IT_120_Module 5_Lab_4

Rosi Reyes-Alvarenga

Exercise 1: Caesar Cipher

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

Explanation: I know that the key is 4 so I just shift 4 letters from the original letter. For example if you shift 4 from M, you end up at the letter Q. I did this process with each letter.

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

Explanation: I know that the key is 6, so I just shifted 6 letters from the beginning letter. For example if you shift 6 from C you end up at the letter I. I did this process with each letter.

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

Explanation: I know that the key is 4, and in this case I have to decrypt so I did the previous process backwards. I instead shifted 4 keys backwards from the beginning letter. For example if you shift 4 letters backwards from Q you end up at the letter M. I did this process with each letter.

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

I did the same process above except this time I had to shift 6 backwards starting at the letter S.

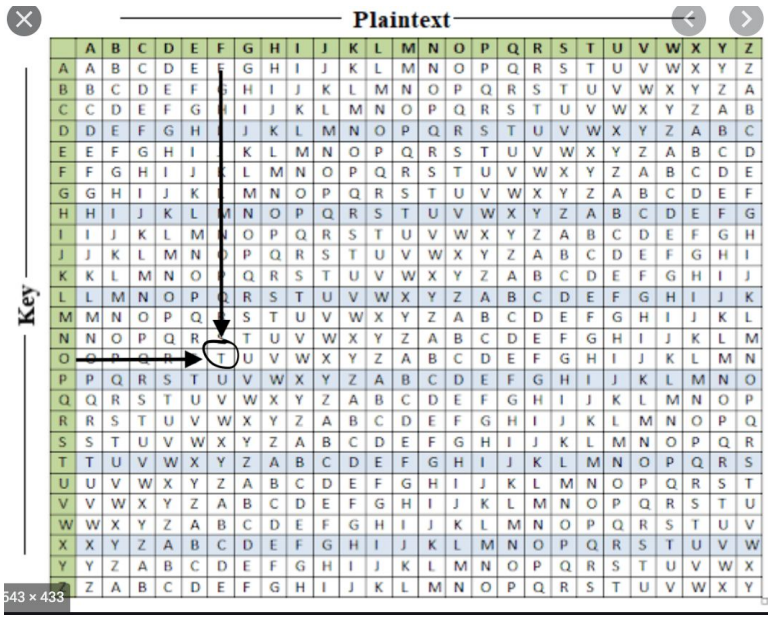
At first I thought I had to shift 4 because the previous example was 4 but that didn't make any sense so then I tried 6 since in the first two examples the two keys used were 4 and 6.

