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: Pereteatcu Arina FAF - 223,

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.

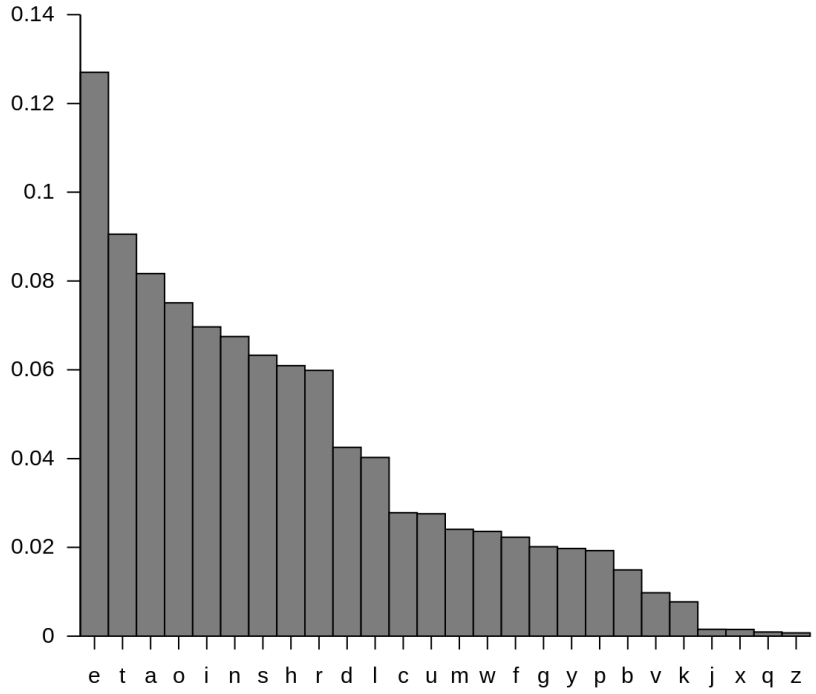

Fig.1: English letter frequency

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. 20)

I have a cryptogram c = *T cvr zngwqp avcniv wqv Gnkvzavi nuvgxgj nc wqv oxptiztzvgwhngcvivghv xg Rtpqxgjwng, otxsf hndixvi pvikxhv rtp pvw du avwrvvg wqvAsthl Hqtzavi tgo wqv Pwtwv Ovutiwzvgw. Tg nccxhxts jixggxgjsfivztilvo wqtw Pwtwv'p duuvi vhqvsngp rviv ovsxjqwvo rxwq wqv hifuwtg-tsfpwp' rnil tgo ivto wqv pnsdwxngp vkvif znigxgj rxwq wqvxi nitgjv edxhvtgo hnccvv. Wqv hngcvivghv pndjqw wn sxzxw wqv wnggtjv nc htuxwts pqxup,tgo tp gvjnwxtwxngp rviv uinhvvoxgj wnrtio xwp hqxvc ivpdsw—wqv Cxkv-Unrvi Wivtwf wqtw thhniovo wnggtjvp xg hviwtxg itwxnp wn wqv DgxwvoPwtwvp, Aixwtxg, Citghv, Xwtsf, tgo Etutg—Ftiosvf'p wvtz rtp ivtoxgj wqvpvhivw xgpwidhwxngp nc wqv gvjnwxtwnip. "Wqv Asthl Hqtzavi, answvo,qxoovg, jdtiovo, pvvp tss, qvtip tss," qv rinwv stwvi, itwqvizvsnoitztwxhtssf. "Wqndjq wqv asxgop tiv oitrg tgo wqv rxgonrp qvtkxsfhdiwtxgvo, xwp cti-pvvlxgj vfvp uvgvwitwv wqv pvhivw hngcvivghv hqtzaviptw Rtpqxgjwng, Wnlfn, Sngong, Utixp, Jvgvkt, Inzv. Xwp pvgpxwxkv vtiphtwhq wqv ctxgwvpw rqxpuvixgjp xg wqv cnivxjg htuxwtsp nc wqv rniso."Vthq gtwxng gtwditssf wixvo wn nawtxg wqv znpw ctknitasv wnggtjv itwxncni xwpvsc; wqv znpw tjjivppxkv xg xwp vccniwp rtp Etutg, rqxhq vkvg wqvgrtp oivtzxgj vyutgpxngxpw oivtzp xg Tpxt adw cvtivo wn nccvgo wqvDgxwvo Pwtwvp. Tw wqv qvxjqw nc wqv hngcvivghv, rqvg Etutg rtpovztgoxgj t itwxn nc 10 wn 7 rxwq*

