(11)

Cryptanalysis Mono-alphabetic Cipher

A mono-alphabetic cipher is a simple substitution cipher wherein each letter of the plaintext is replaced by another letter in the ciphertext. An example of a mono-alphabetic cipher key follows:

Ciphe rtext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Plain text: j r s q x z o e w n d y v p f a t b c i l h g k m u

This key means that any 'j' in the plaintext will be replaced by an 'A' in the ciphertext, any 'r' in the plaintext will be replaced by a 'B' in the ciphertext, and so on.

Cryptanalysis

Breaking the mono-alphabetic cipher was difficult at first, but with a little experience, it became routine. An effective method was developed which was applied successfully to ciphertext as short as three times the key length. The method developed follows:

1. Run the statistical analyzer on the ciphertext.
2. Using the letter frequency statistics and clever observations, make guesses at probable letter substitutions.
3. Backtrack, if necessary.

This simple strategy overwhelms the complexity of the mono-alphabetic cipher.

Example 1:

Here are the number of single letter occurences in the encrypted text:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
18 3 7 35 0 2 14 14 22 26 13 0 25 39 38 12 3 7 1 14 0 21 3 19 15 41

Here is the original encrypted text:

OCDN NZHDIVM XJPMNZ RDGG NOPYT NZXPMDOT AMJH HPGODKGZ KZMNKZXODQZNC RZ RDGG XJINDYZM NJAORVMZ DHKGZHZIOVODJIN JA NZXPMDOT MZGVOZY KJGDXDZN DI OCZ XJIOZSO JA JKZMVODIB NTNOZHNA IZORJMFNA VIY YVOVWVNZNC OJKDXN DIXGPYZO JKZMVODIB NTNOZH KMJOZXODJI HZXCVIDNHNA DIOMPNDJI YZOZXODJI NTNOZHNA AJMHVG HJYZGN JA NZXPMDOTA XMTKOJBMVKCTA YVOV WVNZ NZXPMDOTA RJMHNA QDMPNZNA IZORJMF VIY YDNOMDWPOZY NTNOZH NZXPMDOTA VIY KJGDXDZN JA KMDQVXT VIY XJIADYZIODVGDOTC

First *I guessed the word 'VIY' to be 'and'. The frequency of 'Y' is small enough to be substituted for 'd'.*

OCDN NZHDnaM XJPMNZ RDGG NOPdT NZXPMDOT AMJH HPGODKGZ KZMNKZXODQZNC RZ RDGG XJnNDdZM NJAORaMZ DHKGZHZnOaODJnN JA NZXPMDOT MZGaOZd KJGDXDZN Dn OCZ XJnOZSO JA JKZMaODnB NTNOZHNA nZORJMFNA **and** daOaWaNZNC OJKDXN DnXGPdZO JKZMaODnB NTNOZH KMJOZXODJn HZXCanDNHNA DnOMPNDJn dZOZXODJn NTNOZHNA AJMHaG HJdZGN JA NZXPMDOTA XMTKOJBMaKCTA daOa WaNZ NZXPMDOTA RJMHNA QDMPNZNA nZORJMF and dDNOMDWPOZd NTNOZH NZXPMDOTA and KJGDXDZN JA KMDQaXT and XJnADdZnODaGDOTC

Next*, the 'daOa' is assumed to be 'data'.*

tCDN NZHDnaM XJPMNZ RDGG NtPdT NZXPMDtT AMJH HPGtDKGZ KZMNKZXtDQZNC RZ RDGG XJnNDdZM NJAtRaMZ DHKGZHZntatDJnN JA NZXPMDtT MZGatZd KJGDXDZN Dn tCZ XJntZSt JA JKZMatDnB NTNtZHNA nZtRJMFNA and dataWaNZNC tJKDXN DnXGPdZt JKZMatDnB NTNtZH KMJtZXtDJn HZXCanDNHNA DntMPNDJn dZtZXtDJn NTNtZHNA AJMHaG HJdZGN JA NZXPMDtTA XMTKtJBMaKCTA **data** WaNZ NZXPMDtTA RJMHNA QDMPNZNA

nZtRJMF and dDNtMDWPtZd NTNtZH NZXPMDtTA and KJGDXDZN JA KMDQaXT and XJnADdZntDaGDtTC

'Z' is guessed to be 'e', based on its frequency.

