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

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

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

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

I used a cryptography website (https://www.dcode.fr/caesar-cipher) to decode and encode the messages. I enter the first three question into a box to decode and encode the message and entered the key to get the answer. In the last question, I needed to decode the message by using a brute-force attack and I got MEET HERE with a key of 6 shift.

Exercise 2: Vignere cipher `

1. Encrypt FOLLO WTHEY ELLOW BRICK ROAD with the keyword OZ. TNZKC VHGSX SKZNK AFHQJ FNOC

2. Decrypt LOSVW AZBSH DHQID ARSLG EL, encrypted with the Vignere cipher using SHOES as a key. THERE IS NO PLACE LIKE HOME

I used the same website but for Vigenere cipher (https://www.dcode.fr/vigenere-cipher). I had no problems with entering all the encrypted messages into the boxes and decode with the key. Also, I had to fix the spacing.

Exercise 3: Breaking the Caesar Cipher

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

WHEN SHOULD I RETURN (+19)

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

WAIT FOR A PHONE CALL (+20)

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

THE RABBIT CRAWLED OUT OF ITS HOLE (+13)

4. Decrypt the message encrypted with a Caesar cipher:

MAXLX TKXGM MAXWK HBWLR HNKXE HHDBG ZYHK

THESE ARENT THE DROIDS YOURE LOOKING FOR (+19)

I used the same website (https://www.dcode.fr/caesar-cipher) to decode all the messages. I enter the all the encrypted messages into the box, but I needed to decode the all message by using brute-force attacks and I got the answers the key is right next answer for each one. Also, I had to fix the spacing.

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 MY SIZE DO YOU RECKLESS IS HE NOW THINGS ARE WORSE (YODA)

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

(CITY)

I used the same website (https://www.dcode.fr/vigenere-cipher) to decode all the messages. I enter the all the encrypted messages into the box, but I needed to decode the all message by knowing the key length of letters. So, I put in the given key length and found all the answers and put the key right next to it. Also, I had to fix the spacing.

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 (+23)

I looked at the encryption code in the same website (https://www.dcode.fr/caesar-cipher) and saw that the letters were repeating clear to see. I thought of trying a Caesar cipher and use a brute-force attack. I got the answer above with a key of +23.