wqv Dgxwvo Pwtwvp tgo Jivtw Aixwtxg,wqv Asthl Hqtzavi ivto rqtw Ftiosvf stwvi htssvo wqv znpw xzuniwtgwwvsvjitz xw vkvi pnskvo."Xw xp gvhvpptif wn tknxo tgf hstpq rxwq Jivtw Aixwtxg tgo Tzvixht,utiwxhdstisf Tzvixht, xg ivjtio wn wqv tiztzvgw sxzxwtwxng bdvpwxng," wqvEtutgvpv Cnivxjg Nccxhv htasvo xwp tzatpptoni xg Rtpqxgjwng ngGnkvzavi 28. "Fnd rxss wn wqv dwznpw ztxgwtxg t zxoosv twwxwdov tgoivondasv fndi vccniwp wn htiif ndw ndi unsxhf. Xg htpv nc xgvkxwtasvgvhvppxwf fnd rxss rnil wn vpwtasxpq fndi pvhngo uinunpts nc 10 wn 6.5. Xc,xg puxwv nc fndi dwznpw vccniwp, xw avhnzvp gvhvpptif xg kxvr nc wqvpxwdtwxng tgo xg wqv xgwvivpwp nc jvgvits unsxhf wn ctss athl ng fndiuinunpts Gn. 3, fnd rxss vgovtkni wn sxzxw wqv unrvi nc hnghvgwitwxng tgoztgvdkvi nc wqv Uthxcxh af t jdtitgwvv wn ivodhv ni tw svtpw wn ztxgwtxgwqv pwtwdp bdn nc Uthxcxh ovcvgpvp tgo wn ztlv tg tovbdtwv ivpviktwxngrqxhq rxss ztlv hsvti wqtw [wqxp xp] ndi xgwvgwxng xg tjivvxgj wn t 10 wn 6 itwxn. Gn4 xp wn av tknxovo tp cti tp unppxasv."Vthq 0.5 xg wqv itwxn zvtgw 50,000 wngp nc htuxwts pqxup, ni tandw tatwwsv pqxu tgo t qtsc. Rxwq wqv xgcniztwxng xg wqxp zvpptjv wvssxgj wqvTzvixhtg gvjnwxtwnip wqtw Etutg rndso fxvso xc uivppvo, tss wqvf qto wnon rtp uivpp. Wqxp Pvhivwtif nc Pwtwv Hqtisvp Vktgp Qdjqvp oxo, tgo ngOvhvzavi 10 Etutg htuxwdstwvo, xgpwidhwxgj xwp gvjnwxtwni, xg t htasvivto af wqv Asthl Hqtzavi, wqtw "wqviv xp gnwqxgj wn on adw thhvuw wqvitwxn uinunpvo af wqv Dgxwvo Pwtwvp." Tp pxjgvo, wqv Cxkv-Unrvi Wivtwftssnwwvo htuxwts pqxup wn wqv Dgxwvo Pwtwvp, Jivtw Aixwtxg, Etutg, Citghv,tgo Xwtsf xg wqv itwxn nc 10:10:6:3.3:3.3. Xw rtp hngpxovitasf svpp wqtgEtutg qto qnuvo cni. Qdjqvp pvgw Ftiosvf t svwwvi nc hnzzvgotwxng.Odixgj wqv hngcvivghv, wqv Asthl Hqtzavi qto wdigvo ndw zniv wqtg5,000 pnsdwxngp tgo witgpstwxngp. Ftiosvf gvtisf pdccvivo t gvikndpaivtlonrg, tgo xg Cvaidtif rvgw wn Tixmngt cni cndi zngwqp wn ivhnkviqxp qvtswq. Pvkvits nc qxp tppxpwtgwp qto tsivtof qto windasv xg wqxpivjtio. Ngv ataasvo xghnqvivgwsf; t jxis oivtzvo nc hqtpxgj tindgo wqvavoinnz t adssonj wqtw, rqvg htdjqw, qto "hnov" rixwwvg ng xwp pxov;tgnwqvi hndso sxjqwvg wqv vgnizndp pthl nc uvaasvp wqtw pqv htiixvo xg tivhdiixgj gxjqwztiv ngsf af cxgoxgj t pwngv tsngj t sngvsf avthq wqtwvythwsf ztwhqvo ngv nc qvi uvaasvp, rqxhq pqv hndso wqvg htpw xgwn wqvpvt. Tss wqivv ivpxjgvo.

So first we look at the frequencies as shown bellow:

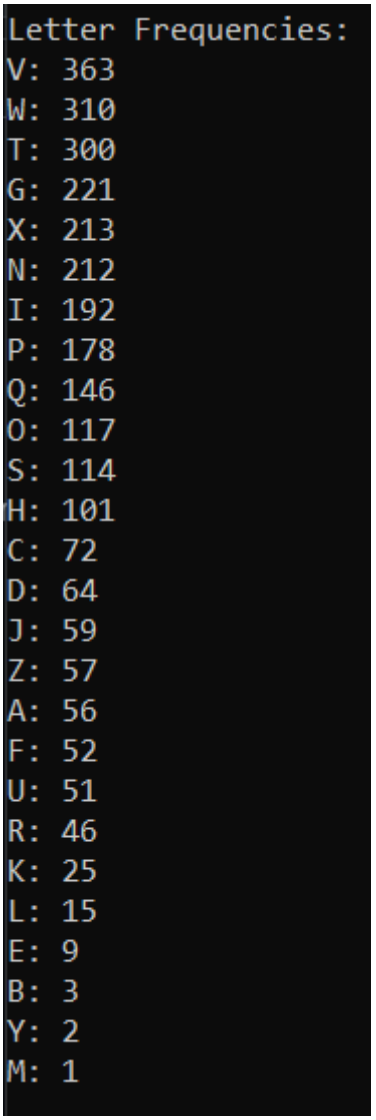

Fig.3: Frequency of cryptogram letters(in my case)

And we also look at this table:

V	W	T	G	X	N	I	P	Q	O	S	H	C	D	J	Z	A	F	U	R	K	L	E	B	Y	M
363	310	300	221	213	212	192	178	146	117	114	101	72	64	59	57	56	52	51	46	25	15	9	3	2	1
12.2	10.4	10.1	7.4	7.2	7.1	6.4	6.0	4.9	3.9	3.8	3.4	2.4	2.1	2.0	1.9	1.9	1.7	1.7	1.5	0.8	0.5	0.3	0.1	0.1	0.0
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

Fig.4: Frequency of cryptogram letters

As we can see, The letter V and W appear more frequently, therefore we can change them to E and T.

So I get: *A UeB FNOtRH GeUNSe tRe ONVeFGeS NPeOIOW NU tRe DIHASFAFeOtCNOUeSeOCe IO BAHRIOWtNO, DAILY*

CNMSIeS HeSVICe BAH Het MP GetBeeO tReGLACK CRAFGeS AOD tRe HtAte DePAStFeOt. AO NUUICIAL

WSIOOIOWLYSeFASKeD tRAt HtAte'H MPPeS eCReLNOH BeSe DeLIWRteD BItR tRe CSYPtAO-ALYHtH' BNSK AOD

SeAD tRe HNLMtINOH eVeSY FNSOIOW BItR tReIS NSAOWe JMICeAOD CNUUee. tRe CNOUeSeOCe HNMWRt

tN LIFIt tRe tNOOAWe NU CAPItAL HRIPH,AOD AH OeWNtIAtINOH BeSe PSNCeeDIOW tNBASD ItH CRIeU

SeHMLt-tRe UIVe-PNBeS tSeAtY tRAt ACCNSDeD tNOOAWeH IO CeStAIO SAtINH tN tRe MOIteDHtAteH, GSItAIO, USAOCe, ItALY, AOD JAPAO-YASDLeY'H teAF BAH SeADIOW tReHeCSet