tCDN N**e**HDnaM XJPMNe RDGG NtPdT NeXPMDtT AMJH HPGtDKGe KeMNKeXtDQeNC Re RDGG XJnNDdeM NJAtRaMe DHKGeHentatDJnN JA NeXPMDtT MeGated KJGDXDeN Dn tCe XJnteSt JA JKeMatDnB NTNteHNA netRJMFNA and dataWaNeNC tJKDXN DnXGPdet JKeMatDnB NTNteH KMJteXtDJn HeXCanDNHNA DntMPNDJn deteXtDJn NTNteHNA AJMHaG HJdeGN JA NeXPMDtTA XMTKtJBMaKCTA data WaNe NeXPMDtTA RJMHNA QDMPNeNA netRJMF and dDNtMDWPted NTNteH NeXPMDtTA and KJGDXDeN JA KMDQaXT and XJnADdentDaGDtTC

'C' is guessed to be 'h', based on the 'tCe'.

thDN NeHDnaM XJPMNe RDGG NtPdT NeXPMDtT AMJH HPGtDKGe KeMNKeXtDQeNh Re RDGG XJnNDdeM NJAtRaMe DHKGeHentatDJnN JA NeXPMDtT MeGated KJGDXDeN Dn **the** XJnteSt JA JKeMatDnB NTNteHNA netRJMFNA and dataWaNeNh tJKDXN DnXGPdet JKeMatDnB NTNteH KMJteXtDJn HeXhanDNHNA DntMPNDJn deteXtDJn NTNteHNA AJMHaG HJdeGN JA NeXPMDtTA XMTKtJBMaKhTA data WaNe NeXPMDtTA RJMHNA QDMPNeNA netRJMF and dDNtMDWPted NTNteH NeXPMDtTA and KJGDXDeN JA KMDQaXT and XJnADdentDaGDtTh

'netRJMF' is guessed to be 'network'.

thDN NeHDnar XoPrNe wDGG NtPdT NeXPrDtT AroH HPGtDKGe KerNKeXtDQeNh we wDGG XonNDder NoAtware DHKGeHentatDonN oA NeXPrDtT reGated KoGDXDeN Dn the XonteSt oA oKeratDnB NTNteHNA networkNA and dataWaNeNh toKDXN DnXGPdet oKeratDnB NTNteH KroteXtDon HeXhanDNHNA DntrPNDon deteXtDon NTNteHNA AorHaG HodeGN oA NeXPrDtTA XrTKtoBraKhTA data WaNe NeXPrDtTA worHNA QDrPNeNA **network** and dDNtrDWPted NTNteH NeXPrDtTA and KoGDXDeN oA KrDQaXT and XonADdentDaGDtTh

'reGated' is guessed to be 'related'.

thDN NeHDnar XoPrNe wDll NtPdT NeXPrDtT AroH HPltDKle KerNKeXtDQeNh we wDll XonNDder NoAtware DHKleHentatDonN oA NeXPrDtT **related** KolDXDeN Dn the XonteSt oA oKeratDnB NTNteHNA networkNA and dataWaNeNh toKDXN DnXlPdet oKeratDnB NTNteH KroteXtDon HeXhanDNHNA DntrPNDon deteXtDon NTNteHNA AorHal HodelN oA NeXPrDtTA XrTKtoBraKhTA data WaNe NeXPrDtTA worHNA QDrPNeNA network and dDNtrDWPted NTNteH NeXPrDtTA and KolDXDeN oA KrDQaXT and XonADdentDalDtTh

'D' is guessed to be 'i', based on 'wDll' and 'Dn'.

thiN NeHinar XoPrNe **will** NtPdT NeXPritT AroH HPltiKle KerNKeXtiQeNh we will XonNider NoAtware iHKleHentationN oA NeXPritT related KoliXieN **in** the XonteSt oA oKeratinB NTNteHNA networkNA and dataWaNeNh toKiXN inXlPdet oKeratinB NTNteH KroteXtion HeXhaniNHNA intrPNion deteXtion NTNteHNA AorHal HodelN oA NeXPritTA XrTKtoBraKhTA data WaNe NeXPritTA worHNA QirPNeNA network and diNtriWPted NTNteH NeXPritTA and KoliXieN oA KriQaXT and XonAidentialitTh

'NeHinar' is guessed to be 'seminar'.

this **seminar** XoPrse will stPdT seXPritT Arom mPltiKle KersKeXtiQesh we will Xonsider soAtware imKlementations oA seXPritT related KoliXies in the XonteSt oA oKeratinB sTstemsA networksA and dataWasesh toKiXs inXlPdet oKeratinB sTstem KroteXtion meXhanismsA intrPsion deteXtion sTstemsA Aormal models oA seXPritTA XrTKtoBraKhTA data Wase seXPritTA wormsA QirPsesA network and distriWPted sTstem seXPritTA and KoliXies oA KriQaXT and XonAidentialitTh

'XoPrse' is guessed to be 'course'. 'stPdT' is guessed to be 'study'. 'seXPritT' is guessed to be 'security'.

