IT\_120\_Module 5\_Lab\_4

Exercise 1: Caesar Cipher

1. Encrypt the message MATH with the Caesar cipher with 4 as the key.

**QEXL** To encrypt this, I used a Caesar Cipher tool found on Cryptii.com. In order to encrypt the message I would first go to the second box and make sure the word “encode” is clicked on. Then underneath, I would put the shift at 4 as the directions said. After that, I go back to the first box and type in “MATH.” Once that is completed, I would go back to the second box and click on the word “decode” so that it is highlighted. This shows me the ciphertext of the original word in the third box.

1. Encrypt the message CRYPTO with the Caesar cipher with 6 as the key.

**GVCTXS** To encrypt this, I used a Caesar Cipher tool found on Cryptii.com. In order to encrypt the message I would first go to the second box and make sure the word “encode” is clicked on. Then underneath, I would put the shift at 6 as the directions said. After that, I go back to the first box and type in “CRYPTO.” Once that is completed, I would go back to the second box and click on the word “decode” so that it is highlighted. This shows me the ciphertext of the original word in the third box.

3. The message QIIX PEXIV was encrypted using the Caesar cipher with 4 as the key. Decrypt the message.

**MEET LATER** To decrypt this, I used a Caesar Cipher tool found on Cryptii.com. In order to decrypt the message I would first go to the second box and make sure the word “decode” is clicked on. Then underneath, I would put the shift at 4 as the directions said. After that, I go back to the first box and type in “QIIX PEXIV.” Once that is completed, I would go back to the second box and click on the word “decode” so that it is highlighted. This shows me the ciphertext of the original word in the third box.

1. The message SKKZ NKXK was encrypted using a Caesar cipher. Decrypt the message.

**MEET HERE** To decrypt this, I used a Caesar Cipher tool found on Cryptii.com. In order to decrypt the message I would first go to the second box and make sure the word “decode” is clicked on. After that, I go back to the first box and type in “SKKZ NKXK.” I would then return to the second box and play trial and error with the shift number to in find out what the word is. The result in the shift is 6 since I put it at that number and then decoded the ciphertext so that it shows “MEET HERE” as the plaintext word in the third box.

Exercise 2: Vignere cipher `

1. Encrypt FOLLO WTHEY ELLOW BRICK ROAD with the keyword OZ.

**TNZKC VHGSX SKZNK AFHQJ FNOC** To encrypt this message, I used a Vignere cipher tool found on dcode.fr. I would first go down to the section where it says Vignere Encoder. I would then type the message into the large box. After, I would go down to the Cipher key and type in the word “OZ” into the box. Then, I click on ENCRYPT right at the bottom. The new encrypted message will then show on the top left corner of the webpage under “results.”

1. Decrypt LOSVW AZBSH DHQID ARSLG EL, encrypted with the Vignere cipher using SHOES as a key.

**THERE IS NO PLACE LIKE HOME** To decrypt this message, I used a Vignere cipher tool found on dcode.fr. I would go to the top section where it says Vignere cipher decoder. In the big box, I would type in the encrypted message. Afterwards underneath “Decryption Method,” I would select the first option which is “Knowing a key/password.” From there, I would type in the box the key from the directions. Then, I would click on DECRYPT at the bottom. The new decrypted message will then show on the top left corner of the webpage under “results.” At first I thought it was wrong because of the way the message was spelled out but then I realize it was correct and that the spacing of the letters and words were different since it was shown as THERE ISNOP LACEL IKEHO ME.

Exercise 3: Breaking the Caesar Cipher

1. Decrypt the message encrypted with a Caesar cipher: PAXG LAHNEW B KXMNKG

**WHEN SHOULD I RETURN**

1. Decrypt the message encrypted with a Caesar cipher: QUCN ZIL U JBIHY WUFF

**WAIT FOR A PHONE CALL**

1. Decrypt the message encrypted with a Caesar cipher: GUR ENOOVG PENJYRQ BHG BS VGF UBYR

**THE RABBIT CRAWLED OUT OF ITS HOLE**

1. Decrypt the message encrypted with a Caesar cipher:

MAXLX TKXGM MAXWK HBWLR HNKXE HHDBG ZYHK

**THESE ARENT THE DROIDS YOU ARE LOOKING FOR**

For all of these problems, I used the same method I used for the third problem in exercise 1 using the website, Cryptii.com. I first go to the second box and make sure the word “decode” is clicked on which will then appear on the first box. From there I would type the encrypted message into that box. From there it was all trial and error in figuring out which shift key to determine what the plaintext word is which you can change back in the second box. Changing the number in the shift key allows for each letter to shift to the next or previous letter of the alphabet. You continue this process until the message forms into readable text found in the third box. For problem 1, the shift number is 19. For problem 2, the shift number is 20. For problem 3, the shift number is 13. Finally for problem 4, the shift number is 19.