IOHtSMCtINOH NU tRe OeWNtIAtNSH. "tRe GLACK CRAFGeS, GNLteD,RIDDeO, WMASDeD, HeeH ALL, ReASH

ALL," Re BSNte LAteS, SAtReSFeLNDSAFAtICALLY. "tRNMWR tRe GLIODH ASe DSABO AOD tRe BIODNBH

ReAVILYCMStAIOeD, ItH UAS-HeeKIOW eYeH PeOetSAte tRe HeCSet CNOUeSeOCe CRAFGeSHAt

BAHRIOWtNO, tNKYN, LNODNO, PASIH, WeOeVA, SNFe. ItH HeOHItIVe eASHCAtCR tRe UAIOteHt

BRIHPeSIOWH IO tRe UNSeIWO CAPItALH NU tRe BNSLD."eACR OAtINO OAtMSALLY tSIeD tN NGtAIO tRe

FNHt UAVNSAGLe tNOOAWe SAtINUNS ItHeLU; tRe FNHt AWWSeHHIVe IO ItH eUUNStH BAH JAPAO, BRICR

eVeO tReOBAH DSeAFIOW eQPAOHINOIHt DSeAFH IO AHIA GMt UeASeD tN NUUeOD tReMOIteD HtAteH.

At tRe ReIWRt NU tRe CNOUeSeOCe, BReO JAPAO BAHDeFAODIOW A SAtIN NU 10 tN 7 BItR tRe MOIteD

HtAteH AOD WSeAt GSItAIO,tRe GLACK CRAFGeS SeAD BRAt YASDLeY LAteS CALLeD tRe FNHt

IFPNStAOtteLeWSAF It eVeS HNLVeD."It IH OeCeHHASY tN AVNID AOY CLAHR BItR WSeAt GSItAIO AOD

AFeSICA,PAStICMLASLY AFeSICA, IO SeWASD tN tRe ASFAFeOt LIFItAtINO XMeHtINO," tReJAPAOeHe

UNSeIWO NUUICe CAGLeD ItH AFGAHHADNS IO BAHRIOWtNO NOONVeFGeS 28. "YNM BILL tN tRe MtFNHt

FAIOtAIO A FIDDLe AttItMDe AODSeDNMGLe YNMS eUUNStH tN CASSY NMt NMS PNLICY. IO CAHe NU

IOeVItAGLeOeCeHHItY YNM BILL BNSK tN eHtAGLIHR YNMS HeCNOD PSNPNHAL NU 10 tN 6.5. IU,IO HPIte
NU YNMS MtFNHt eUUNStH, It GeCNFeH OeCeHHASY IO VIeB NU tReHItMAtINO AOD IO tRe IOteSeHtH
NU WeOeSAL PNLICY tN UALL GACK NO YNMSPSNPNHAL ON. 3, YNM BILL eODeAVNS tN LIFIt tRe PNBeS NU
CNOCeOtSAtINO AODFAOeMVeS NU tRe PACIUIC GY A WMASAOtee tN SeDMCe NS At LeAHt tN FAIOtAIOtRe
HtAtMH XMN NU PACIUIC DeUeOHeH AOD tN FAKe AO ADeXMAte SeHeSVAtINOBRICR BILL FAKe CLeAS tRAt
[tRIH IH] NMS IOteOtINO IO AWSeeIOW tN A 10 tN 6 SAtIN. ON4 IH tN Ge AVNIDeD AH UAS AH
PNHHIGLe."eACR 0.5 IO tRe SAtIN FeAOt 50,000 tNOH NU CAPItAL HRIPH, NS AGNMt AGAttLe HRIP AOD
A RALU. BItR tRe IOUNSFAtINO IO tRIH FeHHAWe teLLIOW tReAFeSICAO OeWNtIAtNSH tRAt JAPAO
BNMLD YIeLD IU PSeHHeD, ALL tReY RAD tNDN BAH PSeHH. tRIH HeCSetASY NU HtAte CRASLeH eVAOH
RMWReH DID, AOD NODeCeFGeS 10 JAPAO CAPItMLAteD, IOHtSMCtIOW ItH OeWNtIAtNS, IO A CAGLeSeAD
GY tRe GLACK CRAFGeS, tRAt "tReSe IH ONtRIOW tN DN GMt ACCePt tReSAtIN PSNPNHeD GY tRe
MOIteD HtAteH." AH HIWOeD, tRe UIVe-PNBeS tSeAtYALLNtteD CAPItAL HRIPH tN tRe MOIteD
HtAteH, WSeAt GSItAIO, JAPAO, USAOCe,AOD ItALY IO tRe SAtIN NU 10:10:6:3.3:3.3. It BAH
CNOHIDeSAGLY LeHH tRAOJAPAO RAD RNPeD UNS. RMWReH HeOt YASDLeY A LetteS NU CNFFeODAtINO.DMSIOW
tRe CNOUeSeOCe, tRe GLACK CRAFGeS RAD tMSOeD NMt FNSe tRAO5,000 HNLMtINOH AOD tSAOHLAtINOH.
YASDLeY OeASLY HMUUeSeD A OeSVNMHGSeAKDNBO, AOD IO UeGSMASY BeOt tN ASIZNOA UNS UNMS FNOtRH tN
SeCNVeSRIH ReALtR. HeVeSAL NU RIH AHHIHtAOtH RAD ALSeADY RAD tSNMGLe IO tRIHSeWASD. NOe GAGGLeD
IOCNReSeOtLY; A WISL DSeAFeD NU CRAHIOW ASNMOD tReGeDSNNF A GMLLDNW tRAt, BReO CAMWRt, RAD "CNDe"
BSItteO NO ItH HIDe;AONtReS CNMLD LIWRteO tRe eONSFNMH HACK NU PeGGLeH tRAt HRe CASSIeD IO
ASeCMSSIOW OIWRtFASe NOLY GY UIODIOW A HtNOe ALNOW A LNOeLY GeACR tRAteQACtLY FAtCReD NOe NU ReS
PeGGLeH, BRICR HRe CNMLD tReO CAHt IOtN tReHeA. ALL tRSee SeHIWOeD.