this seminar **course** will **study security** from multiKle KersKectiQesh we will consider software imKlementations of security related Kolicies in the conteSt of oKeratinB systemsf networksf and dataWasesh toKics includet oKeratinB system Krotection mechanismsf intrusion detection systemsf formal models of securityf cryKtoBraKhyf data Wase securityf wormsf Qirusesf network and distriWuted system securityf and Kolicies of KriQacy and confidentialityh

The final letters are filled in by scanning the text.

this seminar course will study security from multiple perspectivesh we will consider software implementations of security related policies in the context of operating systemsf networksf and databasesh topics includet operating system protection mechanismsf intrusion detection systemsf formal models of securityf cryptographyf data base securityf wormsf virusesf network and distributed system securityf and policies of privacy and confidentialityh

Some of the punctuation in the original message seems to have translated to alphabetic characters. The original mono-alphabetic cipher

implementation (which eventually turns out to be a shift cipher) comes under scrutiny.

When I wrote out the key I realized:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
f g h i j k l m n o p q r s t u v w x y z a b c d e

It's a shift cipher!

********** **********

Example 2

Here are the number of single letter occurences in the encrypted text:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
133	32	10	25	6	19	0	85	22	41	40	200	31	25	66	66	0	9	65	26	68	88	34	4	96	79

Here is the original encrypted text:

AOL MPYZA ZALW PU IYLHRPUN HUF JPWOLY PZ AV AYF AV MPUK MLHABYLZ DOPJO JVYYLZWVUK AV AOL VYPNPUHS WSHPU ALEA DOLYLHZ JVKLZ ZBIZAPABAL NYVBWZ VM SLAALYZ VY MPNBYLZ MVY DVYKZ WOYHZLZ VY LCLU JVTWSLAL JVUJLWAZ JPWOLYZ YLWSHJL LCLYF PUKPCPKBHS SLAALY VM LCLYF DVYK AOLF AOLYLMVYL ALUK AV YLMSLJA AOL JOHYHJALYPZAPJZ VM AOL SHUNBHNL VM AOL VYPNPUHS ALEA AOPZ THRLZ AOLT CBSULYHISL AV ZABKPLZ VM SLAALY MYLXBLUJF MVY LEHTWSL AOL TVZA JVTTVU SLAALYZ PU LUNSPZO HYL L A H V HUK U PM H YLHZVUHISL HTVBUA VY KLWAO VM LUNSPZO ALEA LUJPWOLYLK PU AOL ZHTL ZPTWSL JPWOLY DLYL ZABKPLK MVY SLAALY MYLXBLUJF AOL SLAALY AOHA JHTL BW TVZA VMALU DVBSK YLWYLZLUA L AOL ZLJVUK TVZA JVTTVU SLAALY DVBSK IL A HUK ZV VU IF DVYRPUN AOPZ VBA HUK MPSSPUN PU AOL SLAALYZ ZVTL DPSS MVYT VICPVBZ DVYKZ DPAO SLAALYZ TPZZPUN HSSVDPUN AOL JVKLIYLHRLY AV MPSS PU AOL NHWZ HUK YLJVCLY AOVZL SLAALYZ HZ DLSS JVUAHJA HUHSFZPZ HUVAOLY IHZPJ DLHWVU BZLK IF AOL JVKLIYLHRLY AHRLZ AOPZ WYPUJPWSL H ZALW MBYAOLY ZVTL SLAALYZ DPSS HWWLHY MYLXBLUASF HSVUNZPKL LHJO VAOLY AOL TVZA VICPVBZ LEHTWSL PU AOL LUNSPZO SHUNBHNL PZ AO HZ PU AOL VY AOHA IF JVTIPUPUN AOLZL ADV DLHWVUZ AOL JVKLIYLHRLY JVBSK THRL H

YLHZVUHISL NBLZZ AOHA DOLYL H ZPUNSL SLAALY HWWLHYLK YLWLHALKSF HMALY AOL A DOPJO OL OHK HSYLHKF YLJVCLYLK MYVT SLAALY MYLXBLUJF AOL BURUVDU SLAALY DHZ WYVIHISF O WHYAPJBSHYSF PM AOL ULEA SLAALY OHK HSYLHKF ILLU YLJVCLYLK HZ L PU AOHA JHZL OL TPNOA JVUJSBKL AOHA AOL SLAALY HMALY AOL L DHZ WYVIHISF AOL ZAHYA VM H ULD DVYK HUK ZV AOL WYVJLZZ VM IBPSKPUN BW AOL TLZZHNL DVBSK NV VU

