Ahmad Shayeq Nijrabi

IT\_120\_Module 5\_Lab\_4

Saturday, February 20, 2021

Exercise 1: Caesar Cipher

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

Ans: QEXL

Description: I used the Caesar ciphar tool to encrypt the message MATH and got the result as QEXL. I got this website’s link from cryptography presentation and it was a helpful resource for a quick encryption. The encryption steps were the following – typed the plain text, entered the key as 4, clicked the encrypt/decrypt button, and got the result. <https://www.xarg.org/tools/caesar-cipher/>

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

Ans: IXEVZU

Description: The encryption process I used for this question was same as question one with the key as the only difference. The only thing that I changed in this question was the keyword to 6 from 4.

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

Ans: MEET LATER

Description: Decrypting these letters were a bit different from encryptions above as the keyword was unknown. I didn’t know what to enter as the key, so after typing the encrypted letters on screen and choosing random keys, I kept getting wrong answers. Eventually I choose guess as the key and that eventually generated the proper key (22) and correct answer. <https://www.xarg.org/tools/caesar-cipher/>

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

Ans: MEET HERE

Description: The process for this question was same as question three with the key being as the only difference. After choosing guess for key I got 20 this time instead of 22 from last time.

Exercise 2: Vignere cipher `

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

Ans: TNZKC VHGSX SKZNK AFHQJ FNOC

Description: I tried to encrypt this message with the Caesar cipher tool, but it didn’t work so I found Vigenere Tool specific website. The steps of encryption are as below:

- open the website <https://www.boxentriq.com/code-breaking/vigenere-cipher>

- type the plain text in Vigenere tool text bar

- type OZ as the key on the key bar

- standard mode & English language

- click encode to generate the encrypted result

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

Ans: THERE IS NO PLACE LIKE HOME

Description: The process for decryption of this message was as below:

- open the website <https://www.boxentriq.com/code-breaking/vigenere-cipher>

- type the encrypted text in Vigenere tool text bar

- type shoes as the key on the key bar

- standard mode & English language

- click decode to generate the decrypted result

Exercise 3: Breaking the Caesar Cipher

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

Ans: WHEN SHOULD I RETURN

Description: I used the Robert Eisele website’s Caesar cipher encryption/decryption tool to decrypt this message. The process included – typing the plain text on text bar, choosing guess as the key, and decrypting. <https://www.xarg.org/tools/caesar-cipher/>

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

Ans: Wait for a phone call.

Description: the steps are similar to the first question.

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

Ans: THE RABBIT CRAWLED OUT OF ITS HOLE

Description: The process was same as question one of this exercise.

* Entering the plain text
* Choosing “guess” as the key
* Decrypting the message
* Same website was used

4. Decrypt the message encrypted with a Caesar cipher:

MAXLX TKXGM MAXWK HBWLR HNKXE HHDBG ZYHK

Ans: THESE AREN’T THE DROIDS YOU’RE LOOKING FOR

Description: the decryption process of this message was also same as other questions in this exercise, but there was a problem with the arrangement of letter’s spacing in this message that got solved in the second try.

Exercise 4: Breaking the Vignere Cipher `

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

BCRRBCQORHKEPSLSLCWRWXXDESPEZMPYQWCEBCBOSFHCIZHSQWVHCBRWRVLNEGDRCKRRQS.

Ans: do or do not there is no try judge me by my size do you reckless is he now things are worse

Description: decrypting this long message was a little different as it seems. The issue was that there is no letter mentioned for key in this message which is required for most Vignere ciphere site.. However, I managed to find an option on the BOXENTRIQ site called auto solve (without key) which made the decryption of the message easily possible and generated a list of auto solve results and this decrypted messages was the closest one to the correct answer. <https://www.boxentriq.com/code-breaking/vigenere-cipher>

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

Ans:

Original decrypted message: it was the best of times it was the worst 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.

Edited: 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.

Description: the decryption process for this message was similar to message one of this exsercise. I’ve written two same decrypted message above, because the website generated the answer without spacing so I edit it by myself.

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

Ans:

Original encrypted message: 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

Edited: 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. ’Tis some visitor, I muttered, tapping at my chamber

door – Only this, and nothing more.

Description: The process of decrypting this message was also similar to the previous exercise. The steps are as bellow:

* Type or paste the encrypted message on the text bar of Vigenere Tool
* Select auto solve (without key) as the key is unkown
* Auto results generate many messages
* Choose the best fit and correct one
* Website: <https://www.boxentriq.com/code-breaking/vigenere-cipher>