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
Ceban Vasile

Checked: asist. univ. Dumitru Nirca

Chișinău 2024

## Topic: Mono-alphabetic Cipher

## Tasks:

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

## Theoretical notes:

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

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

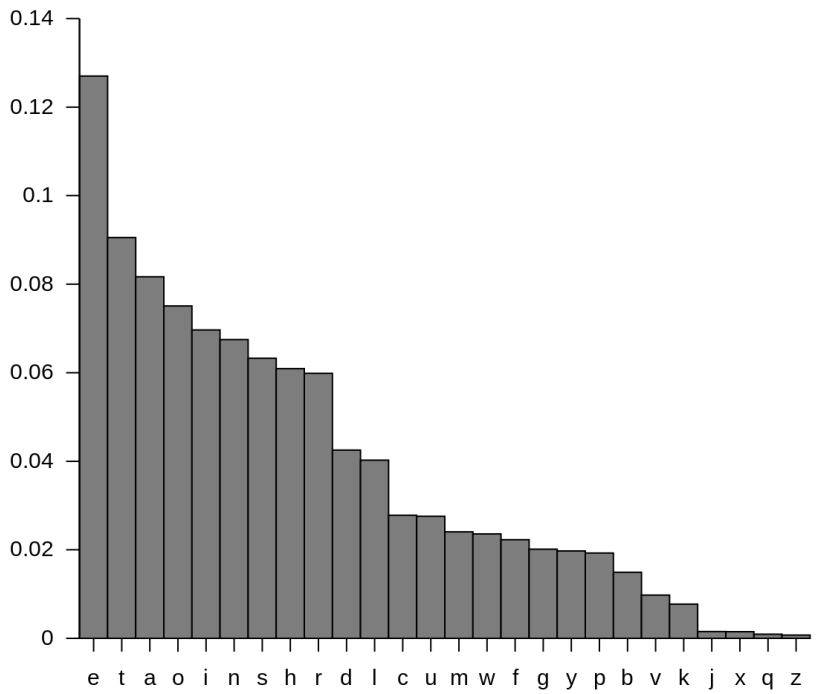



**Fig.1**: English letter frequency

| Letter | Frequency | Letter | Frequency |
|---|---|---|---|
| E | 11.16% | M | 3.01% |
| A | 8.50% | H | 3.00% |
| R | 7.58% | G | 2.47% |
| I | 7.54% | B | 2.07% |
| O | 7.16% | F | 1.81% |
| T | 6.95% | Y | 1.78% |
| N | 6.65% | W | 1.29% |
| S | 5.74% | K | 1.10% |
| L | 5.49% | V | 1.01% |
| C | 4.54% | X | 0.29% |
| U | 3.63% | Z | 0.27% |
| D | 3.38% | J | 0.20% |
| P | 3.17% | Q | 0.20% |

doi:10.1371/journal.pone.0152774.t002

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

# Implementation(Var. Nr.2)

I have a cryptogram c = *Wqv tooxwxng nc pvhivhf wn wqv witgpcniztwxngp uinodhvohifuwnjituqf. Widv, xw rtp zniv nc t jtzv wqtg tgfwqxgj vspv—xw pndjqwwn ovstf hnzuivqvgpxng cni ngsf wqv pqniwvpw unppxasv wxzv, gnw wqvsngjvpw—tgo wqv hifuwtgtsfpxp rtp, sxlvrxpv, edpw t udmmsv. Vjfuw'p rtpwqdp t bdtpx hifuwnsnjf xg hngwitpw wn wqv ovtosf pvixndp phxvghv nc wnotf.Fvw jivtw wqxgjp qtkv pztss avjxggxgjp, tgo wqvpv qxvinjsfuqp oxoxghsdov, wqndjq xg tg xzuvicvhw ctpqxng, wqv wrn vsvzvgwp nc pvhivhf tgowitgpcniztwxng wqtw hnzuixpv wqv vppvgwxts twwixadwvp nc wqv phxvghv. Tgopn hifuwnsnjf rtp anig. Xg xwp cxipw 3,000 fvtip, xw oxo gnw jinr pwvtoxsf. Hifuwnsnjf tinpvxgovuvgovgwsf xg ztgf usthvp, tgo xg znpw nc wqvz xw oxvo wqv ovtwqp ncxwp hxkxsxmtwxngp. Xg nwqvi usthvp, xw pdikxkvo, vzavoovo xg t sxwvitwdiv,tgo cinz wqxp wqv gvyw jvgvitwxng hndso hsxza wn qxjqvi svkvsp.Adw uinjivpp rtp psnr tgo evilf. Zniv rtp snpw wqtg ivwtxgvo. Zdhq nc wqvqxpwnif nc hifuwnsnjf nc wqxp wxzv xp t utwhqrnil, t hitmf bdxsw ncdgivstwvo xwvzp, puindwxgj, csndixpqxgj, rxwqvixgj. Ngsf wnrtio wqvRvpwvig Ivgtxpptghv onvp wqv thhivwxgj lgnrsvojv avjxg wn adxso du tznzvgwdz. Wqv pwnif nc hifuwnsnjf odixgj wqvpv fvtip xp, xg nwqvi rniop,vythwsf wqv pwnif nc ztglxgo. Hqxgt, wqv ngsf qxjq hxkxsxmtwxng nc tgwxbdxwf wn dpv xovnjituqxhrixwxgj, pvvzp gvkvi wn qtkv ovkvsnuvo zdhq ivts hifuwnjituqf —uviqtup cni wqtw ivtpng. Xg ngv htpv lgnrg cni zxsxwtif udiunpvp, wqv11wq-hvgwdif hnzuxstwxng, Rd-hqxgj wpdgj-ftn ("Vppvgwxtsp cinz ZxsxwtifHstppxhp"), ivhnzzvgovo t widv xc pztss hnov. Wn t sxpw nc 40 ustxgwvywxwvzp, itgjxgj cinz ivbdvpwp cni anrp tgo tiinrp wn wqv ivuniw nc tkxhwnif, wqv hniivpungovgwp rndso tppxjg wqv cxipw 40 xovnjitzp nc tunvz. Wqvg, rqvg t sxvdwvgtgw rxpqvo, cni vytzusv, wn ivbdvpw znivtiinrp, qv rtp wn Rixwv wqv hniivpungoxgj xovnjitz tw t puvhxcxvo usthvng tg nioxgtif oxputwhq tgo pwtzu qxp pvts ng xw.Xg Hqxgt'p jivtw gvxjqani wn wqv rvpw, Xgoxt, rqnpv hxkxsxmtwxngsxlvrxpv ovkvsnuvo vtisf tgo wn qxjq vpwtwv, pvkvits cnizp nc pvhivwhnzzdgxhtwxngp rviv lgnrg tgo, t Uutivgwsf, uithwxhvo. Wqv Tiwqt-ptpwit, t hstppxh*