First, *I guessed the word 'AOL' to be 'the'. 'L' is by far the most frequently occuring letter and 'the' often begins sentences.*

the MPYZt ZteW PU IYeHRPUN HUF JPWheY PZ tV tYF tV MPUK MeHtBYeZ DhPJh JVYYeZWVUK tV the VYPNPUHS WSHPU teEt DheYeHZ JVKeZ ZBIZtPtBte NYVBWZ VM SetteYZ VY MPNBYeZ MVY DVYKZ WhYHZeZ VY eCeU JVTWSete JVUJeWtZ JPWheYZ YeWSHJe eCeYF PUKPCPKBHS SetteY VM eCeYF DVYK theF theYeMVYe teUK tV YeMSeJt the JhHYHJteYPZtPJZ VM the SHUNBHNe VM the VYPNPUHS teEt thPZ THReZ theT CBSUeYHISe tV ZtBKPeZ VM SetteY MYeXBeUJF MVY eEHTWSe the TVZt JVTTVU SetteYZ PU eUNSPZh HYe e t H V HUK U PM H YeHZVUHISe HTVBUt VY KeWth VM eUNSPZh teEt eUJPWheYeK PU the ZHTe ZPTWSe JPWheY DeYe ZtBKPeK MVY SetteY MYeXBeUJF the SetteY thHt JHTe BW TVZt VMteU DVBSK YeWYeZeUt e the ZeJVUK TVZt JVTTVU SetteY DVBSK Ie t HUK ZV VU IF DVYRPUN thPZ VBt HUK MPSSPUN PU the SetteYZ ZVTe DPSS MVYT VICPVBZ DVYKZ DPth SetteYZ TPZZPUN HSSVDPUN the JVKeIYeHReY tV MPSS PU the NHWZ HUK YeJVCeY thVZe SetteYZ HZ DeSS JVUtHJt HUHSFZPZ HUVtheY IHZPJ DeHWVU BZeK IF the JVKeIYeHReY tHReZ thPZ WYPUJPWSe H ZteW MBYtheY ZVTe SetteYZ DPSS HWWeHY MYeXBeUtSF HSVUNZPKe eHJh VtheY the TVZt VICPVBZ eEHTWSe PU the eUNSPZh SHUNBHNe PZ th HZ PU the VY thHt IF JVTIPUPUN theZe tDV DeHWVUZ the JVKeIYeHReY JVBSK THRe H YeHZVUHISe NBeZZ thHt DheYe H ZPUNSe SetteY HWWeHYeK YeWeHteKSF HMteY the t DhPJh he hHK HSYeHKF YeJVCeYeK MYVT SetteY MYeXBeUJF the BURUVDU SetteY DHZ WYVIHISF h WHYtPJBSHYSF PM the UeEt SetteY hHK HSYeHKF IeeU YeJVCeYeK HZ e PU thHt JHZe he TPNht JVUJSBKe thHt the SetteY HMteY the e DHZ WYVIHISF the ZtHYt VM H UeD DVYK HUK ZV the WYVJeZZ VM IBPSKPUN BW the TeZZHNe DVBSK NV VU

'SetteYZ' is guessed to be 'letters'.

the MPrst steW PU IreHRPUN HUF JPWher Ps tV trF tV MPUK MeHtBres DhPJh JVrresWVUK tV the VrPNPUHl WlHPU teEt DhereHs JVKes sBIstPtBte NrVBWs VM **letters** Vr MPNBres MVr DVrKs WhrHses Vr eCeU JVTWlete JVUJeWts JPWhers reWlHJe eCerF PUKPCPKBHl letter VM eCerF DVrK theF thereMVre teUK tV reMleJt the JhHrHJterPstPJs VM the lHUNBHNe VM the VrPNPUHl teEt thPs THRes theT CBlUerHIle tV stBKPes VM letter MreXBeUJF MVr eEHTWle the TVst JVTTVU letters PU eUNlPsh Hre e t H V HUK U PM H reHsVUHIle HTVBUt Vr KeWth VM eUNlPsh teEt eUJPWhereK PU the sHTe sPTWle JPWher Dere stBKPeK MVr letter MreXBeUJF the letter thHt JHTe BW TVst VMteU DVBlK reWreseUt e the seJVUK TVst JVTTVU letter DVBlK Ie t HUK sV VU IF

