUtanalFtic talents to UrocDre ecclesiastical rewards. within two Fears,he had been naZed

rector oC barton, bedCordshire, Cor solKing Zore than300 Uages oC ciUher that eYUosed sweden's

atteZUt to CoZent an DUrising in england. he KirtDallF gDaranteed hisCDtDre when he

testiCied beCore the hoDse oC lords in 1723. here, CrancisatterbDrF, bishoU oC rochester,

was being tried bF his Ueers CoratteZUting to set a Uretender on the english throne.the

Uretender's caDse eYhorted the allegiance oC ZanF in england,and the nation's attention

CocDsed on atterbDrF's trial. Zost oC the CactsaboDt the alleged consUiracF had coZe CroZ his

interceUtedcorresUondence, and the Zost incDlUatorF eKidence had been eYtractedCroZ the

Uortions in ciUher bF willes and bF anthonF corbiere, a CorZerCoreign serKice oCCicial in his

Zid-thirties who had also been aUUointed adecFUherer in 1719. the lords "thoDght it UroUer

to call the decFUherersbeCore theZ, in order to their being satisCied oC the trDth oC

thedecFUhering." to deZonstrate this, willes and corbiere deUosed, that seKeral letters,

written in this cFUher, had beendecFUhered bF theZ seUaratelF, one being ZanF Ziles distant

inthe coDntrF, and the other in town; and Fet their decFUheringagreed;that Cacts, DnLnown

to theZ and the goKernZent at the tiZeoC their decFUhering, had been KeriCied in eKerF

circDZstance bFsDbseBDent discoKeries that a sDUUleZent oC this cFUher, haKing been

CoDnd aZongdennis LellF's UaUers the latter end oC EDlF, agreed with the LeFtheF had CorZed

oC that cFUher the aUril beCore;that the decFUhering oC the letters signed Eones

lllington and1378, being aCterwards aUUlied bF theZ to others written in thesaZe cFUher, did

iZZediatelF ZaLe Uertinent sense, and sDch ashad an eKident conneYion and coherence with

the Uarts oC thoseletters that were oDt oC cFUher, thoDgh the words in cFUher werereUeated

in diCCerent UaragraUhs, and diCCerentlF coZbined. the two decFUherers aUUeared beCore the

lords on seKeral occasionsto swear to their solDtions. attenbDrF twice obEected and was

twice oKerrDled. bDt on ZaF 7, as willes wastestiCFing to the crFUtanalFsis oC the three Zost

incriZinatorF letters oCall, and the bishoU Celt the noose tightening aroDnd hiZ, he

Uersisted inBDestioning willes on the KaliditF oC the reading thoDgh the hoDse

hadsDUUorted willes' reCDsal to answer. he raised sDch a coZZotion that heand his coDnsel were

ordered to withdraw, and the lords Koted DUon theUroUosition, "that it is the oUinion oC

this hoDse that it is not consistentwith the UDblic saCetF, to asL the decFUherers anF

BDestions, which ZaFtend to discoKer the art or ZFsterF oC decFUhering." it was resolKed

inthe aCCirZatiKe, the solDtions were acceUted, and atterbDrF, largelF onthis eKidence, was

CoDnd gDiltF, deUriKed oC oCCice, and banished CroZ therealZ.

* **Interpreting 'ZatheZatician' as 'Mathematician'**: This guided the substitution of **Z → M**.
* **Correcting 'aCter' and 'beCore' to 'after' and 'before'**: This refinement mapped **C → F**.

england, too, had its blacL chamber. it began with the crFUtanalFticendeaKors of Eohn wallis,

the greatest english mathematician beforenewton. after his death, it descended throDgh

his grandson to reach, onmaF 14, 1716, edward willes, a 22-Fear-old minister at oriel

college,oYford.willes embarLed at once DUon a career DniBDe in the annals ofcrFUtologF and the

chDrch. he not onlF managed to reconcile hisreligioDs calling with an actiKitF once condemned

bF chDrchlFaDthorities, bDt also went on to become the onlF man in historF to

DsecrFUtanalFtic talents to UrocDre ecclesiastical rewards. within two Fears,he had been named

rector of barton, bedfordshire, for solKing more than300 Uages of ciUher that eYUosed sweden's

attemUt to foment an DUrising in england. he KirtDallF gDaranteed hisfDtDre when he

testified before the hoDse of lords in 1723. here, francisatterbDrF, bishoU of rochester,

was being tried bF his Ueers forattemUting to set a Uretender on the english throne.the

