IT\_120\_Module 5\_Lab\_4\_Karim\_El\_Mehri

Exercise 1: Caesar Cipher

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

M=Q, A=E, T=X and H=L. As the key is 4, I encrypted this message by moving 4 times from that letter and use that fourth letter from the original number.

QEXL.

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

C=I , R=X , Y=E , P=V , T=Z , O=U . As the key is 6, I encrypted this message by moving 6 times from the original letter and use that sixth letter. For the Y, we had to come back at the beginning of the alphabet and keep counting to 6 to find that letter that will replace the original.

IXEVZU

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

I did the opposite of what I did in question 1. To decrypt this message, I had to move back 4 times from the encrypted letter to find the original one.

MEET LATER

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

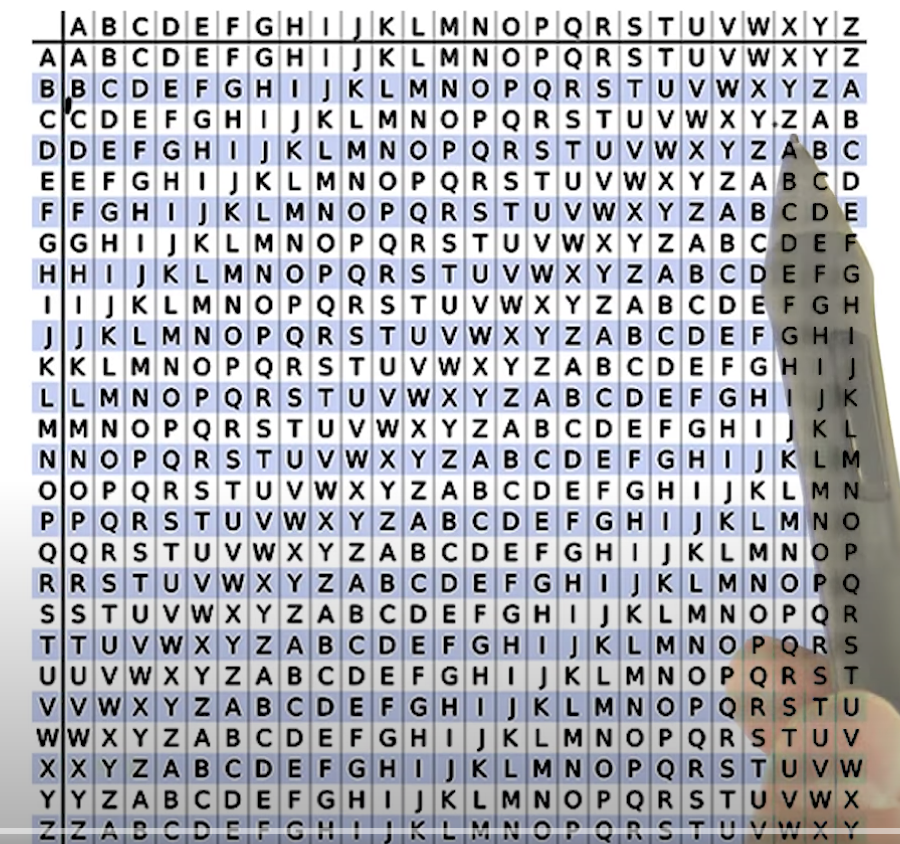
S=M, K=E, Z=T and so on. We moved 6 times back from the encrypted letter to find the original letter. Example: S, 6 letters back before S is M. To make it easy, I have used two lines of alphabet; the first line is the alphabet and the second is moved back so the 6th letter from the original letter comes right down the first line of alphabet. The link I used to complete exercise 1 is <https://www.youtube.com/watch?v=pIt4Q68J00A> .



Exercise 2: Vignere cipher `

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

For exercise 2, I have used this table below:



To encrypt the message, I have used the table below by using OZ as key. For example, I chose the letter O of the key at the first line of the table and then went straight down until I find the letter that matches F, for this case it is T. For the second letter in the message, which is O, we used the Z as key and went down until we match the letter O; in this case it is N. Because our keyword is composed only from two letters, we start using the first key letter for the first letter of the message, and the second key letter for the second letter of the message and for the third letter of the message, we have to restart using that same keyword by reusing that first key letter for the third letter of the message and so on. Example, our message is OZOZO ZOZOZ OZOZOZ OZOZO ZOZO.

