**Assignment#01**

****

Fall 2022

CSE-425 Computer security

Submitted by: **Ashfaq Ahmad**

Registration No: **19PWCSE1795**

Class Section: **B**

“On my honor, as student of University of Engineering and Technology, I have neither given nor received unauthorized assistance on this academic work.”

Student Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Submitted to:

**Dr: Sadeeq jan sab**

**Nov** 11, 2022

**Department of Computer Systems Engineering**

**University of Engineering and Technology, Peshawar**

1. 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”**

**Solution:**

**Frequencies:**

**A=5 , B=6, C=7,D=28, E=6, F=23, G=3, H=15, I=15, J=0, K=24, L=2, M=21, N=3, O=8, P=7, Q=1, R=10, S=7, T=16, U=19, V=0, W=0, X=10, Y=6, Z=30**

**1ST Iteration:**

**Change ’Z’ with ‘a’ we get.**

**“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”**

**2nd Iteration:**

**Change ’H’ with ‘n’ we get.**

**“KFD KTBD FaM EUBD KFD PaYIOM MaTX KU KaYG UR BanA KFTnCM UR MFUDM anX MFTNM anX MDaYTnC PaQ UR EaSSaCDM anX GTnCM anX PFA KFD MDa TM SUTYTnC FUK anX PFDKFDI NTCM FaLD PTnCM SOK PaTK a STK KFD UAMKDIM EITDX SDRUID PD FaLD UOI EFaK RUI MUBD UR OM aID UOK UR SIDaKF anX aYY UR OM aID RaK nU FOIIA MaTX KFD EaINDnKDI KFDA KFanGDX FTB BOEF RUI KFaK”**

**3rd Iteration:**

**Change ’X’ with ’d’ we get.**

**“KFD KTBD FaM EUBD KFD PaYIOM MaTd KU KaYG UR BanA KFTnCM UR MFUDM and MFTNM and MDaYTnC PaQ UR EaSSaCDM and GTnCM and PFA KFD MDa TM SUTYTnC FUK and PFDKFDI NTCM FaLD PTnCM SOK PaTK a STK KFD UAMKDIM EITDd SDRUID PD FaLD UOI EFaK RUI MUBD UR OM aID UOK UR SIDaKF and aYY UR OM aID RaK nU FOIIA MaTd KFD EaINDnKDI KFDA KFanGDd FTB BOEF RUI KFaK”**

Thus we get the word ‘and’ successfully. It mean up to till our guessing seems correct. Let’s take further iteration.

**4th Iteration:**

**Change ’X’ with‘d’ we get.**

**“KwD KTBD waM EUBD KwD PaYIOM MaTd KU KaYG UR BanA KwTnCM UR MwUDM and MwTNM and MDaYTnC PaQ UR EaSSaCDM and GTnCM and PwA KwD MDa TM SUTYTnC wUK and PwDKwDI NTCM waLD PTnCM SOK PaTK a STK KwD UAMKDIM EITDd SDRUID PD waLD UOI EwaK RUI MUBD UR OM aID UOK UR SIDaKw and aYY UR OM aID RaK nU wOIIA MaTd KwD EaINDnKDI KwDA KwanGDd wTB BOEw RUI KwaK”**

The above guessing is wrong

**5th Iteration:**

**Change ’T’ with ‘i’ we get.**

**“KFD KiBD FaM EUBD KFD PaYIOM Maid KU KaYG UR BanA KFinCM UR MFUDM and MFiNM and MDaYinC PaQ UR EaSSaCDM and GinCM and PFA KFD MDa iM SUiYinC FUK and PFDKFDI NiCM FaLD PinCM SOK PaiK a SiK KFD UAMKDIM EIiDd SDRUID PD FaLD UOI EFaK RUI MUBD UR OM aID UOK UR SIDaKF and aYY UR OM aID RaK nU FOIIA Maid KFD EaINDnKDI KFDA KFanGDd FiB BOEF RUI KFaK”**