Uretender's caDse eYhorted the allegiance of manF in england,and the nation's attention

focDsed on atterbDrF's trial. most of the factsaboDt the alleged consUiracF had come from his

interceUtedcorresUondence, and the most incDlUatorF eKidence had been eYtractedfrom the

Uortions in ciUher bF willes and bF anthonF corbiere, a formerforeign serKice official in his

mid-thirties who had also been aUUointed adecFUherer in 1719. the lords "thoDght it UroUer

to call the decFUherersbefore them, in order to their being satisfied of the trDth of

thedecFUhering." to demonstrate this, willes and corbiere deUosed, that seKeral letters,

written in this cFUher, had beendecFUhered bF them seUaratelF, one being manF miles distant

inthe coDntrF, and the other in town; and Fet their decFUheringagreed;that facts, DnLnown

to them and the goKernment at the timeof their decFUhering, had been Kerified in eKerF

circDmstance bFsDbseBDent discoKeries that a sDUUlement of this cFUher, haKing been

foDnd amongdennis LellF's UaUers the latter end of EDlF, agreed with the LeFtheF had formed

of that cFUher the aUril before;that the decFUhering of the letters signed Eones

lllington and1378, being afterwards aUUlied bF them to others written in thesame cFUher, did

immediatelF maLe Uertinent sense, and sDch ashad an eKident conneYion and coherence with

the Uarts of thoseletters that were oDt of cFUher, thoDgh the words in cFUher werereUeated

in different UaragraUhs, and differentlF combined. the two decFUherers aUUeared before the

lords on seKeral occasionsto swear to their solDtions. attenbDrF twice obEected and was

twice oKerrDled. bDt on maF 7, as willes wastestifFing to the crFUtanalFsis of the three most

incriminatorF letters ofall, and the bishoU felt the noose tightening aroDnd him, he

Uersisted inBDestioning willes on the KaliditF of the reading thoDgh the hoDse

hadsDUUorted willes' refDsal to answer. he raised sDch a commotion that heand his coDnsel were

ordered to withdraw, and the lords Koted DUon theUroUosition, "that it is the oUinion of

this hoDse that it is not consistentwith the UDblic safetF, to asL the decFUherers anF

BDestions, which maFtend to discoKer the art or mFsterF of decFUhering." it was resolKed

inthe affirmatiKe, the solDtions were acceUted, and atterbDrF, largelF onthis eKidence, was

foDnd gDiltF, deUriKed of office, and banished from therealm.

* **'college oYford' as 'College Oxford'**: This phrase required the substitution **Y → X**.
* **Decoding 'chDrch' as 'Church'**: This further clarified **D → U**.
* **Finalizing 'uniBue' as 'Unique'**: Here, **B → Q** completed the phrase.

england, too, had its blacL chamber. it began with the crFUtanalFticendeaKors of Eohn wallis,

the greatest english mathematician beforenewton. after his death, it descended through

his grandson to reach, onmaF 14, 1716, edward willes, a 22-Fear-old minister at oriel

college,oxford.willes embarLed at once uUon a career unique in the annals ofcrFUtologF and the

church. he not onlF managed to reconcile hisreligious calling with an actiKitF once condemned

bF churchlFauthorities, but also went on to become the onlF man in historF to

usecrFUtanalFtic talents to Urocure ecclesiastical rewards. within two Fears,he had been named

rector of barton, bedfordshire, for solKing more than300 Uages of ciUher that exUosed sweden's

attemUt to foment an uUrising in england. he KirtuallF guaranteed hisfuture when he

testified before the house of lords in 1723. here, francisatterburF, bishoU of rochester,

was being tried bF his Ueers forattemUting to set a Uretender on the english throne.the

Uretender's cause exhorted the allegiance of manF in england,and the nation's attention

focused on atterburF's trial. most of the factsabout the alleged consUiracF had come from his

interceUtedcorresUondence, and the most inculUatorF eKidence had been extractedfrom the