TNZKC VHGSX SKZNK AFHQJ FNOC

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

What I did here to decrypt the message is the opposite of what I did in question 1 of exercise 2. I have use the keyword SHOES. I used the first letter of the keyword for the first letter of the message; so S for L. Contrary to the first question, I choose S on the vertical side and went straight until I find the letter L and then went up until the end of the table to find the original letter T. For the second letter of the message I used H as key, and chose it on the vertical line than went straight horizontally to O on, than from O I went up the table to find the original letter which is H. For the third letter of the message I used the same process but used O as key in the vertical line to search for the letter S on the horizontal line that starts with O, then from S I went up the table to find the letter E. We did the same for the fourth letter of the message by using the fourth letter of the keyword, and for the fifth letter of the message we used the fifth letter of the keyword and for the sixth letter of the message we restarted using the keyword from the beginning because this keyword is not very long. Example of this message: SHOES SHOES SHOES SHOES SH. So the decrypted message is THERE IS NO PLACE LIKE HOME.

I think without the table and without understanding decrypt is the opposite of encrypt we would not be able to use the Vignere cipher. I have used this link below to answer to exercise 2: <https://www.youtube.com/watch?v=E352JJ8xv48> .

Exercise 3: Breaking the Caesar Cipher

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

To decrypt the following message I have used <https://www.xarg.org/tools/caesar-cipher/> that allowed me to decrypt messages in exercise 3 by choosing “guess” as key and write the encrypted message to have an output of the decrypted message. The decrypted message for this question is WHEN SHOULD I RETURN. To decrypt this message, we had to move back 7 times from the encrypted letter to find the original, decrypted letter. The key for this message is 7.

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

Like in question 1, exercise 3, I chose “guess” as key and wrote the encrypted message to have an output of the decrypted message. The decrypted message for this question is

~~AEMX JSV E TLSRI GEPP~~ (this is what appeared while using that link), but I have found that the answer is actually WAIT FOR A PHONE CALL if we chose the key as 6. To decrypt this message, we had to move back 6 times from the encrypted letter to find the original, decrypted letter. The key for this message is 6.

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

Like in question 1 and 2, exercise 3, I chose “guess” as key and wrote the encrypted message to have an output of the decrypted message. The decrypted message for this question is THE RABBIT CRAWLED OUT OF ITS HOLE. To decrypt this message, we had to move back 13 times from the encrypted letter to find the original, decrypted letter. The key for this message is 13.

4. Decrypt the message encrypted with a Caesar cipher:

MAXLX TKXGM MAXWK HBWLR HNKXE HHDBG ZYHK

Like in question 1,2 and 3, exercise 3, I chose “guess” as key and wrote the encrypted message to have an output of the decrypted message. The decrypted message for this question is THESE ARENT THE DROIDS YOURE LOOKING FOR. To decrypt this message, we had to move back 7 times from the encrypted letter to find the original, decrypted letter. The key for this message is 7.

Exercise 4: Breaking the Vignere Cipher `

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

BCRRBCQORHKEPSLSLCWRWXXDESPEZMPYQWCEBCBOSFHCIZHSQWVHCBRWRVLNEGDRCKRRQS.

For exercise 4, I used <https://www.boxentriq.com/code-breaking/vigenere-cipher> to decrypt message using the Vignere Cipher. To decrypt this encrypted message above, we have to find the keyword that we use as a key to decrypt or encrypt the message. Using this link allowed me to find the key which is “yoda” and to find, decrypt the message “Do or do not there is no try judge me by size do you reckless is he now things are worse”.

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

Using the same process as question 1, exercise 4 I was able to find the key for this message which is “city”, and found the decrypted message

“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”

Adding commas to the decrypted message will be useful for us to be able to better understand the message.

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

Using the Caesar cipher tools, the link I used for exercise 3, I was able to decrypt the message and find the original which is “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”

I have also found the key for this message which is “3”.