Now, we can see that the word “tRe” might be replaced by “tHe” , so replacing R->H we get:

A UeB FNOthR GeUNSe the ONVeFGeS NPeOIOW NU the DIRASFAFeOtCNOUeSeOCe IO BARhIOWtNO, DAILY
CNMSIeS ReSVICe BAR Ret MP GetBeeO theGLACK ChAFGeS AOD the RtAte DePAStFeOt. AO NUUICIAL
WSIOOIOWLYSeFASKeD thAt RtAte'R MPPeS eCheLNOR BeSe DeLIWhteD BIth the CSYPtAO-ALYRtR' BNSK AOD
SeAD the RNLMtINOR eVeSY FNSOIOW BIth theIS NSAOWe JMICeAOD CNUUee. the CNOUeSeOCe RNMWht
tN LIFIt the tNOOAWe NU CAPItAL RhIPR,AOD AR OeWNtIAtINOR BeSe PSNCeeDIOW tNBASD ItR ChIeU
SeRMLt-the UIVe-PNBeS tSeAtY thAt ACCNSDeD tNOOAWeR IO CeStAIO SAtINR tN the
MOIteDRtAteR, GSItAIO, USAOCe, ItALY, AOD JAPAO-YASDLeY'R teAF BAR SeADIOW theReCSet
IORtSMCtINOR NU the OeWNtIAtNSR. "the GLACK ChAFGeS, GNLteD,hIDDeO, WMASDeD, ReeR ALL, heASR
ALL," he BSNte LAteS, SAtheSFeLNDSAFAtICALLY. "thNMWh the GLIODR ASe DSABO AOD the BIODNBR
heAVILYCMStAIOeD, ItR UAS-ReeKIOW eYeR PeOetSAte the ReCSet CNOUeSeOCe ChAFGeSRAt
BARhIOWtNO, tNKYN, LNODNO, PASIR, WeOeVA, SNFe. ItR ReORItIVe eASRCAtCh the UAIOteRt
BhIRPeSIOWR IO the UNSeIWO CAPItALR NU the BNSLD."eACh OAtINO OAtMSALLY tSIeD tN NGtAIO the
FNRt UAVNSAGLe tNOOAWe SAtINUNS ItReLU; the FNRt AWWSeRRIVe IO ItR eUUNStR BAR JAPAO, BhICh
eVeO theOBAR DSeAFIOW eQPAORINOIRt DSeAFR IO ARIA GMt UeASeD tN NUUeOD theMOIteD RtAteR.
At the heIWht NU the CNOUeSeOCe, BheO JAPAO BARDeFAODIOW A SAtIN NU 10 tN 7 BIth the MOIteD
RtAteR AOD WSeAt GSItAIO,the GLACK ChAFGeS SeAD BhAt YASDLeY LAteS CALLeD the FNRt
IFPNStAOtteLeWSAF It eVeS RNLVeD."It IR OeCeRRASY tN AVNID AOY CLARh BIth WSeAt GSItAIO AOD
AFeSICA,PAStICMLASLY AFeSICA, IO SeWASD tN the ASFAFeOt LIFItAtINO XMeRtINO," theJAPAOeRe
UNSeIWO NUUICe CAGLeD ItR AFGARRADNS IO BARhIOWtNO NOONVeFGeS 28. "YNM BILL tN the MtFNRt
FAIOtAIO A FIDDLe AttItMDe AODSeDNMGLe YNMS eUUNStR tN CASSY NMt NMS PNLICY. IO CARe NU

IOeVItAGLeOeCeRRItY YNM BILL BNSK tN eRtAGLIRh YNMS ReCNOD PSNPNRAL NU 10 tN 6.5. IU,IO RPIte
NU YNMS MtFNRt eUUNStR, It GeCNFeR OeCeRRASY IO VIeB NU theRItMAtINO AOD IO the IOteSeRtR
NU WeOeSAL PNLICY tN UALL GACK NO YNMSPSNPNRAL ON. 3, YNM BILL eODeAVNS tN LIFIt the PNBeS NU
CNOCeOtSAtINO AODFAOeMVeS NU the PACIUIC GY A WMASAOtee tN SeDMCe NS At LeARt tN FAIOtAIOthe
RtAtMR XMN NU PACIUIC DeUeOReR AOD tN FAKe AO ADeXMAte SeReSVAtINOBhICh BILL FAKe CLeAS thAt
[thIR IR] NMS IOteOtINO IO AWSeeIOW tN A 10 tN 6 SAtIN. ON4 IR tN Ge AVNIDeD AR UAS AR
PNRRIGLe."eACh 0.5 IO the SAtIN FeAOt 50,000 tNOR NU CAPItAL RhIPR, NS AGNMt AGAttLe RhIP AOD
A hALU. BIth the IOUNSFAtINO IO thIR FeRRAWe teLLIOW theAFeSICAO OeWNtIAtNSR thAt JAPAO
BNMLD YIeLD IU PSeRReD, ALL theY hAD tNDN BAR PSeRR. thIR ReCSetASY NU RtAte ChASLeR eVAOR
hMWheR DID, AOD NODeCeFGeS 10 JAPAO CAPItMLAteD, IORtSMCtIOW ItR OeWNtIAtNS, IO A CAGLeSeAD
GY the GLACK ChAFGeS, thAt "theSe IR ONthIOW tN DN GMt ACCePt theSAtIN PSNPNReD GY the
MOIteD RtAteR." AR RIWOeD, the UIVe-PNBeS tSeAtYALLNtteD CAPItAL RhIPR tN the MOIteD
RtAteR, WSeAt GSItAIO, JAPAO, USAOCe,AOD ItALY IO the SAtIN NU 10:10:6:3.3:3.3. It BAR
CNORIDeSAGLY LeRR thAOJAPAO hAD hNPeD UNS. hMWheR ReOt YASDLeY A LetteS NU CNFFeODAtINO.DMSIOW
the CNOUeSeOCe, the GLACK ChAFGeS hAD tMSOeD NMt FNSe thAO5,000 RNLMtINOR AOD tSAORLAtINOR.
YASDLeY OeASLY RMUUeSeD A OeSVNMRGSeAKDNBO, AOD IO UeGSMASY BeOt tN ASIZNOA UNS UNMS FNOthR tN
SeCNVeShIR heALth. ReVeSAL NU hIR ARRIRtAOtR hAD ALSeADY hAD tSNMGLe IO thIRSeWASD. NOe GAGGLeD
IOCNheSeOtLY; A WISL DSeAFeD NU ChARIOW ASNMOD theGeDSNNF A GMLLDNW thAt, BheO CAMWht, hAD "CNDe"
BSItteO NO ItR RIDe;AONtheS CNMLD LIWhteO the eONSFNMR RACK NU PeGGLeR thAt Rhe CASSIeD IO
ASeCMSSIOW OIWhtFASe NOLY GY UIODIOW A RtNOe ALNOW A LNOeLY GeACh thAteQACtLY FAtCheD NOe NU heS
PeGGLeR, BhICh Rhe CNMLD theO CARt IOtN theReA. ALL thSee SeRIWOeD.