*rnil ng pwtwvhitcw twwixadwvo wn Ltdwxsft, xg ovphixaxgjwqv vpuxngtjv pvikxhv nc Xgoxt tp uithwxhtssf ixoosxgj wqv hndgwif rxwqp Uxvp, ivhnzzvgovo wqtw wqv nccxhvip nc wqv xgpwxwdwvp nc £ puxngtjv jxkvwqvxi puxvp wqvxi tppxjgzvgwp af pvhivw rixwxgj.Uviqtup znpw xgwvivpwxgj wn hifuwnsnjxpwp, tztwvdi niuincvppxngts, xp wqtw Ktwpftftgt'p ctzndp wvywannl nc vinwxhp, wqv Ltztpdwit,sxpwp pvhivw rixwxgj tp ngv nc wqv 64 tiwp, ni fnjtp, wqtw rnzvgpqndso lgnr tgo uithwxhv. Wqv cndiwq jivtw hxkxsxmtwxng nc tgwxbdxwf, wqvZvpnun-wtzxtg, itwqvi utitssvsvo Vjfuw vtisf xg xwp hifuwnjituqxhvknsdwxng, adw wqvg pdiutppvo xw. Wqdp, xg wqv stpw uvixno nc hdgvxcnizrixwxgj, xg hnsnuqngp rixwwvg tw Didl (xg uivpvgw-otf Xitb) dgovi wqvPvsvdhxo lxgjp xg wqv stpw cvr phniv fvtip avcniv wqv Hqixpwxtg vit,nhhtpxngts phixavp hngkviwvo wqvxi gtzvp xgwn gdzavip. Wqvvghxuqvizvgw—xc pdhq xw av—ztf qtkv avvg ngsf cni tzdpvzvgw ni wnpqnr ncc.*

So first we look at the frequencies as shown bellow:

| Letter | Count | Frequency | Replace |
|---|---|---|---|
| V | 273 | 11.04 | e |
| W | 250 | 10.11 | t |
| X | 201 | 8.13 | a |
| N | 195 | 7.89 | i |
| P | 188 | 7.6 | s |
| T | 185 | 7.48 | n |
| I | 169 | 6.83 | o |
| G | 165 | 6.67 | r |
| Q | 111 | 4.49 | h |
| H | 89 | 3.6 | d |
| S | 84 | 3.4 | c |
| O | 79 | 3.19 | l |
| U | 66 | 2.67 | m |
| F | 64 | 2.59 | p |
| Z | 61 | 2.47 | m |
| J | 59 | 2.39 | u |
| D | 59 | 2.39 | f |
| C | 56 | 2.26 | y |

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

And we also look at this table:

| E | T | A | O | I | N | S | H | R | D | L | C | U | M | W | F | G | Y | P | B | V | K | J | X | Q | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12.7 | 9.1 | 8.2 | 7.5 | 7.0 | 6.7 | 6.3 | 6.1 | 6.0 | 4.3 | 4.0 | 2.8 | 2.8 | 2.4 | 2.4 | 2.2 | 2.0 | 2.0 | 1.9 | 1.5 | 1.0 | 0.8 | 0.15 | 0.15 | 0.10 | 0.07 |

The frequencies of the intercept are:

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

And as we see the “V” in my text has a similar appearance and the most used letter “E” so I conclude *V* **->** *e* and also by the look of it I see that the “W” and “T” have the same percentage so I assume that *W* **->** *t*. So I get: *tQe TOOXtXNG NC PeHIeHF tN tQe tITGPCNIZTtXNGP UINODHeOHIFUtNJITUQF. tIDe, Xt RTP ZNIe NC T*

*JTZe tQTG TGFtQXGJ eSPe—Xt PNDJQttN OeSTF HNZUIeQeGPXNG CNI NGSF tQe PQNItePt UNPPXASe*

*tXZe, GNt tQeSNGJePt—TGO tQe HIFUtTGTSFPXP RTP, SXLeRXPe, EDPt T UDMMSe. eJFUt'P RTPtQDP T*

*BDTPX HIFUtNSNJF XG HNGtITPt tN tQe OeTOSF PeIXNDP PHXeGHe NC tNOTF.Fet JIeTt tQXGJP QTKe*

*PZTSS AeJXGGXGJP, TGO tQePe QXeINJSFUQP OXOXGHSDOe, tQNDJQ XG TG XZUeICeHt CTPQXNG, tQe tRN*

*eSeZeGtP NC PeHIeHF TGOtITGPCNIZTtXNG tQTt HNZUIXPe tQe ePPeGtXTS TttIXADteP NC tQe*