DVrRPUN thPs VBt HUK MPllPUN PU the letters sVTe DPll MVrT VICPVBs DVrKs DPth letters TPssPUN HllVDPUN the JVKeIreHRer tV MPll PU the NHWs HUK reJVCer thVse letters Hs Dell JVUtHJt HUHlFsPs HUVther IHsPJ DeHWVU BseK IF the JVKeIreHRer tHRes thPs WrPUJPWle H steW MBrther sVTe letters DPll HWWeHr MreXBeUtlF HlVUNsPKe eHJh Vther the TVst VICPVBs eEHTWle PU the eUNlPsh lHUNBHNe Ps th Hs PU the Vr thHt IF JVTIPUPUN these tDV DeHWVUs the JVKeIreHRer JVBlK THRe H reHsVUHIle NBess thHt Dhere H sPUNle letter HWWeHreK reWeHteKlF HMter the t DhPJh he hHK HlreHKF reJVCereK MrVT letter MreXBeUJF the BURUVDU letter DHs WrVIHIlF h WHrtPJBlHrlF PM the UeEt letter hHK HlreHKF IeeU reJVCereK Hs e PU thHt JHse he TPNht JVUJlBKe thHt the letter HMter the e DHs WrVIHIlF the stHrt VM H UeD DVrK HUK sV the WrVJess VM IBPlKPUN BW the TessHNe DVBlK NV VU

'Hre' is guessed to be 'are'.

the MPrst steW PU IreaRPUN aUF JPWher Ps tV trF tV MPUK MeatBres DhPJh JVrresWVUK tV the VrPNPUal WlaPU teEt Dhereas JVKes sBIstPtBte NrVBWs VM letters Vr MPNBres MVr DVrKs Whrases Vr eCeU JVTWlete JVUJeWts JPWhers reWlaJe eCerF PUKPCPKBal letter VM eCerF DVrK theF thereMVre teUK tV reMleJt the JharaJterPstPJs VM the laUNBaNe VM the VrPNPUal teEt thPs TaRes theT CBlUeraIle tV stBKPes VM letter MreXBeUJF MVr eEaTWle the TVst JVTTVU letters PU eUNlPsh **are** e t a V aUK U PM a reasVUaIle aTVBUt Vr KeWth VM eUNlPsh teEt eUJPWhereK PU the saTe sPTWle JPWher Dere stBKPeK MVr letter MreXBeUJF the letter that JaTe BW TVst VMteU DVBlK reWreseUt e the seJVUK TVst JVTTVU letter DVBlK Ie t aUK sV VU IF DVrRPUN thPs VBt aUK MPllPUN PU the letters sVTe DPll MVrT VICPVBs DVrKs DPth letters TPssPUN allVDPUN the JVKeIreaRer tV MPll PU the NaWs aUK reJVCer thVse letters as Dell JVUtaJt aUalFsPs aUVther IasPJ DeaWVU BseK IF the JVKeIreaRer taRes thPs WrPUJPWle a steW MBrther sVTe letters DPll aWWear MreXBeUtlF alVUNsPKe eaJh Vther the TVst VICPVBs eEaTWle PU the eUNlPsh laUNBaNe Ps th as PU the Vr that IF JVTIPUPUN these tDV DeaWVUs the JVKeIreaRer JVBlK TaRe a reasVUaIle NBess that Dhere a sPUNle letter aWWeareK reWeateKlF aMter the t DhPJh he haK alreaKF reJVCereK MrVT letter MreXBeUJF the BURUVDU letter Das WrVIaIlF h WartPJBlarlF PM the UeEt letter haK alreaKF IeeU reJVCereK as e PU that Jase he TPNht JVUJlBKe that the letter aMter the e Das WrVIaIlF the start VM a UeD DVrK aUK sV the WrVJess VM IBPlKPUN BW the TessaNe DVBlK NV VU

'E' is guessed to be 'X' and 'U' is guessed to be 'n' based on 'UeEt' and 'teEt'.

the MPrst steW Pn IreaRPnN anF JPWher Ps tV trF tV MPnK MeatBres DhPJh JVrresWVnK tV the VrPNPnal WlaPn text Dhereas JVKes sBIstPtBte NrVBWs VM letters Vr MPNBres MVr DVrKs Whrases Vr eCen JVTWlete JVnJeWts JPWhers reWlaJe eCerF PnKPCPKBal letter VM eCerF DVrK theF thereMVre tenK tV reMleJt the JharaJterPstPJs VM the lanNBaNe VM the VrPNPnal **text** thPs TaRes theT CBlneraIle tV stBKPes VM letter MreXBenJF MVr exaTWle the TVst JVTTVn letters Pn enNlPsh are e t a V anK n PM a reasVnaIle aTVBnt Vr KeWth VM