Here we observe that in the word “ALNOW” and “LNOELY” we can change N->O and we get:

A UeB FonthR GeUoSe the noVeFGeS oPenInW oU the DIRASFAFentConUeSenCe In BARhInWton, DAILY
CoMSIeS ReSVICe BAR Ret MP GetBeen theGLACK ChAFGeS AnD the RtAte DePAStFent. An oUUICIAL
WSInnInWLYSeFASKeD thAt RtAte'R MPPeS eCheLonR BeSe DeLIWhteD BIth the CSYPtAn-ALYRtR' BoSK AnD
SeAD the RoLMtIonR eVeSY FoSnInW BIth theIS oSAnWe JMICeAnD CoUUee. the ConUeSenCe RoMWht
to LIFIt the tonnAWe oU CAPItAL RhIPR,AnD AR neWotIAtIonR BeSe PSoCeeDInW toBASD ItR ChIeU
SeRMLt-the UIVe-PoBeS tSeAtY thAt ACCoSDeD tonnAWeR In CeStAIn SAtIoR to the
MnIteDRtAteR, GSItAIn, USAnCe, ItALY, AnD JAPAn-YASDLeY'R teAF BAR SeADInW theReCSet
InRtSMCtIonR oU the neWotIAtoSR. "the GLACK ChAFGeS, GoLteD,hIDDen, WMASDeD, ReeR ALL, heASR
ALL," he BSote LAteS, SAtheSFeLoDSAFAtICALLY. "thoMWh the GLInDR ASe DSABn AnD the BInDoBR
heAVILYCMStAIneD, ItR UAS-ReeKInW eYeR PenetSAte the ReCSet ConUeSenCe ChAFGeSRAt
BARhInWton, toKYo, LonDon, PASIR, WeneVA, SoFe. ItR RenRItIVe eASRCAtCh the UAInteRt
BhIRPeSInWR In the UoSeIWn CAPItALR oU the BoSLD."eACh nAtIon nAtMSALLY tSIeD to oGtAIn the
FoRt UAVoSAGLe tonnAWe SAtIoUoS ItReLU; the FoRt AWWSeRRIVe In ItR eUUoStR BAR JAPAn, BhICh
eVen thenBAR DSeAFInW eQPAnRIonIRt DSeAFR In ARIA GMt UeASeD to oUUenD theMnIteD RtAteR.
At the heIWht oU the ConUeSenCe, Bhen JAPAn BARDeFAnDInW A SAtIo oU 10 to 7 BIth the MnIteD
RtAteR AnD WSeAt GSItAIn,the GLACK ChAFGeS SeAD BhAt YASDLeY LAteS CALLeD the FoRt
IFPoStAntteLeWSAF It eVeS RoLVeD."It IR neCeRRASY to AVoID AnY CLARh BIth WSeAt GSItAIn AnD
AFeSICA,PAStICMLASLY AFeSICA, In SeWASD to the ASFAFent LIFItAtIon XMeRtIon," theJAPAneRe
UoSeIWn oUUICe CAGLeD ItR AFGARRADoS In BARhInWton onnoVeFGeS 28. "YoM BILL to the MtFoRt
FAIntAIn A FIDDLe AttItMDe AnDSeDoMGLe YoMS eUUoStR to CASSY oMt oMS PoLICY. In CARe oU
IneVItAGLeneCeRRItY YoM BILL BoSK to eRtAGLIRh YoMS ReConD PSoPoRAL oU 10 to 6.5. IU,In RPIte

oU YoMS MtFoRt eUUoStR, It GeCoFeR neCeRRASY In VIeB oU theRItMAtIon AnD In the InteSeRtR
oU WeneSAL PoLICY to UALL GACK on YoMSPSoPoRAL no. 3, YoM BILL enDeAVoS to LIFIt the PoBeS oU
ConCentSAtIon AnDFAneMVeS oU the PACIUIC GY A WMASAntee to SeDMCe oS At LeARt to FAIntAInthe
RtAtMR XMo oU PACIUIC DeUenReR AnD to FAKe An ADeXMAte SeReSVAtIonBhICh BILL FAKe CLeAS thAt
[thIR IR] oMS IntentIon In AWSeeInW to A 10 to 6 SAtIo. no4 IR to Ge AVoIDeD AR UAS AR PoRRIGLe."eACh 0.5 In the SAtIo FeAnt 50,000 tonR oU CAPItAL RhIPR, oS AGoMt AGAttLe RhIP AnD
A hALU. BIth the InUoSFAtIon In thIR FeRRAWe teLLInW theAFeSICAn neWotIAtoSR thAt JAPAn
BoMLD YIeLD IU PSeRReD, ALL theY hAD toDo BAR PSeRR. thIR ReCSetASY oU RtAte ChASLeR eVAnR
hMWheR DID, AnD onDeCeFGeS 10 JAPAn CAPItMLAteD, InRtSMCtInW ItR neWotIAtoS, In A CAGLeSeAD
GY the GLACK ChAFGeS, thAt "theSe IR nothInW to Do GMt ACCePt theSAtIo PSoPoReD GY the
MnIteD RtAteR." AR RIWneD, the UIVe-PoBeS tSeAtYALLotteD CAPItAL RhIPR to the MnIteD
RtAteR, WSeAt GSItAIn, JAPAn, USAnCe,AnD ItALY In the SAtIo oU 10:10:6:3.3:3.3. It BAR ConRIDeSAGLY LeRR thAnJAPAn hAD hoPeD UoS. hMWheR Rent YASDLeY A LetteS oU CoFFenDAtIon.DMSInW
the ConUeSenCe, the GLACK ChAFGeS hAD tMSneD oMt FoSe thAn5,000 RoLMtIonR AnD tSAnRLAtIonR.
YASDLeY neASLY RMUUeSeD A neSVoMRGSeAKDoBn, AnD In UeGSMASY Bent to ASIZonA UoS UoMS FonthR to
SeCoVeShIR heALth. ReVeSAL oU hIR ARRIRtAntR hAD ALSeADY hAD tSoMGLe In thIRSeWASD. one GAGGLeD
InCoheSentLY; A WISL DSeAFeD oU ChARInW ASoMnD theGeDSooF A GMLLDoW thAt, Bhen CAMWht, hAD "CoDe"
BSItten on ItR RIDe;AnotheS CoMLD LIWhten the enoSFoMR RACK oU PeGGLeR thAt Rhe CASSIeD In
ASeCMSSInW nIWhtFASe onLY GY UInDInW A Rtone ALonW A LoneLY GeACh thAteQACtLY FAtCheD one oU heS
PeGGLeR, BhICh Rhe CoMLD then CARt Into theReA. ALL thSee SeRIWneD.