Exercise 2: Vignere cipher `

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

TNZKC VHGSX SKZNK AFHQJ FNOC

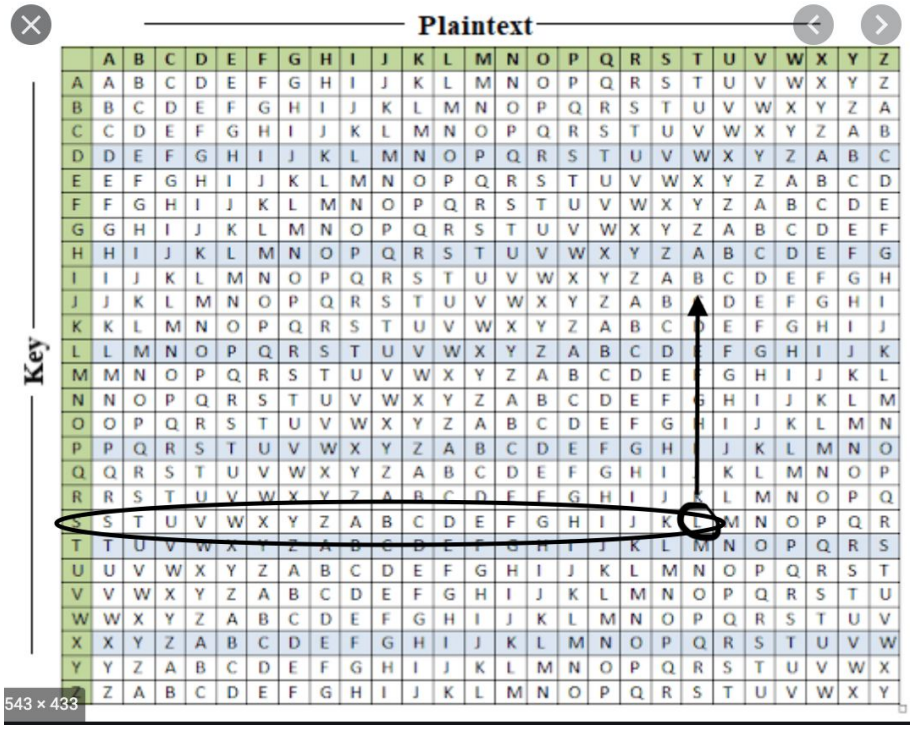
Explanation: I used the vigenere cipher table. I repeated the keyword OZ throughout the message that is to be encrypted and matched the key with its corresponding letter. For example O matches with F and O matches with N etc.. Then what I would do at the table is I would go down on the left side of the table to look for the letter O or Z and then I would go to the top and look for the letter it corresponds to. Then I would see what letter they connect at and then that would give me the answer or letter to use in the encrypted message. Process below.



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

THERE IS NO PLACE LIKE HOME

Explanation: I used the vigenere cipher table to decrypt the message, but this time around it was a bit different. Instead of looking for the letter where both the key letter and plain text letter met I instead went to the corresponding key letter and went through the row to look for the letter that it matched to. Then from there I would go up and see what letter it matched to. For example S pairs with L. Then from there I would go to the S row on the left and continue right on the row until I found the letter L. Then when I found the letter L I saw that I found the letter L under the column of T. Example of process shown below.



Exercise 3: Breaking the Caesar Cipher

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

WHEN SHOULD I RETURN

explanation: I used the website https://www.xarg.org/tools/caesar-cipher/

After I saw the answer and the number of the key I would try it out on my own just to understand how the site got to that answer. I know that the key is 7 so for example I counted 7 letters from P and ended up at W. I did that with each letter in the encrypted message.

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

WAIT FOR A PHONE CALL

Explanation: I used the website https://www.xarg.org/tools/caesar-cipher/

I struggled with this one a bit but only because everytime I would enter guess into the Key option it would give inaccurate numbers so I physically had to go through each number and look at the results for each number. I got to the key number 6 and got my final answer. Then again to understand how the site got to the answer I went through the same process as above except this time I only shifted 6 letters. For example, I shifted 6 letters to the right from Q and I got to W, which was the first letter of the message.

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

THE RABBIT CRAWLED OUT OF ITS HOLE

Explanation: I used the website https://www.xarg.org/tools/caesar-cipher/

I entered it on the website and got the answer along with the key number which is 13. Then like in the previous two exercises I did the process myself. I shifted 13 letters from the original letter. For example I shifted 13 letters from G and I got the letter T, which is the first letter of the message. I did that with each letter in the encrypted message.

4. Decrypt the message encrypted with a Caesar cipher:

MAXLX TKXGM MAXWK HBWLR HNKXE HHDBG ZYHK

THESE AREN'T THE DROIDS YOU'RE LOOKING FOR

Explanation: I used the website https://www.xarg.org/tools/caesar-cipher/

I entered it on the website and got the answer along with the key number which is 7. Then after knowing the key number I did the process on my own. I shifted 7 letters from each letter in the encrypted message.

Exercise 4: Breaking the Vignere Cipher `

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

BCRR BCQO RHKE PSLS LCWR WXXD ESPE ZMPY QWCE BCBO SFHC IZHS QWVH CBRW RVLN EGDR CKRR QS.

