

Mary Mac Bradshaw

Dr. Ermicio

IT-120-B

21 February 2021

Module 5: Lab 4 Exercises

Exercise 1

1. QEXL; I obtained this answer using Caesar cipher by shifting the original letters of MATH with one further in the alphabet. With 4 as the key, this means that each letter is substituted with a letter that is four after the original in the alphabet. For example, the letter M is followed by (1) N, (2) O, (3) P, (4) Q, so the letter Q would be M encrypted with 4 as the key, followed by EXL.
2. IXEVZU; I obtained this answer using Caesar cipher by shifting the original letters of CRYPTO with one further in the alphabet. With 6 as the key, this means that each letter is substituted with a letter that is four after the original in the alphabet. For example, the letter C is followed by (1) D, (2) E, (3) F, (4) G, (5) H, (6) I, so the letter I would be C encrypted with 6 as the key, followed by XEVZU. For letters that reach the end of the alphabet -- such as Y, in this example -- I simply restarted back at the beginning of the alphabet.
3. MEET LATER; In this exercise, Caesar cipher was used to decrypt rather than encrypt, meaning that we shift the original letters of QIIX PEXIV to the left in the alphabet rather than to the right. Using 4 as the key for the first letter Q, for example, I shifted Q to the left four times: (1) P, (2) O, (3) N, and (4) M. I used the same method for the remaining letters and obtained the decrypted message of MEET LATER.

4. MEET HERE; In this exercise, Caesar cipher was used to decrypt rather than encrypt, meaning that we shift the original letters of SKKZ NKXK to the left in the alphabet rather than to the right. Using 6 as the key for the first letter S, I shifted it to the left six times: (1) R, (2) Q, (3) P, (4) O, (5) N, and (6) M. I used the same method for the remaining letters and got the decrypted message of MEET HERE.

Exercise 2

1. TNZKC VHGSX SKZKN AFHQJ FNOC; Using Vigenere cipher, I started with the second row, where each row has the letters shifted to the left one position in a cyclic way. To encrypt, I used the keyword letter and the plaintext letter as the row index and column index, respectively, and the entry at the row-column intersection is the letter in the ciphertext. For example, the first letter in the plaintext is F and its corresponding keyword letter is O. This means that the row of F and the column of O are used, and the entry T at the intersection is the encrypted result. With the second letter O, the row O and Z are used, as Z is the second letter of the keyword OZ, to get the letter N. The keyword OZ are then alternated for the remainder of the plaintext letters; ultimately, resulting in the encryption of TNZKC VHGSX SKZKN AFHQJ FNOC.
2. THERE IS NO PLACE LIKE HOME; Using Vignere cipher, I decrypted the message this time rather than encrypting it.

<https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html>

Exercise 3

1. When should I return; Using Caesar cypher, I decrypted this message with 7 as the key. I used trial and error as a means of producing a message that made sense. Using the plaintext PAXG LAHNEW B KXMNKG, I decrypted the original message by shifting the letters to the right. For the first letter, P, that means that I shifted it to the right seven times to get the letter W; for the second letter, A, I did the same and got the letter H; for the third letter, X, I did the same process and got the letter E. I followed the same exact process for the whole message to decrypt it.
2. Wait for a phone call; Using Caesar cypher, I decrypted this message with 6 as the key. I used trial and error as a means of producing a message that made sense. Using the plaintext QUCN ZIL U JBIHY WUFF, I decrypted the original message by shifting the letters to the right. For the first letter, Q, that means that I shifted it to the right six times to get the letter W; for the second letter, U, I did the same and got the letter A; for the third letter, C, I did the same process and got the letter I. I followed the same exact process for the whole message to decrypt it.
3. The rabbit crawled out of its hole; Using Caesar cypher, I decrypted this message with 13 as the key. I used trial and error as a means of producing a message that made sense. Using the plaintext GUR ENOOVG PENJYRQ BHG BS VGF UBYR, I decrypted the original message by shifting the letters to the right. For the first letter, G, that means that I shifted it to the right thirteen times to get the letter T; for the second letter, U, I did the same and got the letter H; for the third letter, R, I did the same process and got the letter E. I followed the same exact process for the whole message to decrypt it.

4. These aren't the droids you're looking for; Using Caesar cypher, I decrypted this message with 7 as the key. I used trial and error as a means of producing a message that made sense. Using the plaintext MAXLX TKXGM MAXWK HBWLR HNKXE HHDBG ZYHK, I decrypted the original message by shifting the letters to the right. For the first letter, M, that means that I shifted it to the right seven times to get the letter T; for the second letter, A, I did the same and got the letter H; for the third letter, X, I did the same process and got the letter S. I followed the same exact process for the whole message to decrypt it.

Exercise 4

1. Do or do not -- there is no try. Judge me by my size do you. Reckless is he. Now things are worse; Using Vigenere cipher with a length of 4 to decrypt the plaintext, I translated BCRNBCQORHKEEPSLSLCWRWXXDESPEZMPYQWCEBCBOSFHCIZHSQWVH CBRWRVLNEDRCKRRQS into this message.
2. 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; Using Vigenere cipher with a length of 4 as well to decrypt the plaintext, I translated and decrypted it to this message.

Exercise 5

1. 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 someone gently rapping, rapping at my chamber door. 'Tis some visitor, I

muttered, tapping at my door -- only this, and nothing more; Using both Caesar and Vigenere ciphering, I pulled together the translation and decryption of the plaintext.