enNlPsh text enJPWhereK Pn the saTe sPTWle JPWher Dere stBKPeK MVr letter MreXBenJF the letter that JaTe BW TVst VMten DVBlK reWresent e the seJVnK TVst JVTTVn letter DVBlK Ie t anK sV Vn IF DVrRPnN thPs VBt anK MPllPnN Pn the letters sVTe DPll MVrT VICPVBs DVrKs DPth letters TPssPnN allVDPnN the JVKeIreaRer tV MPll Pn the NaWs anK reJVCer thVse letters as Dell JVntaJt analFsPs anVther IasPJ DeaWVn BseK IF the JVKeIreaRer taRes thPs WrPnJPWle a steW MBrther sVTe letters DPll aWWear MreXBentlF alVnNsPKe eaJh Vther the TVst VICPVBs exaTWle Pn the enNlPsh lanNBaNe Ps th as Pn the Vr that IF JVTIPnPnN these tDV DeaWVns the JVKeIreaRer JVBlK TaRe a reasVnaIle NBess that Dhere a sPnNle letter aWWeareK reWeateKlF aMter the t DhPJh he haK alreaKF reJVCereK MrVT letter MreXBenJF the BnRnVDn letter Das WrVIaIlF h WartPJBlarlF PM the **next** letter haK alreaKF Ieen reJVCereK as e Pn that Jase he TPNht JVnJlBKe that the letter aMter the e Das WrVIaIlF the start VM a neD DVrK anK sV the WrVJess VM IBPlKPnN BW the TessaNe DVBlK NV Vn

'D' is guessed to be 'w' based on 'Dhereas' and 'neD'.

the MPrst steW Pn IreaRPnN anF JPWher Ps tV trF tV MPnK MeatBres whPJh JVrresWVnK tV the VrPNPnal WlaPn text **whereas** JVKes sBIstPtBte NrVBWs VM letters Vr MPNBres MVr wVrKs Whrases Vr eCen JVTWlete JVnJeWts JPWhers reWlaJe eCerF PnKPCPKBal letter VM eCerF wVrK theF thereMVre tenK tV reMleJt the JharaJterPstPJs VM the lanNBaNe VM the VrPNPnal text thPs TaRes theT CBlneraIle tV stBKPes VM letter MreXBenJF MVr exaTWle the TVst JVTTVn letters Pn enNlPsh are e t a V anK n PM a reasVnaIle aTVBnt Vr KeWth VM enNlPsh text enJPWhereK Pn the saTe sPTWle JPWher were stBKPeK MVr letter MreXBenJF the letter that JaTe BW TVst VMten wVBlK reWresent e the seJVnK TVst JVTTVn letter wVBlK Ie t anK sV Vn IF wVrRPnN thPs VBt anK MPllPnN Pn the letters sVTe wPll MVrT VICPVBs wVrKs wPth letters TPssPnN allVwPnN the JVKeIreaRer tV MPll Pn the NaWs anK reJVCer thVse letters as well JVntaJt analFsPs anVther IasPJ weaWVn BseK IF the JVKeIreaRer taRes thPs WrPnJPWle a steW MBrther sVTe letters wPll aWWear MreXBentlF alVnNsPKe eaJh Vther the TVst VICPVBs exaTWle Pn the enNlPsh lanNBaNe Ps th as Pn the Vr that IF JVTIPnPnN these twV weaWVns the JVKeIreaRer JVBlK TaRe a reasVnaIle NBess that where a sPnNle letter aWWeareK reWeateKlF aMter the t whPJh he haK alreaKF reJVCereK MrVT letter MreXBenJF the BnRnVwn letter was WrVIaIlF h WartPJBlarlF PM the next letter haK alreaKF Ieen reJVCereK as e Pn that Jase he TPNht JVnJlBKe that the letter aMter the e was WrVIaIlF the start VM a **new** wVrK anK sV the WrVJess VM IBPlKPnN BW the TessaNe wVBlK NV Vn

'steW' is gueesd to be 'step'.

the MPrst **step** Pn IreaRPnN anF JPpher Ps tV trF tV MPnK MeatBres whPJh JVrrespVnK tV the VrPNPnal plaPn text whereas JVKes sBIstPtBte NrVBps VM letters Vr MPNBres MVr wVrKs phrases Vr eCen JVmplete JVnJepts JPphers replaJe eCerF PnKPCPKBal letter VM eCerF wVrK theF thereMVre tenK tV reMleJt the JharaJterPstPJs VM the lanNBaNe VM the VrPNPnal text thPs maRes them CBlneraIle tV stBKPes VM letter MreXBenJF MVr example the mVst JVmmVn letters Pn enNlPsh are e t a V anK n PM a reasVnaIle amVBnt Vr Kepth VM enNlPsh text enJPphereK Pn the same sPmple JPpher were stBKPeK MVr letter MreXBenJF

