Department of Computer System Engineering

Subject: Computer Security Assignment No. 01

Submitted by: Amir Suliman

Registration No: 19PWCSE1805

Class Section: B

Submitted to:

Dr: Sadeeq Jan

November 10, 2022

Q1. Decrypt the following message using a monoalphabetic cipher and find the key as well.

"KFD KTBD FZM EUBD KFD PZYIOM MZTX KU KZYG UR BZHA KFTHCM UR MFUDM ZHX MFTNM ZHX MDZYTHC PZQ UR EZSSZCDM ZHX GTHCM ZHX PFA KFD MDZ TM SUTYTHC FUK ZHX PFDKFDI NTCM FZLD PTHCM SOK PZTK Z STK KFD UAMKDIM EITDX SDRUID PD FZLD UOI EFZK RUI MUBD UR OM ZID UOK UR SIDZKF ZHX ZYY UR OM ZID RZK HU FOIIA MZTX KFD EZINDHKDI KFDA KFZHGDX FTB BOEF RUI KFZK"

Frequency of each word:

Word	K	F	D	T	B	Z	M	E	U
Frequency	24	23	28	16	6	30	21	6	19
Word	P	Y	I	O	X	G	R	H	A
Frequency	7	6	15	8	10	3	10	15	5
Word	C	N	Q	S	L				
Frequency	7	3	1	7	2				

Let's change Z with a:

"KFD KTBD FaM EUBD KFD PaYIOM MaTX KU KaYG UR BaHA KFTHCM UR MFUDM aHX MFTNM aHX MDaYTHC PaQ UR EaSSaCDM aHX GTHCM aHX PFA KFD MDa TM SUTYTHC FUK aHX PFDKFDI NTCM FaLD PTHCM SOK PaTK a STK KFD UAMKDIM EITDX SDRUID PD FaLD UOI EFaK RUI MUBD UR OM aID UOK UR SIDaKF aHX aYY UR OM aID RaK HU FOIIA MaTX KFD EaINDHKDI KFDA KFaHGDX FTB BOEF RUI KFaK"

Now Let's change K with t:

"tFD tTBD FaM EUBD tFD PaYIOM MaTX tU taYG UR BaHA tFTHCM UR MFUDM aHX MFTNM aHX MDaYTHC PaQ UR EaSSaCDM aHX GTHCM aHX PFA tFD MDa TM SUTYTHC FUt aHX PFDtFDI NTCM FaLD PTHCM SOt PaTt a STt tFD UAMtDIM EITDX SDRUID PD FaLD UOI EFat RUI MUBD UR OM aID UOt UR SIDatF aHX aYY UR OM aID Rat HU FOIIA MaTX tFD EaINDHtDI tFDA tFaHGDX FTB BOEF RUI tFat"

Now Let's change R with c:

"tFD tTBD FaM EUBD tFD PaYIOM MaTX tU taYG Uc BaHA tFTHCM Uc MFUDM aHX MFTNM aHX MDaYTHC PaQ Uc EaSSaCDM aHX GTHCM aHX PFA tFD MDa TM SUTYTHC FUt aHX PFDtFDI NTCM FaLD PTHCM SOt PaTt a STt tFD UAMtDIM EITDX SDcUID PD FaLD UOI EFat cUI MUBD Uc OM aID UOt Uc SIDatF aHX aYY Uc OM aID cat HU FOIIA MaTX tFD EaINDHtDI tFDA tFaHGDX FTB BOEF cUI tFat"

The above guess is wrong

Now Let's change F with h:

"thD tTBD haM EUBD thD PaYIOM MaTX tU taYG UR BaHA thTHCM UR MhUDM aHX MhTNM aHX MDaYTHC PaQ UR EaSSaCDM aHX GTHCM aHX PhA thD MDa TM SUTYTHC hUt aHX PhDthDI NTCM haLD PTHCM SOt PaTt a STt thD UAMtDIM EITDX SDRUID PD haLD UOI Ehat RUI MUBD UR OM aID UOt UR SIDath aHX aYY UR OM aID Rat HU hOIIA MaTX thD EaINDHtDI thDA thaHGDX hTB BOEh RUI that"

Now Let's change D with e:

"the tTBe haM EUBe the PaYIOM MaTX tU taYG UR BaHA thTHCM UR MhUeM aHX MhTNM aHX MeaYTHC PaQ UR EaSSaCeM aHX GTHCM aHX PhA the Mea TM SUTYTHC hUt aHX PhetheI NTCM haLe PTHCM SOt PaTt a STt the UAMteIM EITeX SeRUIe Pe haLe UOI Ehat RUI MUBe UR OM aIe UOt UR SIeath aHX aYY UR OM aIe Rat HU hOIIA MaTX the EaINeHteI theA thaHGeX hTB BOEh RUI that"