Also, analyzing the words “oPenInW ” , “GetBeen ” we can change W->G , B->W, we get:

A Uew FonthR BeUoSe the noVeFBeS oPenIng oU the DIRASFAFentConUeSenCe In wARhIngton, DAILY
CoMSIeS ReSVICe wAR Ret MP Between theBLACK ChAFBeS AnD the RtAte DePAStFent. An oUUICIAL
gSInnIngLYSeFASKeD thAt RtAte'R MPPeS eCheLonR weSe DeLIghteD wIth the CSYPtAn-ALYRtR' woSK AnD
SeAD the RoLMtIonR eVeSY FoSnIng wIth theIS oSAnge JMICeAnD CoUUee. the ConUeSenCe RoMght
to LIFIt the tonnAge oU CAPItAL RhIPR,AnD AR negotIAtIonR weSe PSoCeeDIng towASD ItR ChIeU
SeRMLt-the UIVe-PoweS tSeAtY thAt ACCoSDeD tonnAgeR In CeStAIn SAtIoR to the
MnIteDRtAteR, BSItAIn, USAnCe, ItALY, AnD JAPAn-YASDLeY'R teAF wAR SeADIng theReCSet
InRtSMCtIonR oU the negotIAtoSR. "the BLACK ChAFBeS, BoLteD,hIDDen, gMASDeD, ReeR ALL, heASR
ALL," he wSote LAteS, SAtheSFeLoDSAFAtICALLY. "thoMgh the BLInDR ASe DSAwn AnD the wInDowR
heAVILYCMStAIneD, ItR UAS-ReeKIng eYeR PenetSAte the ReCSet ConUeSenCe ChAFBeSRAt
wARhIngton, toKYo, LonDon, PASIR, geneVA, SoFe. ItR RenRItIVe eASRCAtCh the UAInteRt whIRPeSIngR In the UoSeIgn CAPItALR oU the woSLD."eACh nAtIon nAtMSALLY tSIeD to oBtAIn the
FoRt UAVoSABLe tonnAge SAtIoUoS ItReLU; the FoRt AggSeRRIVe In ItR eUUoStR wAR JAPAn, whICh
eVen thenwAR DSeAFIng eQPAnRIonIRt DSeAFR In ARIA BMt UeASeD to oUUenD theMnIteD RtAteR.
At the heIght oU the ConUeSenCe, when JAPAn wARDeFAnDIng A SAtIo oU 10 to 7 wIth the MnIteD
RtAteR AnD gSeAt BSItAIn,the BLACK ChAFBeS SeAD whAt YASDLeY LAteS CALLeD the FoRt
IFPoStAntteLegSAF It eVeS RoLVeD."It IR neCeRRASY to AVoID AnY CLARh wIth gSeAt BSItAIn AnD
AFeSICA,PAStICMLASLY AFeSICA, In SegASD to the ASFAFent LIFItAtIon XMeRtIon," theJAPAneRe
UoSeIgn oUUICe CABLeD ItR AFBARRADoS In wARhIngton onnoVeFBeS 28. "YoM wILL to the MtFoRt
FAIntAIn A FIDDLe AttItMDe AnDSeDoMBLe YoMS eUUoStR to CASSY oMt oMS PoLICY. In CARe oU
IneVItABLeneCeRRItY YoM wILL woSK to eRtABLIRh YoMS ReConD PSoPoRAL oU 10 to 6.5. IU,In RPIte

oU YoMS MtFoRt eUUoStR, It BeCoFeR neCeRRASY In VIew oU theRItMAtIon AnD In the InteSeRtR
oU geneSAL PoLICY to UALL BACK on YoMSPSoPoRAL no. 3, YoM wILL enDeAVoS to LIFIt the PoweS oU
ConCentSAtIon AnDFAneMVeS oU the PACIUIC BY A gMASAntee to SeDMCe oS At LeARt to FAIntAInthe
RtAtMR XMo oU PACIUIC DeUenReR AnD to FAKe An ADeXMAte SeReSVAtIonwhICh wILL FAKe CLeAS thAt
[thIR IR] oMS IntentIon In AgSeeIng to A 10 to 6 SAtIo. no4 IR to Be AVoIDeD AR UAS AR
PoRRIBLe."eACh 0.5 In the SAtIo FeAnt 50,000 tonR oU CAPItAL RhIPR, oS ABoMt ABAttLe RhIP AnD
A hALU. wIth the InUoSFAtIon In thIR FeRRAge teLLIng theAFeSICAn negotIAtoSR thAt JAPAn
woMLD YIeLD IU PSeRReD, ALL theY hAD toDo wAR PSeRR. thIR ReCSetASY oU RtAte ChASLeR eVAnR
hMgheR DID, AnD onDeCeFBeS 10 JAPAn CAPItMLAteD, InRtSMCtIng ItR negotIAtoS, In A CABLeSeAD
BY the BLACK ChAFBeS, thAt "theSe IR nothIng to Do BMt ACCePt theSAtIo PSoPoReD BY the
MnIteD RtAteR." AR RIgneD, the UIVe-PoweS tSeAtYALLotteD CAPItAL RhIPR to the MnIteD
RtAteR, gSeAt BSItAIn, JAPAn, USAnCe,AnD ItALY In the SAtIo oU 10:10:6:3.3:3.3. It wAR
ConRIDeSABLY LeRR thAnJAPAn hAD hoPeD UoS. hMgheR Rent YASDLeY A LetteS oU CoFFenDAtIon.DMSIng
the ConUeSenCe, the BLACK ChAFBeS hAD tMSneD oMt FoSe thAn5,000 RoLMtIonR AnD tSAnRLAtIonR.
YASDLeY neASLY RMUUeSeD A neSVoMRBSeAKDown, AnD In UeBSMASY went to ASIZonA UoS UoMS FonthR to
SeCoVeShIR heALth. ReVeSAL oU hIR ARRIRtAntR hAD ALSeADY hAD tSoMBLe In thIRSegASD. one BABBLeD
InCoheSentLY; A gISL DSeAFeD oU ChARIng ASoMnD theBeDSooF A BMLLDog thAt, when CAMght, hAD "CoDe"
wSItten on ItR RIDe;AnotheS CoMLD LIghten the enoSFoMR RACK oU PeBBLeR thAt Rhe CASSIeD In
ASeCMSSIng nIghtFASe onLY BY UInDIng A Rtone ALong A LoneLY BeACh thAteQACtLY FAtCheD one oU heS
PeBBLeR, whICh Rhe CoMLD then CARt Into theReA. ALL thSee SeRIgneD.