*PHXeGHe. TGOPN HIFUtNSNJF RTP ANIG. XG XtP CXIPt 3,000 FeTIP, Xt OXO GNt JINR PteTOXS*

*HIFUtNSNJF TINPeXGOeUeGOeGtSF XG ZTGF USTHeP, TGO XG ZNPt NC tQeZ Xt OXeO tQe OeTtQP NCXtP*
*HXKXSXMTtXNGP. XG NtQeI USTHeP, Xt PDIKXKeO, eZAeOOeO XG T SXteITtDIe,TGO CINZ tQXP tQe*
*GeYt JeGeITtXNG HNDSO HSXZA tN QXJQeI SeKeSP.ADt UINJIePP RTP PSNR TGO EeILF. ZNIe RTP SNPt tQTG*
*IetTXGeO. ZDHQ NC tQeQXPtNIF NC HIFUtNSNJF NC tQXP tXZe XP T UTtHQRNIL, T HITMF BDXSt*
*NCDGIeSTteO XteZP, PUINDtXGJ, CSNDIXPQXGJ, RXtQeIXGJ. NGSF tNRTIO tQeRePteIG IeGTXPPTGHe*
*ONeP tQe THHIetXGJ LGNRSeOJe AeJXG tN ADXSO DU TZNZeGtDZ. tQe PtNIF NC HIFUtNSNJF ODIXGJ*
*tQePe FeTIP XP, XG NtQeI RNIOP,eYTHtSF tQe PtNIF NC ZTGLXGO. HQXGT, tQe NGSF QXJQ HXKXSXMTtXNG*
*NC TGtXBDXtF tN DPe XOeNJITUQXHRIXtXGJ, PeeZP GeKeI tN QTKe OeKeSNUeO ZDHQ IeTS HIFUtNJITUQF*
*—UeIQTUP CNI tQTt IeTPNG. XG NGe HTPe LGNRG CNI ZXSXtTIF UDIUNPeP, tQe11tQ-HeGtDIF*
*HNZUXSTtXNG, RD-HQXGJ tPDGJ-FTN ("ePPeGtXTSP CINZ ZXSXtTIFHSTPPXHP"), IeHNZZeGOeO T tIDe XC*
*PZTSS HNOe. tN T SXPt NC 40 USTXGteYtXteZP, ITGJXGJ CINZ IeBDePtP CNI ANRP TGO TIINRP tN tQe*
*IeUNIt NC TKXHtNIF, tQe HNIIePUNGOeGtP RNDSO TPPXJG tQe CXIPt 40 XOeNJITZP NC TUNeZ. tQeG,*
*RQeG T SXeDteGTGt RXPQeO, CNI eYTZUSe, tN IeBDePt ZNIeTIINRP, Qe RTP tN RIXte tQe HNIIePUNGOXGJ*
*XOeNJITZ Tt T PUeHXCXeO USTHeNG TG NIOXGTIF OXPUTtHQ TGO PtTZU QXP PeTS NG Xt.XG HQXGT'P JIeTt*
*GeXJQANI tN tQe RePt, XGOXT, RQNPe HXKXSXMTtXNGSXLeRXPe OeKeSNUeO eTISF TGO tN QXJQ ePtTte,*
*PeKeITS CNIZP NC PeHIetHNZZDGXHTtXNGP ReIe LGNRG TGO, T UUTIeGtSF, UITHtXHeO. tQe TItQT-PTPtIT,*
*T HSTPPXH RNIL NG PtTteHITCt TttIXADteO tN LTDtXSFT, XG OePHIXAXGJtQe ePUXNGTJe PeIKXHe NC*
*XGOXT TP UITHtXHTSSF IXOOSXGJ tQe HNDGtIF RXtQP UXeP, IeHNZZeGOeO tQTt tQe NCCXHeIP NC tQe*
*XGPtXtDteP NC £ PUXNGTJe JXKetQeXI PUXeP tQeXI TPPXJGZeGtP AF PeHIet RIXtXGJ.UeIQTUP ZNPt*
*XGteIePtXGJ tN HIFUtNSNJXPtP, TZTteDI NIUINCePPXNGTS, XP tQTt KTtPFTFTGT'P CTZNDP teYtANNL*
*NC eINtXHP, tQe LTZTPDtIT,SXPtP PeHIet RIXtXGJ TP NGe NC tQe 64 TItP, NI FNJTP, tQTt RNZeGPQNDSO*
*LGNR TGO UITHtXHe. tQe CNDItQ JIeTt HXKXSXMTtXNG NC TGtXBDXtF, tQeZePNUN-tTZXTG, ITtQeI*

*UTITSSeSeO eJFUt eTISF XG XtP HIFUtNJITUQXHeKNSDtXNG, ADt tQeG PDIUTPPeO Xt. tQDP, XG tQe*
*STPt UeIXNO NC HDGeXCNIZRIXtXGJ, XG HNSNUQNGP RIXtteG Tt DIDL (XG UIePeGt-OTF XITB) DGOeI*
*tQePeSeDHXO LXGJP XG tQe STPt CeR PHNIe FeTIP AeCNIe tQe HQIXPtXTG eIT,NHHTPXNGTS PHIXAeP*
*HNGKeIteO tQeXI GTZeP XGtN GDZAeIP. tQeeGHXUQeIZeGt—XC PDHQ Xt Ae—ZTF QTKe AeeG NGSF CNI*
*TZDPeZeGt NI tNPQNR NCC.*

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 a has 7.5% frequency and i has 8.1% which is more closer to X value 8%, so we have word "it", so **X -> i**. Also we have "tN" combination, tha can be "to" let's take a look. In english frequency table "O" is on 4th place and in my frequency table N is 4th with similar frequency %, therefore **N -> o.**

*the TOOitioG oC PeHIeHF to the tITGPCoIZTtioGP UIoODHeOHIFUtoJITUhF. tIDe, it RTP ZoIe oC T*
*JTZe thTG TGFthiGJ eSPe—it PoDJhtto OeSTF HoZUIeheGPioG CoI oGSF the PhoItePt UoPPiASe tiZe, Got theSoGJePt—TGO the HIFUtTGTSFPiP RTP, SiLeRiPe, EDPt T UDMMSe. eJFUt'P RTPthDP T*
*BDTPi HIFUtoSoJF iG HoGtITPt to the OeTOSF PeIioDP PHieGHe oC toOTF.Fet JIeTt thiGJP hTKe*
*PZTSS AeJiGGiGJP, TGO thePe hieIoJSFUhP OiOiGHSDOe, thoDJh iG TG iZUeICeHt CTPhioG, the tRo*
*eSeZeGtP oC PeHIeHF TGOtITGPCoIZTtioG thTt HoZUIiPe the ePPeGtiTS TttIiADteP oC the PHieGHe. TGOPo HIFUtoSoJF RTP AoIG. iG itP CiIPt 3,000 FeTIP, it OiO Got JIoR PteTOiSF. HIFUtoSoJF TIoPeiGOeUeGOeGtSF iG ZTGF USTHeP, TGO iG ZoPt oC theZ it OieO the OeTthP oCitP*
*HiKiSiMTtioGP. iG otheI USTHeP, it PDIKiKeO, eZAeOOeO iG T SiteITtDIe,TGO CIoZ thiP the GeYt JeGeITtioG HoDSO HSiZA to hiJheI SeKeSP.ADt UIoJIePP RTP PSoR TGO EeILF. ZoIe RTP SoPt thTG*
*IetTiGeO. ZDHh oC thehiPtoIF oC HIFUtoSoJF oC thiP tiZe iP T UTtHhRoIL, T HITMF BDiSt oCDGIeSTteO iteZP, PUIoDtiGJ, CSoDIiPhiGJ, RitheIiGJ. oGSF toRTIO theRePteIG IeGTiPPTGHe OoeP the THHIetiGJ LGoRSeOJe AeJiG to ADiSO DU TZoZeGtDZ. the PtoIF oC HIFUtoSoJF ODIiGJ*
*thePe FeTIP iP, iG otheI RoIOP,eYTHtSF the PtoIF oC ZTGLiGO. HhiGT, the oGSF hiJh HiKiSiMTtioG oC TGtiBDitF to DPe iOeoJITUhiHRIitiGJ, PeeZP GeKeI to hTKe OeKeSoUeO ZDHh IeTS HIFUtoJITUhF —UeIhTUP CoI thTt IeTPoG. iG oGe HTPe LGoRG CoI ZiSitTIF UDIUoPeP, the11th-HeGtDIF*