Now Let's change M with s:

"the tTBe has EUBe the PaYIOs saTX tU taYG UR BaHA thTHCs UR shUes aHX shTNs aHX seaYTHC PaQ UR EaSSaCes aHX GTHCs aHX PhA the sea Ts SUTYTHC hUt aHX PhetheI NTCs haLe PTHCs SOt PaTt a STt the UAsteIs EITeX SeRUIe Pe haLe UOI Ehat RUI sUBe UR Os aIe UOt UR SIeath aHX aYY UR Os aIe Rat HU hOIIA saTX the EaINeHteI theA thaHGeX hTB BOEh RUI that"

Now Let's change U with o:

“the tTBe has EoBe the PaYIOs saTX to taYG oR BaHA thTHCs oR shoes aHX shTNs aHX seaYTHC PaQ oR EaSSaCes aHX GTHCs aHX PhA the sea Ts SoTYTHC hot aHX PhetheI NTCs haLe PTHCs SOt PaTt a STt the oAsteIs EITeX SeRoIe Pe haLe oOI Ehat RoI soBe oR Os aIe oOt oR SIeath aHX aYY oR Os aIe Rat Ho hOIIA saTX the EaINeHteI theA thaHGeX hTB BOEh RoI that”

Now Let’s change H with n:

“the tTBe has EoBe the PaYIOs saTX to taYG oR BanA thTnCs oR shoes anX shTNs anX seaYTnC PaQ oR EaSSaCes anX GTnCs anX PhA the sea Ts SoTYTnC hot anX PhetheI NTCs haLe PTnCs SOt PaTt a STt the oAsteIs EITeX SeRoIe Pe haLe oOI Ehat RoI soBe oR Os aIe oOt oR SIeath anX aYY oR Os aIe Rat no hOIIA saTX the EaINenteI theA thanGeX hTB BOEh RoI that”

Now Let’s change A with d:

“the tTBe has EoBe the PaYIOs saTX to taYG oR Band thTnCs oR shoes anX shTNs anX seaYTnC PaQ oR EaSSaCes anX GTnCs anX Phd the sea Ts SoTYTnC hot anX PhetheI NTCs haLe PTnCs SOt PaTt a STt the odsteIs EITeX SeRoIe Pe haLe oOI Ehat RoI soBe oR Os aIe oOt oR SIeath anX aYY oR Os aIe Rat no hOIId saTX the EaINenteI thed thanGeX hTB BOEh RoI that”

This guess is wrong

Now Let’s change T with i:

“the tiBe has EoBe the PaYIOs saiX to taYG oR BanA thinCs oR shoes anX shiNs anX seaYinC PaQ oR EaSSaCes anX GinCs anX PhA the sea is SoiYinC hot anX PhetheI NiCs haLe PinCs SOt Pait a Sit the oAsteIs EIieX SeRoIe Pe haLe oOI Ehat RoI soBe oR Os aIe oOt oR SIeath anX aYY oR Os aIe Rat no hOIIA saiX the EaINenteI theA thanGeX hiB BOEh RoI that”

Now Let’s change B with m:

“the time has Eome the PaYIOs saiX to taYG oR manA thinCs oR shoes anX shiNs anX seaYinC PaQ oR EaSSaCes anX GinCs anX PhA the sea is SoiYinC hot anX PhetheI NiCs haLe PinCs SOt Pait a Sit the oAsteIs EIieX SeRoIe Pe haLe oOI EhaI RoI some oR Os aIe oOt oR SIeath anX aYY oR Os aIe Rat no hOIIA saiX the EaINenteI theA thanGeX him mOEh RoI that”

Now Let’s change X with d:

“the time has Eome the PaYIOs said to taYG oR manA thinCs oR shoes and shiNs and seaYinC PaQ oR EaSSaCes and GinCs and PhA the sea is SoiYinC hot and PhetheI NiCs haLe PinCs SOt Pait a Sit the oAsteIs EIied SeRoIe Pe haLe oOI EhaI RoI some oR Os aIe oOt oR SIeath and aYY oR Os aIe Rat no hOIIA said the EaINenteI theA thanGed him mOEh RoI that”

Now Let’s change E with c:

“the time has come the PaYIOs said to taYG oR manA thinCs oR shoes and shiNs and seaYinC PaQ oR caSSaCes and GinCs and PhA the sea is SoiYinC hot and PhetheI NiCs haLe PinCs SOt Pait a Sit the oAsteIs cIied SeRoIe Pe haLe oOI chaI RoI some oR Os aIe oOt oR SIeath and aYY oR Os aIe Rat no hOIIA said the caINenteI theA thanGed him mOch RoI that”

Now Let’s change O with u:

“the time has come the PaYIus said to taYG oR manA thinCs oR shoes and shiNs and seaYinC PaQ oR caSSaCes and GinCs and PhA the sea is SoiYinC hot and PhetheI NiCs haLe PinCs Sut Pait a Sit the oAsteIs cIied SeRoIe Pe haLe ouI chaI RoI some oR us aIe out oR SIeath and aYY oR us aIe Rat no huIIA said the caINenteI theA thanGed him much RoI that”

Now Let’s change Y with l:

“the time has come the PaIIus said to taIG oR manA thinCs oR shoes and shiNs and sealinC PaQ oR caSSaCes and GinCs and PhA the sea is SoilinC hot and PhetheI NiCs haLe PinCs Sut Pait a Sit the oAsteIs cIied SeRoIe Pe haLe ouI chaI RoI some oR us aIe out oR SIeath and all oR us aIe Rat no huIIA said the caINenteI theA thanGed him much RoI that”

Now Let's change A with y:

"the time has come the Pallus said to talG oR many thinCs oR shoes and shiNs and sealinC PaQ oR caSSaCes and GinCs and Phy the sea is SoilinC hot and Phethel NiCs haLe PinCs Sut Pait a Sit the oystels clied SeRole Pe haLe oul chat Rol some oR us ale out oR Sleath and all oR us ale Rat no hully said the calNentel they thanGed him much Rol that"

Now Let's change C with g:

"the time has come the Pallus said to talG oR many things oR shoes and shiNs and sealing PaQ oR caSSages and Gings and Phy the sea is Soiling hot and Phethel Nigs haLe Pings Sut Pait a Sit the oystels clied SeRole Pe haLe oul chat Rol some oR us ale out oR Sleath and all oR us ale Rat no hully said the calNentel they thanGed him much Rol that"

Now Let's change S with b:

"the time has come the Pallus said to talG oR many things oR shoes and shiNs and sealing PaQ oR cabbages and Gings and Phy the sea is boiling hot and Phethel Nigs haLe Pings but Pait a bit the oystels clied beRole Pe haLe oul chat Rol some oR us ale out oR bleath and all oR us ale Rat no hully said the calNentel they thanGed him much Rol that"

Now Let's change R with f:

"the time has come the Pallus said to talG of many things of shoes and shiNs and sealing PaQ of cabbages and Gings and Phy the sea is boiling hot and Phethel Nigs haLe Pings but Pait a bit the oystels clied befole Pe haLe oul chat fol some of us ale out of bleath and all of us ale fat no hully said the calNentel they thanGed him much fol that"

Now Let's change G with k:

"the time has come the Pallus said to talk of many things of shoes and shiNs and sealing PaQ of cabbages and kings and Phy the sea is boiling hot and Phethel Nigs haLe Pings but Pait a

bit the oystels clied befole Pe haLe oul chat fol some of us ale out of bleath and all of us ale fat no hully said the calNentel they thanked him much fol that”

Now Let’s change N with p:

“the time has come the Pallus said to talk of many things of shoes and ships and sealing PaQ of cabbages and kings and Phy the sea is boiling hot and Phethel pigs haLe Pings but Pait a bit the oystels clied befole Pe haLe oul chat fol some of us ale out of bleath and all of us ale fat no hully said the calpentel they thanked him much fol that”

Now Let’s change P with w:

“the time has come the wallus said to talk of many things of shoes and ships and sealing waQ of cabbages and kings and why the sea is boiling hot and whethel pigs haLe wings but wait a bit the oystels clied befole we haLe oul chat fol some of us ale out of bleath and all of us ale fat no hully said the calpentel they thanked him much fol that”

Now Let’s change l with r:

“the time has come the walrus said to talk of many things of shoes and ships and sealing waQ of cabbages and kings and why the sea is boiling hot and whether pigs haLe wings but wait a bit the oysters cried before we haLe our chat for some of us are out of breath and all of us are fat no hurry said the carpenter they thanked him much for that”

Now Let’s change Q with r:

“the time has come the walrus said to talk of many things of shoes and ships and sealing war of cabbages and kings and why the sea is boiling hot and whether pigs haLe wings but wait a bit the oysters cried before we haLe our chat for some of us are out of breath and all of us are fat no hurry said the carpenter they thanked him much for that”

Now Let’s change L with v:

“the time has come the walrus said to talk of many things of shoes and ships and sealing war of cabbages and kings and why the sea is boiling hot and whether pigs have wings but wait a bit the oysters cried before we have our chat for some of us are out of breath and all of us are fat no hurry said the carpenter they thanked him much for that”

So the decrypted paragraph is below:

“the time has come the walrus said to talk of many things of shoes and ships and sealing war of cabbages and kings and why the sea is boiling hot and whether pigs have wings but wait a bit the oysters cried before we have our chat for some of us are out of breath and all of us are fat no hurry said the carpenter they thanked him much for that”

Ended