DO OR DO NOT THERE IS NO TRY JUDGE ME BY SIZE DO YOU RECKLESS IS HE NOW THINGS ARE WORSE

Explanation: I really struggled with this one. I insisted on trying to find the key word for this exercise, I watched countless videos trying to learn how to find the key word with the key length. Although I watched countless videos I wasn't able to find the key word. I ended up using the following website (https://www.dcode.fr/vigenere-cipher). I typed in the encrypted message along with the key length and looked at the different key word combinations and the messages they produced. Then I saw that the keyword YODA was the only key word that produced actual phrases instead of just random letters. The keyword yoda produced the message above. Afterwards just to double check I did the process on the vigenere cipher table. I repeated the keyword yoda and matched it to its corresponding letter. For example, Y corresponds to B. Then I would go on the table and look at the row of Y and find the column that B fell under. If you look at the Y row you'll see that B falls under column D. Then I repeated these steps with the rest of the words.

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

KBPY UBAC DMLR QNMG OMLG VETQ VPXU QZLR ZNMG OMLG VETQ VPXY IM HD YQLB QUBR

IT WAS THE BEST OF TIMES IT WAS THE WORST OF TIMES IT WAS THE AGE OF WISDOM IT

Explanation: I used this website https://www.dcode.fr/vigenere-cipher . I saw that the keyword CITY produced actual phrases. The keyword CITY produced the first part above. I figured since it produced the phrase above that it will also work for the following phrases.

YILR JMTE GWYD QWEG UPGC UABR YILR JMXN QKAM HJXJ KMYG VETQ

VPXC RWVF QNBL

WAS THE AGE OF FOOLISHNESS IT WAS THE EPOCH OF BELIEF IT WAS THE EPOCH OF IN

Explanation: I used the keyword city and the vigenere table. I matched the encrypted letters with its corresponding letter in the key word. For example Y corresponds to C etc.. Then on the table I went to the the left side and went through the row of C and found what column the letter Y was under. It was under W so I knew that letter was part of the decrypted message. Then I repeated this process with the rest of the letters in the encrypted message and the keyword letters.

EZXB WTBR AQMU CAMF GAXY UWGM HTBE JBBR YILR JMLC CAHL QNWY

TSGC UABR YILR

CREDULITY IT WAS THE SEASON OF LIGHT IT WAS THE SEASON OF DARKNESS IT WAS T

Explanation: I used the keyword CITY and repeated the same process stated above on the vigenere table.

JMLN TQGE QNAM RMBR YILR JMPG PBXP QNWC UXTG T

HE SPRING OF HOPE IT WAS THE WINTER OF DESPAIR

Explanation: I used the keyword CITY and repeated the same process I used for the second and third phrase. I repeated the process on the vigenere table as well.

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

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

Explanation: I used the website https://www.dcode.fr/vigenere-cipher . This time it was a little difficult because I did not know the keyword or key length. Yet after a few times of putting in random key length numbers I realized that I always got the same letter for keyword which was “X”. The only thing was that everytime I inserted a different number it would repeat the letter x for the number I had inserted in the key length box. For example, If I put the key length to be 3, the keyword would turn out to be “XXX” and if I put 4 it would be “XXXX.” Knowing this I made the keyword “X” and then I began the process of decrypting the message through the use of the vigenere table. I uncovered the first message through the website since that was the message I put in for the site to decrypt.

Although the website decrypted the first message for me, I decrypted the following 3 messages through the vigenere table. To do that, I would go to the X row on the left side of the table and look for the letter that is part of the encrypted message. After finding the letter I was looking for I would look at what letter column it was under and then after I saw what letter column it belonged to I would write it down. For example if you look at the row of x and look for the letter K you'll see that it falls under the column of N. I repeated this process for the following 3 messages.

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

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

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

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

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

DOOR TIS SOME VISITOR I MUTTERED TAPPING AT MY CHAMBER DOOR ONLY THIS AND NOTHING MORE