*HoZUiSTtioG, RD-HhiGJ tPDGJ-FTo ("ePPeGtiTSP CIoZ ZiSitTIFHSTPPiHP"), IeHoZZeGOeO T tIDe iC*
*PZTSS HoOe. to T SiPt oC 40 USTiGteYtiteZP, ITGJiGJ CIoZ IeBDePtP CoI AoRP TGO TIIoRP to the*
*IeUoIt oC TKiHtoIF, the HoIIePUoGOeGtP RoDSO TPPiJG the CiIPt 40 iOeoJITZP oC TUoeZ. theG,*
*RheG T SieDteGTGt RiPheO, CoI eYTZUSe, to IeBDePt ZoIeTIIoRP, he RTP to RIite the HoIIePUoGOiGJ*
*iOeoJITZ Tt T PUeHiCieO USTHeoG TG oIOiGTIF OiPUTtHh TGO PtTZU hiP PeTS oG it.iG HhiGT'P JIeTt*
*GeiJhAoI to the RePt, iGOiT, RhoPe HiKiSiMTtioGSiLeRiPe OeKeSoUeO eTISF TGO to hiJh ePtTte, PeKeITS CoIZP oC PeHIetHoZZDGiHTtioGP ReIe LGoRG TGO, T UUTIeGtSF, UITHtiHeO. the TIthT-PTPtIT,*
*T HSTPPiH RoIL oG PtTteHITCt TttIiADteO to LTDtiSFT, iG OePHIiAiGJthe ePUioGTJe PeIKiHe oC*
*iGOiT TP UITHtiHTSSF IiOOSiGJ the HoDGtIF RithP UieP, IeHoZZeGOeO thTt the oCCiHeIP oC the*
*iGPtitDteP oC £ PUioGTJe JiKetheiI PUieP theiI TPPiJGZeGtP AF PeHIet RIitiGJ.UeIhTUP ZoPt*
*iGteIeptiGJ to HIFUtoSoJiPtP, TZTteDI oIUIoCePPioGTS, iP thTt KTtPFTFTGT'P CTZoDP teYtAooL*
*oC eIotiHP, the LTZTPDtIT,SiPtP PeHIet RIitiGJ TP oGe oC the 64 TItP, oI FoJTP, thTt RoZeGPhoDSO*
*LGoR TGO UITHtiHe. the CoDIth JIeTt HiKiSiMTtioG oC TGtiBDitF, theZePoUo-tTZiTG, ITtheI*
*UTITSSeSeO eJFUt eTISF iG itP HIFUtoJITUhiHeKoSDtioG, ADt theG PDIUTPPeO it. thDP, iG the*
*STPt UeIioO oC HDGeiCoIZRIitiGJ, iG HoSoUhoGP RIitteG Tt DIDL (iG UIePeGt-OTF iITB) DGOeI*
*thePeSeDHiO LiGJP iG the STPt CeR PHoIe FeTIP AeCoIe the HhIiPtiTG eIT,oHHTPioGTS PHIiAeP*
*HoGKeIteO theiI GTZeP iGto GDZAeIP. theeGHiUheIZeGt—iC PDHh it Ae—ZTF hTKe AeeG oGSF CoI*
*TZDPeZeGt oI toPhoR oCC.*

Next we have a lot of occurrency of T letter which can be replaced with a, also to assume this change we can observe the “Tt” combination which will be transformed in “at” and has logic. Therefore **T -> a**. Also 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 “TGO” “aGO” or “anO” so I conclude that “O” may be “D” because this what is used in English so **O -> d**.

Till now we have this:

| Letter | Count | Frequency | Replace |
|---|---|---|---|
| V | 273 | 11.04 | e |
| W | 250 | 10.11 | t |
| X | 201 | 8.13 | i |
| N | 195 | 7.89 | o |
| P | 188 | 7.6 | p |
| T | 185 | 7.48 | a |
| I | 169 | 6.83 | i |
| G | 165 | 6.67 | n |
| Q | 111 | 4.49 | h |
| H | 89 | 3.6 | h |

**Fig.5**: Frequency of cryptogram letters new

And the text: *the addition oC PeHIeHF to the tIanPCoIZationP UIodDHedHIFUtoJIaUhF. tIDe, it RaP ZoIe oC a*
*JaZe than anFthinJ eSPe—it PoDJhtto deSaF HoZUIehenPion CoI onSF the PhoItePt UoPPiASe*
*tiZe, not theSonJePt—and the HIFUtanaSFPiP RaP, SiLeRiPe, EDPt a UDMMSe. eJFUt'P RaPthDP a*
*BDaPi HIFUtoSoJF in HontIaPt to the deadSF PeIioDP PHienHe oC todaF.Fet JIeat thinJP haKe*
*PZaSS AeJinninJP, and thePe hieIoJSFUhP didinHSDde, thoDJh in an iZUeICeHt CaPhion, the tRo*
*eSeZentP oC PeHIeHF andtIanPCoIZation that HoZUIiPe the ePPentiaS attIiADteP oC the PHienHe. andPo HIFUtoSoJF RaP AoIn. in itP CiIPt 3,000 FeaIP, it did not JIoR PteadiSF. HIFUtoSoJF aIoPeindeUendentSF in ZanF USaHeP, and in ZoPt oC theZ it died the deathP oCitP*
*HiKiSiMationP. in otheI USaHeP, it PDIKiKed, eZAedded in a SiteIatDIe,and CIoZ thiP the neYt JeneIation HoDSd HSiZA to hiJheI SeKeSP.ADt UIoJIePP RaP PSoR and EeILF. ZoIe RaP SoPt than*
*Ietained. ZDHh oC thehiPtoIF oC HIFUtoSoJF oC thiP tiZe iP a UatHhRoIL, a HIaMF BDiSt*
*oCDnIeSated iteZP, PUIoDtinJ, CSoDIiPhinJ, RitheIinJ. onSF toRaId theRePteIn IenaiPPanHe*
*doeP the aHHIetinJ LnoRSedJe AeJin to ADiSd DU aZoZentDZ. the PtoIF oC HIFUtoSoJF dDIinJ*