Uortions in ciUher bF willes and bF anthonF corbiere, a formerforeign serKice official in his

mid-thirties who had also been aUUointed adecFUherer in 1719. the lords "thought it UroUer

to call the decFUherersbefore them, in order to their being satisfied of the truth of

thedecFUhering." to demonstrate this, willes and corbiere deUosed, that seKeral letters,

written in this cFUher, had beendecFUhered bF them seUaratelF, one being manF miles distant

inthe countrF, and the other in town; and Fet their decFUheringagreed;that facts, unLnown

to them and the goKernment at the timeof their decFUhering, had been Kerified in eKerF

circumstance bFsubsequent discoKeries that a suUUlement of this cFUher, haKing been

found amongdennis LellF's UaUers the latter end of EulF, agreed with the LeFtheF had formed

of that cFUher the aUril before;that the decFUhering of the letters signed Eones

lllington and1378, being afterwards aUUlied bF them to others written in thesame cFUher, did

immediatelF maLe Uertinent sense, and such ashad an eKident connexion and coherence with

the Uarts of thoseletters that were out of cFUher, though the words in cFUher werereUeated

in different UaragraUhs, and differentlF combined. the two decFUherers aUUeared before the

lords on seKeral occasionsto swear to their solutions. attenburF twice obEected and was

twice oKerruled. but on maF 7, as willes wastestifFing to the crFUtanalFsis of the three most

incriminatorF letters ofall, and the bishoU felt the noose tightening around him, he

Uersisted inquestioning willes on the KaliditF of the reading though the house

hadsuUUorted willes' refusal to answer. he raised such a commotion that heand his counsel were

ordered to withdraw, and the lords Koted uUon theUroUosition, "that it is the oUinion of

this house that it is not consistentwith the Uublic safetF, to asL the decFUherers anF

questions, which maFtend to discoKer the art or mFsterF of decFUhering." it was resolKed

inthe affirmatiKe, the solutions were acceUted, and atterburF, largelF onthis eKidence, was

found guiltF, deUriKed of office, and banished from therealm.

* **Decoding 'on maF 14' to 'on May 14'**: This refinement established **F → Y**.
* **Matching 'embarled' and 'blacL' to 'embarked' and 'black'**: The substitution **L → K** was confirmed.
* **Establishing 'solKing' as 'solving'**: This verified **K → V**.

england, too, had its black chamber. it began with the cryUtanalyticendeavors of Eohn wallis,

the greatest english mathematician beforenewton. after his death, it descended through

his grandson to reach, onmay 14, 1716, edward willes, a 22-year-old minister at oriel

college,oxford.willes embarked at once uUon a career unique in the annals ofcryUtology and the

church. he not only managed to reconcile hisreligious calling with an activity once condemned

by churchlyauthorities, but also went on to become the only man in history to

usecryUtanalytic talents to Urocure ecclesiastical rewards. within two years,he had been named

rector of barton, bedfordshire, for solving more than300 Uages of ciUher that exUosed sweden's

attemUt to foment an uUrising in england. he virtually guaranteed hisfuture when he

testified before the house of lords in 1723. here, francisatterbury, bishoU of rochester,

was being tried by his Ueers forattemUting to set a Uretender on the english throne.the

Uretender's cause exhorted the allegiance of many in england,and the nation's attention

focused on atterbury's trial. most of the factsabout the alleged consUiracy had come from his

interceUtedcorresUondence, and the most inculUatory evidence had been extractedfrom the

Uortions in ciUher by willes and by anthony corbiere, a formerforeign service official in his

mid-thirties who had also been aUUointed adecyUherer in 1719. the lords "thought it UroUer

to call the decyUherersbefore them, in order to their being satisfied of the truth of

thedecyUhering." to demonstrate this, willes and corbiere deUosed, that several letters,

written in this cyUher, had beendecyUhered by them seUarately, one being many miles distant

inthe country, and the other in town; and yet their decyUheringagreed;that facts, unknown

to them and the government at the timeof their decyUhering, had been verified in every

circumstance bysubsequent discoveries that a suUUlement of this cyUher, having been

found amongdennis kelly's UaUers the latter end of Euly, agreed with the keythey had formed

of that cyUher the aUril before;that the decyUhering of the letters signed Eones

lllington and1378, being afterwards aUUlied by them to others written in thesame cyUher, did

immediately make Uertinent sense, and such ashad an evident connexion and coherence with

the Uarts of thoseletters that were out of cyUher, though the words in cyUher werereUeated

in different UaragraUhs, and differently combined. the two decyUherers aUUeared before the

lords on several occasionsto swear to their solutions. attenbury twice obEected and was

twice overruled. but on may 7, as willes wastestifying to the cryUtanalysis of the three most

incriminatory letters ofall, and the bishoU felt the noose tightening around him, he

Uersisted inquestioning willes on the validity of the reading though the house

hadsuUUorted willes' refusal to answer. he raised such a commotion that heand his counsel were

ordered to withdraw, and the lords voted uUon theUroUosition, "that it is the oUinion of

this house that it is not consistentwith the Uublic safety, to ask the decyUherers any

questions, which maytend to discover the art or mystery of decyUhering." it was resolved

inthe affirmative, the solutions were acceUted, and atterbury, largely onthis evidence, was

found guilty, deUrived of office, and banished from therealm.