Now, seeing “noVeFBeS ” and “BeUoSe ” we change F->M, S->R, and get:

A few monthS Before the noVemBer oPenIng of the DISArmAmentConferenCe In wAShIngton, DAILY
CourIer SerVICe wAS Set uP Between theBLACK ChAmBer AnD the StAte DePArtment. An offICIAL
grInnIngLYremArKeD thAt StAte'S uPPer eCheLonS were DeLIghteD wIth the CrYPtAn-ALYStS' worK AnD
reAD the SoLutIonS eVerY mornIng wIth theIr orAnge JuICeAnD Coffee. the ConferenCe Sought
to LImIt the tonnAge of CAPItAL ShIPS,AnD AS negotIAtIonS were ProCeeDIng towArD ItS ChIef
reSuLt-the fIVe-Power treAtY thAt ACCorDeD tonnAgeS In CertAIn rAtIoS to the
unIteDStAteS, BrItAIn, frAnCe, ItALY, AnD JAPAn-YArDLeY'S teAm wAS reADIng theSeCret
InStruCtIonS of the negotIAtorS. "the BLACK ChAmBer, BoLteD,hIDDen, guArDeD, SeeS ALL, heArS
ALL," he wrote LAter, rAthermeLoDrAmAtICALLY. "though the BLInDS Are DrAwn AnD the wInDowS
heAVILYCurtAIneD, ItS fAr-SeeKIng eYeS PenetrAte the SeCret ConferenCe ChAmBerSAt
wAShIngton, toKYo, LonDon, PArIS, geneVA, rome. ItS SenSItIVe eArSCAtCh the fAInteSt
whISPerIngS In the foreIgn CAPItALS of the worLD."eACh nAtIon nAturALLY trIeD to oBtAIn the
moSt fAVorABLe tonnAge rAtIofor ItSeLf; the moSt AggreSSIVe In ItS effortS wAS JAPAn, whICh
eVen thenwAS DreAmIng eQPAnSIonISt DreAmS In ASIA But feAreD to offenD theunIteD StAteS.
At the heIght of the ConferenCe, when JAPAn wASDemAnDIng A rAtIo of 10 to 7 wIth the unIteD
StAteS AnD greAt BrItAIn,the BLACK ChAmBer reAD whAt YArDLeY LAter CALLeD the moSt
ImPortAntteLegrAm It eVer SoLVeD."It IS neCeSSArY to AVoID AnY CLASh wIth greAt BrItAIn AnD
AmerICA,PArtICuLArLY AmerICA, In regArD to the ArmAment LImItAtIon XueStIon," theJAPAneSe
foreIgn offICe CABLeD ItS AmBASSADor In wAShIngton onnoVemBer 28. "You wILL to the utmoSt
mAIntAIn A mIDDLe AttItuDe AnDreDouBLe Your effortS to CArrY out our PoLICY. In CASe of
IneVItABLeneCeSSItY You wILL worK to eStABLISh Your SeConD ProPoSAL of 10 to 6.5. If,In SPIte
of Your utmoSt effortS, It BeComeS neCeSSArY In VIew of theSItuAtIon AnD In the IntereStS
of generAL PoLICY to fALL BACK on YourProPoSAL no. 3, You wILL enDeAVor to LImIt the Power of

ConCentrAtIon AnDmAneuVer of the PACIfIC BY A guArAntee to reDuCe or At LeASt to mAIntAInthe
StAtuS Xuo of PACIfIC DefenSeS AnD to mAKe An ADeXuAte reSerVAtIonwhICh wILL mAKe CLeAr thAt
[thIS IS] our IntentIon In AgreeIng to A 10 to 6 rAtIo. no4 IS to Be AVoIDeD AS fAr AS
PoSSIBLe."eACh 0.5 In the rAtIo meAnt 50,000 tonS of CAPItAL ShIPS, or ABout ABAttLe ShIP AnD
A hALf. wIth the InformAtIon In thIS meSSAge teLLIng theAmerICAn negotIAtorS thAt JAPAn
wouLD YIeLD If PreSSeD, ALL theY hAD toDo wAS PreSS. thIS SeCretArY of StAte ChArLeS eVAnS
hugheS DID, AnD onDeCemBer 10 JAPAn CAPItuLAteD, InStruCtIng ItS negotIAtor, In A CABLereAD
BY the BLACK ChAmBer, thAt "there IS nothIng to Do But ACCePt therAtIo ProPoSeD BY the
unIteD StAteS." AS SIgneD, the fIVe-Power treAtYALLotteD CAPItAL ShIPS to the unIteD
StAteS, greAt BrItAIn, JAPAn, frAnCe,AnD ItALY In the rAtIo of 10:10:6:3.3:3.3. It wAS
ConSIDerABLY LeSS thAnJAPAn hAD hoPeD for. hugheS Sent YArDLeY A Letter of CommenDAtIon.DurIng
the ConferenCe, the BLACK ChAmBer hAD turneD out more thAn5,000 SoLutIonS AnD trAnSLAtIonS.
YArDLeY neArLY SuffereD A nerVouSBreAKDown, AnD In feBruArY went to ArIZonA for four monthS to
reCoVerhIS heALth. SeVerAL of hIS ASSIStAntS hAD ALreADY hAD trouBLe In thISregArD. one BABBLeD
InCoherentLY; A gIrL DreAmeD of ChASIng ArounD theBeDroom A BuLLDog thAt, when CAught, hAD "CoDe"
wrItten on ItS SIDe;Another CouLD LIghten the enormouS SACK of PeBBLeS thAt She CArrIeD In
AreCurrIng nIghtmAre onLY BY fInDIng A Stone ALong A LoneLY BeACh thAteQACtLY mAtCheD one of her
PeBBLeS, whICh She CouLD then CASt Into theSeA. ALL three reSIgneD.