Exercise 4: Breaking the Vignere Cipher `

1. Decrypt the following message, which was encrypted with a Vignere cipher of length 4: `

BCRRBCQORHKEPSLSLCWRWXXDESPEZMPYQWCEBCBOSFHCIZHSQWVHCBRWRVLNEGDRCKRRQS.

**Do or do not there is no try. Judge me by size do you? Reckless is he. Now things are worse.**

Since it says with a Vignere cipher tool, I used the same tool from Exercise 2 which is from dcode.fr. I typed in the encrypted message inside the big box located under the Vignere decoder. From there I click the “Knowing key length/size” underneath which description to use. I typed the key length as 4 and then clicked the ENCRYPT button. Once it showed the results on the top left side. It displays multiple solutions, but the right answer is the first one. The reason is because out of all of them, the message actually forms readable text. Next to the plaintext’s sentence there is a password on the left side which you can also use as a way to decrypt the message. You do this by clicking on “Knowing key/password” and typing the codeword “YODA” into it. This will result in the same decrypted message.

2. Decrypt the following message, which was encrypted with a Vignere cipher of length 4: `

KBPYU BACDM LRQNM GOMLG VETQV PXUQZ LRZNM GOMLG VETQV PXYIM HDYQL BQUBR

YILRJ MTEGW YDQWE GUPGC UABRY ILRJM XNQKA MHJXJ KMYGV ETQVP XCRWV FQNBL

EZXBW TBRAQ MUCAM FGAXY UWGMH TBEJB BRYIL RJMLC CAHLQ NWYTS GCUAB RYILR

JMLNT QGEQN AMRMB RYILR JMPGP BXPQN WCUXT GT

**It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness,**

**it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of**

**Darkness, it was the spring of hope, it was the winter of despair.**

The process for finding the decrypted message was the exact same as for the first problem of this exercise. . I typed in the encrypted message inside the big box located under the Vignere decoder. From there I click the “Knowing key length/size” underneath which description to use. I typed the key length as 4 and then clicked the ENCRYPT button. Once it showed the results on the top left side. It displays multiple solutions, but the right answer is the first one. The reason is because out of all of them, the message actually forms readable text. Next to the plaintext’s sentence there is a password on the left side which you can also use as a way to decrypt the message. You do this by clicking on “Knowing key/password” and typing the codeword “CITY” into it. This will result in the same decrypted message. A Vignere Cipher tool is different compared to a Caesar cipher because this tool is just a Caesar cipher with longer keys that allow it to be crypted multiple ways.

Exercise 5

Use what you know to decrypt the following message. Note, the original word spacing is intact:

LKZB RMLK X JFAKFDEQ AOBXOV TEFIB F MLKABOBA TBXH XKA TBXOV LSBO JXKV X NRXFKQ

XKA ZROFLRP SLIRJB LC CLODLQQBK ILOB TEFIB F KLAABA KBXOIV KXMMFKD PRAABKIV

QEBOB ZXJB X QXMMFKD XP LC PLJB LKB DBKQIV OXMMFKD OXMMFKD XQ JV ZEXJYBO

ALLO Q FP PLJB SFPFQBO F JRQQBOBA QXMMFKD XQ JV ZEXJYBO ALLO LKIV QEFP XKA KLQEFKD JLOB

**ONCE UPON A MIDNIGHT DREARY WHILE I PONDERED WEAK AND WEARY OVER MANY A QUAINT**

**AND CURIOUS VOLUME OF FORGOTTEN LORE WHILE I NODDED NEARLY NAPPING SUDDENLY**

**THERE CAME A TAPPING AS OF SOME ONE GENTLY RAPPING RAPPING AT MY CHAMBER**

**DOOR T IS SOME VISITER I MUTTERED TAPPING AT MY CHAMBER DOOR ONLY THIS AND NOTHING MORE**

For this exercise I tested using both the Caesar and Vignere tools. The steps for encrypting were the same used for both, respectively. For Caesar, the steps are found in exercise 4. For Vignere, the steps are found in exercise 5. They both require that the shift be at 23 in order for the message to be readable. For the Caesar, using the tool from Cryptii.com, it displayed the message correctly. For Vignere, using the tool from dcode.com, the correct answer is the same message as the one using the Caesar tool. I found interesting is that since there are also other solutions because of the Vignere cipher being able to be crypted multiple ways, the same message is still displayed in other ways because some of the right letters that were found in the correct one were swapped with different letters. For example, “weary” is the correct word, but in a different decryption, it is spelled as “wkary.”