**6th Iteration:**

**Change ’D’ with ‘e’ we get.**

**“KFe KiBe FaM EUBe KFe PaYIOM Maid KU KaYG UR BanA KFinCM UR MFUeM and MFiNM and MeaYinC PaQ UR EaSSaCeM and GinCM and PFA KFe Mea iM SUiYinC FUK and PFeKFeI NiCM FaLe PinCM SOK PaiK a SiK KFe UAMKeIM EIied SeRUIe Pe FaLe UOI EFaK RUI MUBe UR OM aIe UOK UR SIeaKF and aYY UR OM aIe RaK nU FOIIA Maid KFe EaINenKeI KFeA KFanGed FiB BOEF RUI KFaK”**

**7th Iteration:**

**Change ’M’ with‘s’ we get.**

**“KFe KiBe Fas EUBe KFe PaYIOs said KU KaYG UR BanA KFinCs UR sFUes and sFiNs and seaYinC PaQ UR EaSSaCes and GinCs and PFA KFe sea is SUiYinC FUK and PFeKFeI NiCs FaLe PinCs SOK PaiK a SiK KFe UAsKeIs EIied SeRUIe Pe FaLe UOI EFaK RUI sUBe UR Os aIe UOK UR SIeaKF and aYY UR Os aIe RaK nU FOIIA said KFe EaINenKeI KFeA KFanGed FiB BOEF RUI KFaK”**

**8th Iteration:**

**Change ’F’ with ‘h’ we get.**

**“Khe KiBe has EUBe Khe PaYIOs said KU KaYG UR BanA KhinCs UR shUes and shiNs and seaYinC PaQ UR EaSSaCes and GinCs and PhA Khe sea is SUiYinC hUK and PheKheI NiCs haLe PinCs SOK PaiK a SiK Khe UAsKeIs EIied SeRUIe Pe haLe UOI EhaK RUI sUBe UR Os aIe UOK UR SIeaKh and aYY UR Os aIe RaK nU hOIIA said Khe EaINenKeI KheA KhanGed hiB BOEh RUI KhaK”**

We get another word ‘has’ successfully. Still our guessing seems correct. Let’s take further iterations.

**9th Iteration:**

**Change ’K’ with’s’ we get.**

**“she siBe has EUBe she PaYIOs said sU saYG UR BanA shinCs UR shUes and shiNs and seaYinC PaQ UR EaSSaCes and GinCs and PhA she sea is SUiYinC hUs and PhesheI NiCs haLe PinCs SOs Pais a Sis she UAsseIs EIied SeRUIe Pe haLe UOI Ehas RUI sUBe UR Os aIe UOs UR SIeash and aYY UR Os aIe Ras nU hOIIA said she EaINenseI sheA shanGed hiB BOEh RUI shas”**

This guessing is probably incorrect. We got the word ‘she’ but it doesn’t make a sense.

**9th Iteration:**

**Change ’K’ with‘t’ we get.**

**“the tiBe has EUBe the PaYIOs said tU taYG UR BanA thinCs UR shUes and shiNs and seaYinC PaQ UR EaSSaCes and GinCs and PhA the sea is SUiYinC hUt and PhetheI NiCs haLe PinCs SOt Pait a Sit the UAsteIs EIied SeRUIe Pe haLe UOI Ehat RUI sUBe UR Os aIe UOt UR SIeath and aYY UR Os aIe Rat nU hOIIA said the EaINenteI theA thanGed hiB BOEh RUI that”**

**10th Iteration:**

**Change ’B’ width’s’ we get.**

**“the time has EUme the PaYIOs said tU taYG UR manA thinCs UR shUes and shiNs and seaYinC PaQ UR EaSSaCes and GinCs and PhA the sea is SUiYinC hUt and PhetheI NiCs haLe PinCs SOt Pait a Sit the UAsteIs EIied SeRUIe Pe haLe UOI Ehat RUI sUme UR Os aIe UOt UR SIeath and aYY UR Os aIe Rat nU hOIIA said the EaINenteI theA thanGed him mOEh RUI that”**