*thePe FeaIP iP, in otheI RoIdP,eYaHtSF the PtoIF oC ZanLind. Hhina, the onSF hiJh HiKiSiMation*
*oC antiBDitF to DPe ideoJIaUhiHRIitinJ, PeeZP neKeI to haKe deKeSoUed ZDHh IeaS HIFUtoJIaUhF*
*—UeIhaUP CoI that IeaPon. in one HaPe LnoRn CoI ZiSitaIF UDIUoPeP, the11th-HentDIF HoZUiSation, RD-HhinJ tPDnJ-Fao ("ePPentiaSP CIoZ ZiSitaIFHSaPPiHP"), IeHoZZended a tIDe iC*
*PZaSS Hode. to a SiPt oC 40 USainteYtiteZP, IanJinJ CIoZ IeBDePtP CoI AoRP and aIIoRP to the*
*IeUoIt oC aKiHtoIF, the HoIIePUondentP RoDSd aPPiJn the CiIPt 40 ideoJIaZP oC aUoeZ. then,*
*Rhen a SieDtenant RiPhed, CoI eYaZUSe, to IeBDePt ZoIeaIIoRP, he RaP to RIite the HoIIePUondinJ*
*ideoJIaZ at a PUeHiCied USaHeon an oIdinaIF diPUatHh and PtaZU hiP PeaS on it.in Hhina'P JIeat*
*neiJhAoI to the RePt, india, RhoPe HiKiSiMationSiLeRiPe deKeSoUed eaISF and to hiJh ePtate,*
*PeKeIaS CoIZP oC PeHIetHoZZDniHationP ReIe LnoRn and, a UUaIentSF, UIaHtiHed. the aItha-PaPtIa,*
*a HSaPPiH RoIL on PtateHIaCt attIiADted to LaDtiSFa, in dePHIiAinJthe ePUionaJe PeIKiHe oC*
*india aP UIaHtiHaSSF IiddSinJ the HoDntIF RithP UieP, IeHoZZended that the oCCiHeIP oC the*
*inPtitDteP oC £ PUionaJe JiKetheiI PUieP theiI aPPiJnZentP AF PeHIet RIitinJ.UeIhaUP ZoPt*
*inteIePtinJ to HIFUtoSoJiPtP, aZateDI oIUIoCePPionaS, iP that KatPFaFana'P CaZoDP teYtAooL*
*oC eIotiHP, the LaZaPDtIa,SiPtP PeHIet RIitinJ aP one oC the 64 aItP, oI FoJaP, that RoZenPhoDSd*
*LnoR and UIaHtiHe. the CoDIth JIeat HiKiSiMation oC antiBDitF, theZePoUo-taZian, IatheI*
*UaIaSSeSed eJFUt eaISF in itP HIFUtoJIaUhiHeKoSDtion, ADt then PDIUaPPed it. thDP, in the*
*SaPt UeIiod oC HDneiCoIZRIitinJ, in HoSoUhonP RIitten at DIDL (in UIePent-daF iIaB) DndeI*
*thePeSeDHid LinJP in the SaPt CeR PHoIe FeaIP AeCoIe the HhIiPtian eIa,oHHaPionaS PHIiAeP*
*HonKeIted theiI naZeP into nDZAeIP. theenHiUheIZent—iC PDHh it Ae—ZaF haKe Aeen onSF CoI*
*aZDPeZent oI toPhoR oCC.*

Now above I have “iP” “aP” “hiP” so we can assume that **P -> s**. Also a lot of “oC” and at end of text “oCC” therefore we assume that text is of and off, let’s change **C -> f.**
Now above I have the word “theiI” so I conclude it must be “their” so **I -> r**.
After we apply it:

*the addition of seHreHF to the transforZations UrodDHedHrFUtoJraUhF. trDe, it Ras Zore of a*
*JaZe than anFthinJ eSse—it soDJhtto deSaF HoZUrehension for onSF the shortest UossiASe*
*tiZe, not theSonJest—and the HrFUtanaSFsis Ras, SiLeRise, EDst a UDMMSe. eJFUt's RasthDs a*
*BDasi HrFUtoSoJF in Hontrast to the deadSF serioDs sHienHe of todaF.Fet Jreat thinJs haKe*
*sZaSS AeJinninJs, and these hieroJSFUhs didinHSDde, thoDJh in an iZUerfeHt fashion, the tRo*
*eSeZents of seHreHF andtransforZation that HoZUrise the essentiaS attriADtes of the*
*sHienHe. andso HrFUtoSoJF Ras Aorn. in its first 3,000 Fears, it did not JroR steadiSF.*
*HrFUtoSoJF aroseindeUendentSF in ZanF USaHes, and in Zost of theZ it died the deaths ofits*
*HiKiSiMations. in other USaHes, it sDrKiKed, eZAedded in a SiteratDre,and froZ this the*
*neYt Jeneration HoDSd HSiZA to hiJher SeKeSs.ADt UroJress Ras sSoR and EerLF. Zore Ras Sost than*
*retained. ZDHh of thehistorF of HrFUtoSoJF of this tiZe is a UatHhRorL, a HraMF BDiSt*
*ofDnreSated iteZs, sUroDtinJ, fSoDrishinJ, RitherinJ. onSF toRard theRestern renaissanHe*
*does the aHHretinJ LnoRSedJe AeJin to ADiSd DU aZoZentDZ. the storF of HrFUtoSoJF dDrinJ*
*these Fears is, in other Rords,eYaHtSF the storF of ZanLind. Hhina, the onSF hiJh HiKiSiMation*
*of antiBDitF to Dse ideoJraUhiHRritinJ, seeZs neKer to haKe deKeSoUed ZDHh reaS HrFUtoJraUhF*
*—UerhaUs for that reason. in one Hase LnoRn for ZiSitarF UDrUoses, the11th-HentDrF*
*HoZUiSation, RD-HhinJ tsDnJ-Fao ("essentiaSs froZ ZiSitarFHSassiHs"), reHoZZended a trDe if*
*sZaSS Hode. to a Sist of 40 USainteYtiteZs, ranJinJ froZ reBDests for AoRs and arroRs to the*
*reUort of aKiHtorF, the HorresUondents RoDSd assiJn the first 40 ideoJraZs of aUoeZ. then,*
*Rhen a SieDtenant Rished, for eYaZUSe, to reBDest ZorearroRs, he Ras to Rrite the HorresUondinJ*
*ideoJraZ at a sUeHified USaHeon an ordinarF disUatHh and staZU his seaS on it.in Hhina's Jreat*
*neiJhAor to the Rest, india, Rhose HiKiSiMationSiLeRise deKeSoUed earSF and to hiJh estate,*
*seKeraS forZs of seHretHoZZDniHations Rere LnoRn and, a UUarentSF, UraHtiHed. the artha-sastra,*