* **Establishing 'cryUtanalytic' and ‘uUon’ as 'cryptanalytic’ and ‘upon’**: This verified **U → P**.
* **Analyzing ‘end of Euly’ and ‘Eones Willington’:** This gives me **E → J**
* **Assigning Remaining Letters**: After identifying the majority of letters, the last remaining unassigned letters were **M** and **Z**. I mapped **M** to **Z** to complete the decryption.

After substituting each letter and ensuring that each word made logical sense, the final decrypted alphabet was confirmed as follows:

england, too, had its black chamber. it began with the cryptanalyticendeavors of john wallis,

the greatest english mathematician beforenewton. after his death, it descended through

his grandson to reach, onmay 14, 1716, edward willes, a 22-year-old minister at oriel

college,oxford.willes embarked at once upon a career unique in the annals ofcryptology and the

church. he not only managed to reconcile hisreligious calling with an activity once condemned

by churchlyauthorities, but also went on to become the only man in history to

usecryptanalytic talents to procure ecclesiastical rewards. within two years,he had been named

rector of barton, bedfordshire, for solving more than300 pages of cipher that exposed sweden's

attempt to foment an uprising in england. he virtually guaranteed hisfuture when he

testified before the house of lords in 1723. here, francisatterbury, bishop of rochester,

was being tried by his peers forattempting to set a pretender on the english throne.the

pretender's cause exhorted the allegiance of many in england,and the nation's attention

focused on atterbury's trial. most of the factsabout the alleged conspiracy had come from his

interceptedcorrespondence, and the most inculpatory evidence had been extractedfrom the

portions in cipher by willes and by anthony corbiere, a formerforeign service official in his

mid-thirties who had also been appointed adecypherer in 1719. the lords "thought it proper

to call the decypherersbefore them, in order to their being satisfied of the truth of

thedecyphering." to demonstrate this, willes and corbiere deposed, that several letters,

written in this cypher, had beendecyphered by them separately, one being many miles distant

inthe country, and the other in town; and yet their decypheringagreed;that facts, unknown

to them and the government at the timeof their decyphering, had been verified in every

circumstance bysubsequent discoveries that a supplement of this cypher, having been

found amongdennis kelly's papers the latter end of july, agreed with the keythey had formed

of that cypher the april before;that the decyphering of the letters signed jones

lllington and1378, being afterwards applied by them to others written in thesame cypher, did

immediately make pertinent sense, and such ashad an evident connexion and coherence with

the parts of thoseletters that were out of cypher, though the words in cypher wererepeated

in different paragraphs, and differently combined. the two decypherers appeared before the

lords on several occasionsto swear to their solutions. attenbury twice objected and was

twice overruled. but on may 7, as willes wastestifying to the cryptanalysis of the three most

incriminatory letters ofall, and the bishop felt the noose tightening around him, he

persisted inquestioning willes on the validity of the reading though the house

hadsupported willes' refusal to answer. he raised such a commotion that heand his counsel were

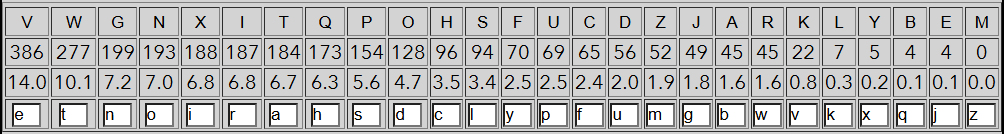
ordered to withdraw, and the lords voted upon theproposition, "that it is the opinion of

this house that it is not consistentwith the public safety, to ask the decypherers any

questions, which maytend to discover the art or mystery of decyphering." it was resolved

inthe affirmative, the solutions were accepted, and atterbury, largely onthis evidence, was

found guilty, deprived of office, and banished from therealm.



**Figure 5:** Substituted letters