the letter that Jame Bp mVst VMten wVBlK represent e the seJVnK mVst JVmmVn letter wVBlK Ie t anK sV Vn IF wVrRPnN thPs VBt anK MPllPnN Pn the letters sVme wPll MVrm VICPVBs wVrKs wPth letters mPssPnN allVwPnN the JVKeIreaRer tV MPll Pn the Naps anK reJVCer thVse letters as well JVntaJt analFsPs anVther IasPJ weapVn BseK IF the JVKeIreaRer taRes thPs prPnJPple a step MBrther sVme letters wPll appear MreXBentlF alVnNsPKe eaJh Vther the mVst VICPVBs example Pn the enNlPsh lanNBaNe Ps th as Pn the Vr that IF JVmIPnPnN these twV weapVns the JVKeIreaRer JVBlK maRe a reasVnaIle NBess that where a sPnNle letter appeareK repeateKlF aMter the t whPJh he haK alreaKF reJVCereK MrVm letter MreXBenJF the BnRnVwn letter was prVIaIlF h partPJBlarlF PM the next letter haK alreaKF Ieen reJVCereK as e Pn that Jase he mPNht JVnJlBKe that the letter aMter the e was prVIaIlF the start VM a new wVrK anK sV the prVJess VM IBPlKPnN Bp the messaNe wVBlK NV Vn

'MPrst' is guessed to be 'first'.

the **first** step in IreaRinN anF Jipher is tV trF tV finK featBres whiJh JVrrespVnK tV the VriNinal plain text whereas JVKes sBIstitBte NrVBps Vf letters Vr fiNBres fVr wVrKs phrases Vr eCen JVmplete JVnJepts Jiphers replaJe eCerF inKiCiKBal letter Vf eCerF wVrK theF therefVre tenK tV refleJt the JharaJteristiJs Vf the lanNBaNe Vf the VriNinal text this maRes them CBlneraIle tV stBKies Vf letter freXBenJF fVr example the mVst JVmmVn letters in enNlish are e t a V anK n if a reasVnaIle amVBnt Vr Kepth Vf enNlish text enJiphereK in the same simple Jipher were stBKieK fVr letter freXBenJF the letter that Jame Bp mVst Vften wVBlK represent e the seJVnK mVst JVmmVn letter wVBlK Ie t anK sV Vn IF wVrRinN this VBt anK fillinN in the letters sVme will fVrm VICiVBs wVrKs with letters missinN allVwinN the JVKeIreaRer tV fill in the Naps anK reJVCer thVse letters as well JVntaJt analFsis anVther IasiJ weapVn BseK IF the JVKeIreaRer taRes this prinJiple a step fBrther sVme letters will appear freXBentlF alVnNsiKe eaJh Vther the mVst VICiVBs example in the enNlish lanNBaNe is th as in the Vr that IF JVmIininN these twV weapVns the JVKeIreaRer JVBlK maRe a reasVnaIle NBess that where a sinNle letter appeareK repeateKlF after the t whiJh he haK alreaKF reJVCereK frVm letter freXBenJF the BnRnVwn letter was prVIaIlF h partiJBlarlF if the next letter haK alreaKF Ieen reJVCereK as e in that Jase he miNht JVnJlBKe that the letter after the e was prVIaIlF the start Vf a new wVrK anK sV the prVJess Vf IBilKinN Bp the messaNe wVBlK NV Vn

'J' is guessed to be 'c' based on 'Jipher' and 'whiJh'.

the first step in IreaRinN anF **cipher** is tV trF tV finK featBres **which** cVrrespVnK tV the VriNinal plain text whereas cVKes sBIstitBte NrVBps Vf letters Vr fiNBres fVr wVrKs phrases Vr eCen cVmplete cVncepts ciphers replace eCerF inKiCiKBal letter Vf eCerF wVrK theF therefVre tenK tV reflect the characteristics Vf the lanNBaNe Vf the VriNinal text this maRes them CBlneraIle tV stBKies Vf letter freXBencF fVr example the mVst cVmmVn letters in enNlish are e t a V anK n if a reasVnaIle amVBnt Vr Kepth Vf enNlish text enciphereK in the same simple cipher were stBKieK fVr letter freXBencF the letter that came Bp mVst Vften wVBlK represent e the secVnK mVst cVmmVn letter wVBlK Ie t anK sV Vn IF wVrRinN this VBt anK fillinN in the letters sVme will fVrm VICiVBs wVrKs with letters missinN allVwinN

the cVKeIreaRer tV fill in the Naps anK recVCer thVse letters as well cVntact analFsis anVther Iasic weapVn BseK IF the cVKeIreaRer taRes this principle a step fBrther sVme letters will appear freXBentlF alVnNsiKe each Vther the mVst VICiVBs example in the enNlish lanNBaNe is th as in the Vr that IF cVmIininN these twV weapVns the cVKeIreaRer cVBlK maRe a reasVnaIle NBess that where a sinNle letter appeareK repeateKlF after the t which he haK alreaKF recVCereK frVm letter freXBencF the BnRnVwn letter was prVIaIlF h particBlarlF if the next letter haK alreaKF Ieen recVCereK as e in that case he miNht cVnclBKe that the letter after the e was prVIaIlF the start Vf a new wVrK anK sV the prVcess Vf lBilKinN Bp the messaNe wVBlK NV Vn