*a HSassiH RorL on stateHraft attriADted to LaDtiSFa, in desHriAinJthe esUionaJe serKiHe of*
*india as UraHtiHaSSF riddSinJ the HoDntrF Riths Uies, reHoZZended that the offiHers of the*
*institDtes of £ sUionaJe JiKetheir sUies their assiJnZents AF seHret RritinJ.UerhaUs Zost*
*interestinJ to HrFUtoSoJists, aZateDr orUrofessionaS, is that KatsFaFana's faZoDs teYtAooL*
*of erotiHs, the LaZasDtra,Sists seHret RritinJ as one of the 64 arts, or FoJas, that RoZenshoDSd*
*LnoR and UraHtiHe. the foDrth Jreat HiKiSiMation of antiBDitF, theZesoUo-taZian, rather*
*UaraSSeSed eJFUt earSF in its HrFUtoJraUhiHeKoSDtion, ADt then sDrUassed it. thDs, in the*
*Sast Ueriod of HDneiforZRritinJ, in HoSoUhons Rritten at DrDL (in Uresent-daF iraB) Dnder*
*theseSeDHid LinJs in the Sast feR sHore Fears <u>Aefore</u> the Hhristian era,oHHasionaS sHriAes*
*HonKerted their naZes into nDZAers. theenHiUherZent—if sDHh it Ae—ZaF haKe Aeen onSF for*
*aZDseZent or toshoR off.*

Also I have the "*<u>Aefore</u>*" so the best word for it is "before", so **A -> b.** Also at the beginning we have the word "Rhen" and the bests match is "Then" or "When", since we have already T, then **R -> W.** Same for "*trDe"* wich I assume is "true"

so apply **D -> u.**

*the addition of seHreHF to the transforZations UroduHedHrFUtoJraUhF. true, it was Zore of a*
*JaZe than anFthinJ eSse—it souJhtto deSaF HoZUrehension for onSF the shortest UossibSe*
*tiZe, not theSonJest—and the HrFUtanaSFsis was, SiLewise, Eust a UuMMSe. eJFUt's wasthus a*
*Buasi HrFUtoSoJF in Hontrast to the deadSF serious sHienHe of todaF.Fet Jreat thinJs haKe*
*sZaSS beJinninJs, and these hieroJSFUhs didinHSude, thouJh in an iZUerfeHt fashion, the two*
*eSeZents of seHreHF andtransforZation that HoZUrise the essentiaS attributes of the*
*sHienHe. andso HrFUtoSoJF was born. in its first 3,000 Fears, it did not Jrow steadiSF.*
*HrFUtoSoJF aroseindeUendentSF in ZanF USaHes, and in Zost of theZ it died the deaths ofits*
*HiKiSiMations. in other USaHes, it surKiKed, eZbedded in a Siterature,and froZ this the*
*neYt Jeneration HouSd HSiZb to hiJher SeKeSs.but UroJress was sSow and EerLF. Zore was Sost than*
*retained. ZuHh of thehistorF of HrFUtoSoJF of this tiZe is a UatHhworL, a HraMF BuiSt*

*ofunreSated iteZs, sUroutinJ, fSourishinJ, witherinJ. onSF toward thewestern renaissanHe does the aHHretinJ LnowSedJe beJin to buiSd uU aZoZentuZ. the storF of HrFUtoSoJF durinJ these Fears is, in other words,eYaHtSF the storF of ZanLind. Hhina, the onSF hiJh HiKiSiMation of antiBuitF to use ideoJraUhiHwritinJ, seeZs neKer to haKe deKeSoUed ZuHh reaS HrFUtoJraUhF —UerhaUs for that reason. in one Hase Lnown for ZiSitarF UurUoses, the11th-HenturF HoZUiSation, wu-HhinJ tsunJ-Fao ("essentiaSs froZ ZiSitarFHSassiHs"), reHoZZended a true if sZaSS Hode. to a Sist of 40 USainteYtiteZs, ranJinJ froZ reBuests for bows and arrows to the reUort of aKiHtorF, the HorresUondents wouSd assiJn the first 40 ideoJraZs of aUoeZ. then, when a Sieutenant wished, for eYaZUSe, to reBuest Zorearrows, he was to write the HorresUondinJ ideoJraZ at a sUeHified USaHeon an ordinarF disUatHh and staZU his seaS on it.in Hhina's Jreat neiJhbor to the west, india, whose HiKiSiMationSiLewise deKeSoUed earSF and to hiJh estate, seKeraS forZs of seHretHoZZuniHations were Lnown and, a UUarentSF, UraHtiHed. the artha-sastra, a HSassiH worL on stateHraft attributed to LautiSFa, in desHribinJthe esUionaJe serKiHe of india as UraHtiHaSSF riddSinJ the HountrF withs Uies, reHoZZended that the offiHers of the institutes of £ sUionaJe JiKetheir sUies their assiJnZents bF seHret writinJ.UerhaUs Zost interestinJ to HrFUtoSoJists, aZateur orUrofessionaS, is that KatsFaFana's faZous teYtbooL of erotiHs, the LaZasutra,Sists seHret writinJ as one of the 64 arts, or FoJas, that woZenshouSd Lnow and UraHtiHe. the fourth Jreat HiKiSiMation of antiBuitF, theZesoUo-taZian, rather UaraSSeSed eJFUt earSF in its HrFUtoJraUhiHeKoSution, but then surUassed it. thus, in the Sast Ueriod of HuneiforZwritinJ, in HoSoUhons written at uruL (in Uresent-daF iraB) under theseSeuHid LinJs in the Sast few sHore Fears before the Hhristian era,oHHasionaS sHribes HonKerted their naZes into nuZbers. theenHiUherZent—if suHh it be—ZaF haKe been onSF for aZuseZent or toshow off.*

Now most of the words we can guess: Like the "*writinJ*" "writing" so **J -> g**. "*in the Sast few sHore Fears before the Hhristian era*" can be interpreted as "in the last few score years before the Christian era" and we got **S -> l, H -> c, F -> y.**

| Letter | Count | Frequency | Replace |
|---|---|---|---|
| P | 252 | 10.19 | None |
| T | 250 | 10.11 | None |
| H | 200 | 8.09 | None |
| O | 195 | 7.89 | None |
| A | 185 | 7.48 | b |
| N | 165 | 6.67 | None |
| M | 127 | 5.14 | None |
| C | 84 | 3.4 | f |
| L | 79 | 3.19 | None |

**Fig.5**: Frequency of cryptogram letters new

Text:

*the addition of secrecy to the transforZations UroducedcryUtograUhy. true, it was Zore of a gaZe than anything else—it soughtto delay coZUrehension for only the shortest Uossible tiZe, not thelongest—and the cryUtanalysis was, liLewise, Eust a UuMMle. egyUt's wasthus a Buasi cryUtology in contrast to the deadly serious science of today.yet great things haKe sZall beginnings, and these hieroglyUhs didinclude, though in an iZUerfect fashion, the two eleZents of secrecy andtransforZation that coZUrise the essential attributes of the science. andso cryUtology was born. in its first 3,000 years, it did not grow steadily. cryUtology aroseindeUendently in Zany Ulaces, and in Zost of theZ it died the deaths ofits ciKiliMations. in other Ulaces, it surKiKed, eZbedded in a literature,and froZ this the neYt generation could cliZb to higher leKels.but Urogress was slow and EerLy. Zore was lost than*

*retained. Zuch of thehistory of cryUtology of this tiZe is a UatchworL, a craMy Built ofunrelated iteZs, sUrouting, flourishing, withering. only toward thewestern renaissance does the accreting Lnowledge begin to build uU aZoZentuZ. the story of cryUtology during these years is, in other words,eYactly the story of ZanLind. china, the only high ciKiliMation of antiBuity to use ideograUhicwriting, seeZs neKer to haKe deKeloUed Zuch real cryUtograUhy*

*—UerhaUs for that reason. in one case Lnown for Zilitary UurUoses, the11th-century coZUilation, wu-ching tsung-yao ("essentials froZ Zilitaryclassics"), recoZZended a true if sZall code. to a list of 40 UlainteYtiteZs, ranging froZ reBuests for bows and arrows to the reUort of aKictory, the corresUondents would assign the first 40 ideograZs of aUoeZ. then,*

*when a lieutenant wished, for eYaZUle, to reBuest Zorearrows, he was to write the corresUonding ideograZ at a sUecified Ulaceon an ordinary disUatch and staZU his seal on it.in china's great*
*neighbor to the west, india, whose ciKiliMationliLewise deKeloUed early and to high estate, seKeral forZs of secretcoZZunications were Lnown and, a UUarently, Uracticed. the artha-sastra,*
*a classic worL on statecraft attributed to Lautilya, in describingthe esUionage serKice of india as Uractically riddling the country withs Uies, recoZZended that the officers of the institutes of £ sUionage giKetheir sUies their assignZents by secret writing.UerhaUs Zost*
*interesting to cryUtologists, aZateur orUrofessional, is that Katsyayana's faZous teYtbooL of erotics, the LaZasutra,lists secret writing as one of the 64 arts, or yogas, that woZenshould Lnow and Uractice. the fourth great ciKiliMation of antiBuity, theZesoUo-taZian, rather Uaralleled egyUt early in its cryUtograUhiceKolution, but then surUassed it. thus, in the last Ueriod of cuneiforZwriting, in coloUhons written at uruL (in Uresent-day iraB) under theseleucid Lings in the last few score years before the christian era,occasional scribes conKerted their naZes into nuZbers. theenciUherZent—if such it be—Zay haKe been only for aZuseZent or toshow off.*

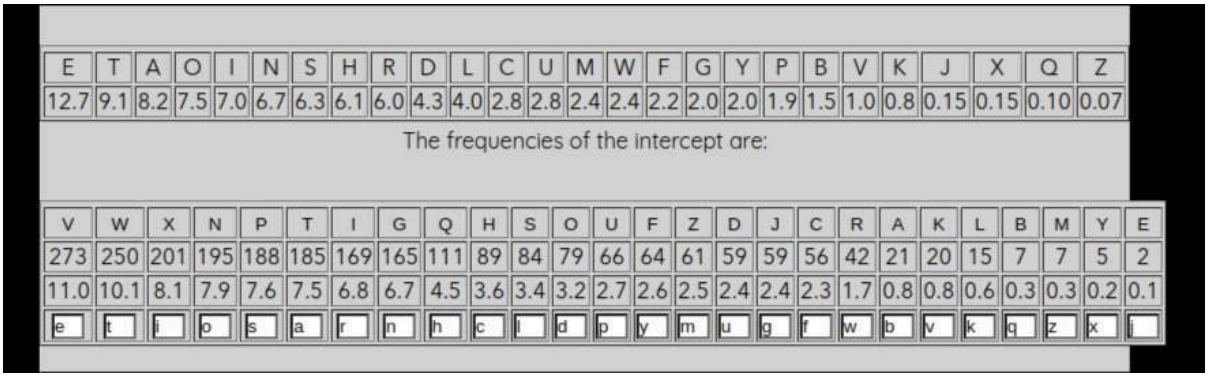
Now “transforZations” is “transformations” so Z -> m, “Lnown” is “known” so L -> k. The words “a UUarently” “Uracticed” “Uractice” “Uractically” we can assume that **U -> p.** From “*seKeral”* we can deduce **K -> v.**
Text:
*the addition of secrecy to the transformations producedcryptography. true, it was more of a*
*game than anything else—it soughtto delay comprehension for only the shortest possible*
*time, not thelongest—and the cryptanalysis was, likewise, Eust a puMMle. egypt's wasthus a*
*Buasi cryptology in contrast to the deadly serious science of today.yet great things have*
*small beginnings, and these hieroglyphs didinclude, though in an imperfect fashion, the two*
*elements of secrecy andtransformation that comprise the essential attributes of the*
*science. andso cryptology was born. in its first 3,000 years, it did not grow steadily.*
*cryptology aroseindependently in many places, and in most of them it died the deaths ofits*

*civiliMations. in other places, it survived, embedded in a literature,and from this the*
*neYt generation could climb to higher levels.but progress was slow and Eerky. more was lost than*
*retained. much of thehistory of cryptology of this time is a patchwork, a craMy Built*
*ofunrelated items, sprouting, flourishing, withering. only toward thewestern renaissance*
*does the accreting knowledge begin to build up amomentum. the story of cryptology during*
*these years is, in other words,eYactly the story of mankind. china, the only high civiliMation*
*of antiBuity to use ideographicwriting, seems never to have developed much real cryptography*
*—perhaps for that reason. in one case known for military purposes, the11th-century*
*compilation, wu-ching tsung-yao ("essentials from militaryclassics"), recommended a true if*
*small code. to a list of 40 plainteYtitems, ranging from reBuests for bows and arrows to the*
*report of avictory, the correspondents would assign the first 40 ideograms of apoem. then,*
*when a lieutenant wished, for eYample, to reBuest morearrows, he was to write the corresponding*
*ideogram at a specified placeon an ordinary dispatch and stamp his seal on it.in china's great*
*neighbor to the west, india, whose civiliMationlikewise developed early and to high estate,*
*several forms of secretcommunications were known and, a pparently, practiced. the artha-sastra,*
*a classic work on statecraft attributed to kautilya, in describingthe espionage service of*
*india as practically riddling the country withs pies, recommended that the officers of the*
*institutes of £ spionage givetheir spies their assignments by secret writing.perhaps most*