The final changes are Q->X

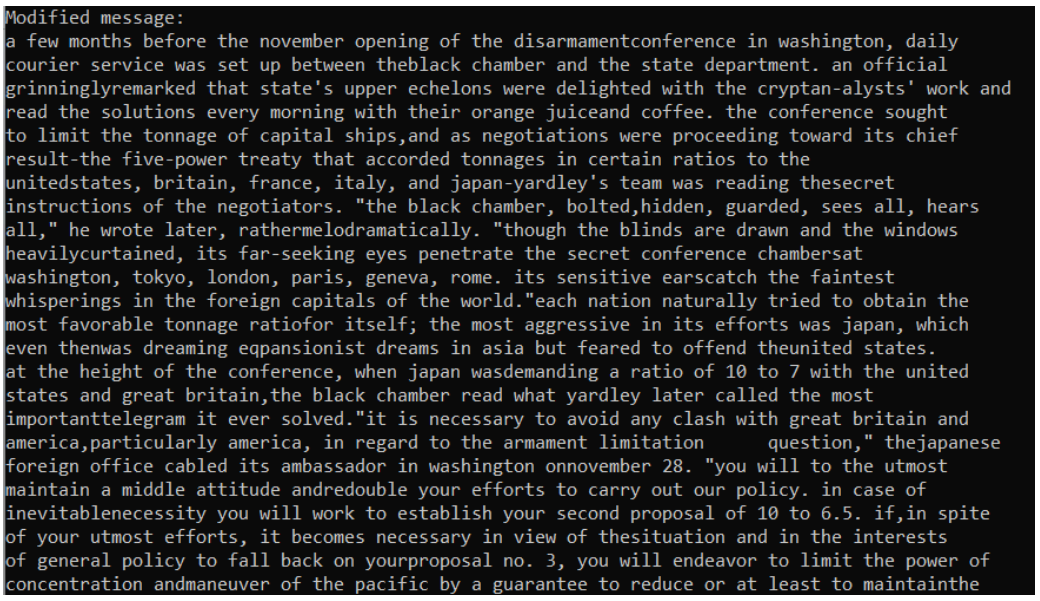

Fig 10. Decryted Alphabet.

And the Full text is :

a few months before the november opening of the disarmament conference in washington, daily
courier service was set up between the black chamber and the state department. an official grinning remarked that state's upper echelons were delighted with the cryptan-alysts' work and
read the solutions every morning with their orange Juice And coffee. the conference sought to limit the tonnage of capital ships,and as negotiations were proceeding toward its chief result-the five-power treaty that accorded tonnages in certain ratios to the
united states, britain, france, italy, and Japan-yardley's team was reading the secret instructions of the negotiators. "the black chamber, bolted,hidden, guarded, sees all, hears all," he wrote later, rather melodramatically. "though the blinds are drawn and the windows heavily curtained, its far-seeking eyes penetrate the secret conference chambersat washington, tokyo, london, paris, geneva, rome. its sensitive ears catch the faintest whisperings in the foreign capitals of the world."each nation naturally tried to obtain the most favorable tonnage ratio for itself; the most aggressive in its efforts was Japan, which even then was dreaming expansionist dreams in asia but feared to offend the united states. at the height of the conference, when Japan was demanding a ratio of 10 to 7 with the united states and great britain,the black chamber read what yardley later called the most important telegram it ever solved."it is necessary to avoid any clash with great britain and america,particularly america, in regard to the armament limitation question," theJapanese foreign office cabled its ambassador in washington on november 28. "you will to the utmost maintain a middle attitude and redouble your efforts to carry out our policy. in case of inevitable necessity you will work to establish your second proposal of 10 to 6.5. if,in spite of your utmost efforts, it becomes necessary in view of the situation and in the interests of general policy to fall back on your proposal no. 3, you will endeavour to limit the power of concentration and maneuver of the pacific by a guarantee to reduce or at least to maintain the

status quo of pacific defenses and to make an adequate reservation which will make clear that
[this is] our intention in agreeing to a 10 to 6 ratio. no4 is to be avoided as far as possible."each 0.5 in the ratio meant 50,000 tons of capital ships, or about a battle ship and a half. with the information in this message telling the american negotiators that Japan would yield if pressed, all they had todo was press. this secretary of state charles evans hughes did, and on december 10 Japan capitulated, instructing its negotiator, in a cable read by the black chamber, that "there is nothing to do but accept the ratio proposed by the united states." as signed, the five-power treaty allotted capital ships to the united states, great britain, Japan, france,and italy in the ratio of 10:10:6:3.3:3.3. it was considerably less thanJapan had hoped for. hughes sent yardley a letter of commendation.during
the conference, the black chamber had turned out more than 5,000 solutions and translations. yardley nearly suffered a nervous breakdown, and in february went to ariZona for four months to
recover his health. several of his assistants had already had trouble in this regard. one babbled
incoherently; a girl dreamed of chasing around the bedroom a bulldog that, when caught, had "code"
written on its side;another could lighten the enormous sack of pebbles that she carried in a recurring nightmare only by finding a stone along a lonely beach that exactly matched one of her
pebbles, which she could then cast into the sea. all three resigned.