'IreaRinN' is guessed to be 'breaking'.

the first step in **breaking** anF cipher is tV trF tV finK featBres which cVrrespVnK tV the Vriginal plain text whereas cVKes sBbstitBte grVBps Vf letters Vr figBres fVr wVrKs phrases Vr eCen cVmplete cVncepts ciphers replace eCerF inKiCiKBal letter Vf eCerF wVrK theF therefVre tenK tV reflect the characteristics Vf the langBage Vf the Vriginal text this makes them CBlnerable tV stBKies Vf letter freXBencF fVr example the mVst cVmmVn letters in english are e t a V anK n if a reasVnable amVBnt Vr Kepth Vf english text enciphereK in the same simple cipher were stBKieK fVr letter freXBencF the letter that came Bp mVst Vften wVBlK represent e the secVnK mVst cVmmVn letter wVBlK be t anK sV Vn bF wVrking this VBt anK filling in the letters sVme will fVrm VbCiVBs wVrKs with letters missing allVwing the cVKebreaker tV fill in the gaps anK recVCer thVse letters as well cVntact analFsis anVther basic weapVn BseK bF the cVKebreaker takes this principle a step fBrther sVme letters will appear freXBentlF alVngsiKe each Vther the mVst VbCiVBs example in the english langBage is th as in the Vr that bF cVmbining these twV weapVns the cVKebreaker cVBlK make a reasVnable gBess that where a single letter appeareK repeateKlF after the t which he haK alreaKF recVCereK frVm letter freXBencF the BnknVwn letter was prVbablF h particBlarlF if the next letter haK alreaKF been recVCereK as e in that case he might cVnclBKe that the letter after the e was prVbablF the start Vf a new wVrK anK sV the prVcess Vf bBilKing Bp the message wVBlK gV Vn

A number of the other words are filled in such as 'any', 'to', 'try', 'find', 'features', etc.

the first step in breaking **any** cipher is **to try** to **find features** which correspond to the original plain text whereas codes substitute groups of letters or figures for words phrases or eCen complete concepts ciphers replace eCery indiCidual letter of eCery word they therefore tend to reflect the characteristics of the language of the original text this makes them Culnerable to studies of letter freXuency for example the most common letters in english are e t a o and n if a reasonable amount or depth of english text enciphered in the same simple cipher were studied for letter freXuency the letter that came up most often would represent e the second most common letter would be t and so on by working this out and filling in the letters some will form obCious words with letters missing allowing the codebreaker to fill in the gaps and recoCer those letters as well contact analysis another basic weapon used by the codebreaker takes this principle a step further some letters will appear freXuently alongside each other

the most obCious example in the english language is th as in the or that by combining these two weapons the codebreaker could make a reasonable guess that where a single letter appeared repeatedly after the t which he had already recoCered from letter freXuency the unknown letter was probably h particularly if the next letter had already been recoCered as e in that case he might conclude that the letter after the e was probably the start of a new word and so the process of building up the message would go on

The remainder of the text is filled in.

the first step in breaking any cipher is to try to find features which correspond to the original plain text whereas codes substitute groups of letters or figures for words phrases or even complete concepts ciphers replace every individual letter of every word they therefore tend to reflect the characteristics of the language of the original text this makes them vulnerable to studies of letter frequency for example the most common letters in english are e t a o and n if a reasonable amount or depth of english text enciphered in the same simple cipher were studied for letter frequency the letter that came up most often would represent e the second most common letter would be t and so on by working this out and filling in the letters some will form obvious words with letters missing allowing the codebreaker to fill in the gaps and recover those letters as well contact analysis another basic weapon used by the codebreaker takes this principle a step further some letters will appear frequently alongside each other the most obvious example in the english language is th as in the or that by combining these two weapons the codebreaker could make a reasonable guess that where a single letter appeared repeatedly after the t which he had already recovered from letter frequency the unknown letter was probably h particularly if the next letter had already been recovered as e in that case he might conclude that the letter after the e was probably the start of a new word and so the process of building up the message would go on

Here is the key that was used:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
t u v w x y z a b c d e f g h i j k l m n o p q r s

It turns out to be a shift cipher too!