**11th Iteration:**

**Change ’E’ width’c’ we get.**

**“the time has cUme the PaYIOs said tU taYG UR manA thinCs UR shUes and shiNs and seaYinC PaQ UR caSSaCes and GinCs and PhA the sea is SUiYinC hUt and PhetheI NiCs haLe PinCs SOt Pait a Sit the UAsteIs cIied SeRUIe Pe haLe UOI chat RUI sUme UR Os aIe UOt UR SIeath and aYY UR Os aIe Rat nU hOIIA said the caINenteI theA thanGed him mOch RUI that”**

**12th Iteration:**

**Change ’U’ width ’o’ we get.**

**“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 chat 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”**

**13th Iteration:**

**Change ’P’ width ’s’ we get.**

**“the time has come the saYIOs said to taYG oR manA thinCs oR shoes and shiNs and seaYinC saQ oR caSSaCes and GinCs and shA the sea is SoiYinC hot and shetheI NiCs haLe sinCs SOt sait a Sit the oAsteIs cIied SeRoIe se haLe oOI chat 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”**

This guessing seems incorrect.

**14th Iteration:**

**Change ’Y’ width ’l’ we get.**

**“the time has come the PalIOs said to talG 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 SOt Pait a Sit the oAsteIs cIied SeRoIe Pe haLe oOI chat RoI some oR Os aIe oOt oR SIeath and all oR Os aIe Rat no hOIIA said the caINenteI theA thanGed him mOch RoI that”**

**15th Iteration:**

**Change ’G’ width ’k’ we get.**

**“the time has come the PalIOs said to talk oR manA thinCs oR shoes and shiNs and sealinC PaQ oR caSSaCes and kinCs and PhA the sea is SoilinC hot and PhetheI NiCs haLe PinCs SOt Pait a Sit the oAsteIs cIied SeRoIe Pe haLe oOI chat RoI some oR Os aIe oOt oR SIeath and all oR Os aIe Rat no hOIIA said the caINenteI theA thanked him mOch RoI that”**

**16th Iteration:**

**Change ’A’ width ’y’ we get.**

**“the time has come the PalIOs said to talk of many thinCs of shoes and shiNs and sealinC PaQ of caSSaCes and kinCs and Phy the sea is SoilinC hot and PhetheI NiCs haLe PinCs SOt Pait a Sit the oysteIs cIied SefoIe Pe haLe oOI chat foI some of Os aIe oOt of SIeath and all of Os aIe fat no hOIIy said the caINenteI they thanked him mOch foI that”**

**17th Iteration:**

**Change ’L’ width ’v’ we get.**

**“the time has come the PalIOs said to talk of many things of shoes and ships and sealing PaQ of caSSages and kings and Phy the sea is Soiling hot and PhetheI pigs have Pings SOt Pait a Sit the oysteIs cIied SefoIe Pe have oOI chat foI some of Os aIe oOt of SIeath and all of Os aIe fat no hOIIy said the caIpenteI they thanked him mOch foI that”**

**18th Iteration:**

**Change ’P’ width ’w’ we get.**

**“the time has come the walIOs said to talk of many things of shoes and ships and sealing waQ of caSSages and kings and why the sea is Soiling hot and whetheI pigs have wings SOt wait a Sit the oysteIs cIied SefoIe we have oOI chat foI some of Os aIe oOt of SIeath and all of Os aIe fat no hOIIy said the caIpenteI they thanked him mOch foI that”**

**19th Iteration:**

**Change ’S’ width ’b’ we get.**

**“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 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”**

**20th Iteration:**

**Change ’Q’ width ’r’ we get.**

**“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”**

**This is final decrypted text.**