*interesting to cryptologists, amateur orprofessional, is that vatsyayana's famous teYtbook*
*of erotics, the kamasutra,lists secret writing as one of the 64 arts, or yogas, that womenshould*
*know and practice. the fourth great civiliMation of antiBuity, themesopo-tamian, rather*
*paralleled egypt early in its cryptographicevolution, but then surpassed it. thus, in the*
*last period of cuneiformwriting, in colophons written at uruk (in present-day iraB) under*
*theseleucid kings in the last few score years before the christian era,occasional scribes*
*converted their names into numbers. theencipherment—if such it be—may have been only for*
*amusement or toshow off.*

Words *"puMMle"* is "puzzle" so **M -> z**, *"teYtbook"* "textbook" so **Y -> x**, "*antiBuity"* is "antiquity" so **B -> q** and last "*Eust" is "just"* so **E -> j**.
These are all letters.

And the alphabet looks something like this:



| E | T | A | O | I | N | S | H | R | D | L | C | U | M | W | F | G | Y | P | B | V | K | J | X | Q | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12.7 | 9.1 | 8.2 | 7.5 | 7.0 | 6.7 | 6.3 | 6.1 | 6.0 | 4.3 | 4.0 | 2.8 | 2.8 | 2.4 | 2.4 | 2.2 | 2.0 | 2.0 | 1.9 | 1.5 | 1.0 | 0.8 | 0.15 | 0.15 | 0.10 | 0.07 |

The frequencies of the intercept are:

| V | W | X | N | P | T | I | G | Q | H | S | O | U | F | Z | D | J | C | R | A | K | L | B | M | Y | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 273 | 250 | 201 | 195 | 188 | 185 | 169 | 165 | 111 | 89 | 84 | 79 | 66 | 64 | 61 | 59 | 59 | 56 | 42 | 21 | 20 | 15 | 7 | 7 | 5 | 2 |
| 11.0 | 10.1 | 8.1 | 7.9 | 7.6 | 7.5 | 6.8 | 6.7 | 4.5 | 3.6 | 3.4 | 3.2 | 2.7 | 2.6 | 2.5 | 2.4 | 2.4 | 2.3 | 1.7 | 0.8 | 0.8 | 0.6 | 0.3 | 0.3 | 0.2 | 0.1 |
| e | t | i | o | s | a | r | n | h | c | l | d | p | y | m | u | g | f | w | b | v | k | q | z | x | j |

Fig 10. Decryted Alphabet.

And the Full text is :

*the addition of secrecy to the transformations producedcryptography. true, it was more of a game than anything else—it soughtto delay comprehension for only the shortest possible time, not thelongest—and the cryptanalysis was, likewise, just a puzzle. egypt's wasthus a quasi cryptology in contrast to the deadly serious science of today.yet great things have small beginnings, and these hieroglyphs didinclude, though in an imperfect fashion, the two elements of secrecy andtransformation that comprise the essential attributes of the science. andso cryptology was born. in its first 3,000 years, it did not grow steadily. cryptology aroseindependently in many places, and in most of them it died the deaths ofits*

*civilizations. in other places, it survived, embedded in a literature,and from this the next generation could climb to higher levels.but progress was slow and jerky. more was lost than retained. much of thehistory of cryptology of this time is a patchwork, a crazy quilt ofunrelated items, sprouting, flourishing, withering. only toward thewestern renaissance does the accreting knowledge begin to build up amomentum. the story of cryptology during these years is, in other words,exactly the story of mankind. china, the only high civilization of antiquity to use ideographicwriting, seems never to have developed much real cryptography —perhaps for that reason. in one case known for military purposes, the11th-century compilation, wu-ching tsung-yao ("essentials from militaryclassics"), recommended a true if small code. to a list of 40 plaintextitems, ranging from requests for bows and arrows to the report of avictory, the correspondents would assign the first 40 ideograms of apoem. then, when a lieutenant wished, for example, to request morearrows, he was to write the corresponding ideogram at a specified placeon an ordinary dispatch and stamp his seal on it.in china's great neighbor to the west, india, whose civilizationlikewise developed early and to high estate, several forms of secretcommunications were known and, a pparently, practiced. the artha-sastra, a classic work on statecraft attributed to kautilya, in describingthe espionage service of india as practically riddling the country withs pies, recommended that the officers of the institutes of £ spionage givetheir spies their assignments by secret writing.perhaps most interesting to cryptologists, amateur orprofessional, is that vatsyayana's famous textbook of erotics, the kamasutra,lists secret writing as one of the 64 arts, or yogas, that womenshould know and practice. the fourth great civilization of antiquity, themesopo-tamian, rather paralleled egypt early in its cryptographicevolution, but then surpassed it. thus, in the last period of cuneiformwriting, in colophons written at uruk (in present-day iraq) under theseleucid kings in the last few score years before the christian era,occasional scribes converted their names into numbers. theencipherment—if such it be—may have been only for amusement or toshow off*

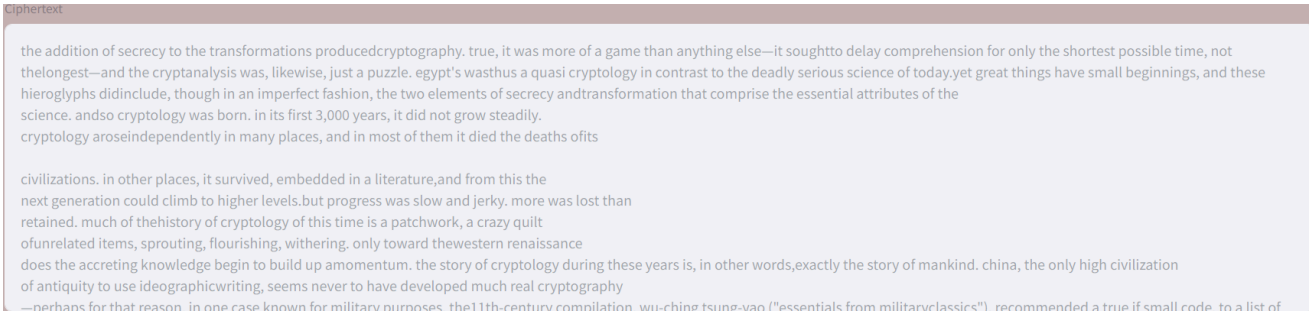



Fig 11. Final Result.