Thanh Xuan Nguyen

IT\_120\_Module 5\_Lab\_4

September 23 2020

Exercise 1: Caesar Cipher

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

To do the encryption with Caesar cipher, the first to do is creating the ciphertext alphabet by shifting the alphabet to the left by number of places given by the key.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext Alphabet | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Ciphertext Alphabet | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d |

In this case, the key is 4, so we shift the alphabet 4 units to the left as below:

MATH has four characters. “M” is encrypted as “Q”, “A” is encrypted as “E”, “T” is encrypted as “X” and “H” is encrypted as “L”

So we have the encryption of the message MATH is QEXL.

Source: “Caesar Shift Cipher”. *Crypto Corner*. <https://crypto.interactive-maths.com/caesar-shift-cipher.html#encrypt>

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

To do the encryption with Caesar cipher, the first to do is creating the ciphertext alphabet by shifting the alphabet to the left by number of places given by the key.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext Alphabet | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Ciphertext Alphabet | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f |

In this case, the key is 6, so we shift the alphabet 6 units to the left as below:

CRYPTO has six characters. “C” is encrypted as “I”, “R” is encrypted as “X”, “Y” is encrypted as “E”, “P” is encrypted as “V”, “T” is encrypted as “Z” and “O” is encrypted as “U”

So we have the encryption of the message CRYPTO is IXEVZU.

Source: “Caesar Shift Cipher”. *Crypto Corner*. <https://crypto.interactive-maths.com/caesar-shift-cipher.html#encrypt>

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

To do the decryption with Caesar cipher, the first to do is creating the plaintext alphabet by shifting the ciphertext alphabet to the right by number of places given by the key.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ciphertext Alphabet | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Plaintext Alphabet | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v |

In this case, the key is 4, so we shift the alphabet 4 units to the right as below:

QIIX PEXIV has nine characters. “Q” is decrypted as “M”, “I” is decrypted as “E”, “X” is decrypted as “T”, “P” is decrypted as “L”, “E” is decrypted as “A” and “V” is decrypted as “R”

So we have the decryption of the message QIIX PEXIV is MEET LATER.

Source: “Caesar Shift Cipher”. *Crypto Corner*. <https://crypto.interactive-maths.com/caesar-shift-cipher.html#encrypt>

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

To do the decryption with Caesar cipher, the first to do is creating the plaintext alphabet by shifting the ciphertext alphabet to the right by number of places given by the key.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ciphertext Alphabet | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Plaintext Alphabet | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t |

In this case, the key is 6, so we shift the alphabet 6 units to the right as below:

SKKZ NKXK has nine characters. “S” is decrypted as “M”, “K” is decrypted as “E”, “Z” is decrypted as “T”, “N” is decrypted as “H” and “X” is decrypted as “R”

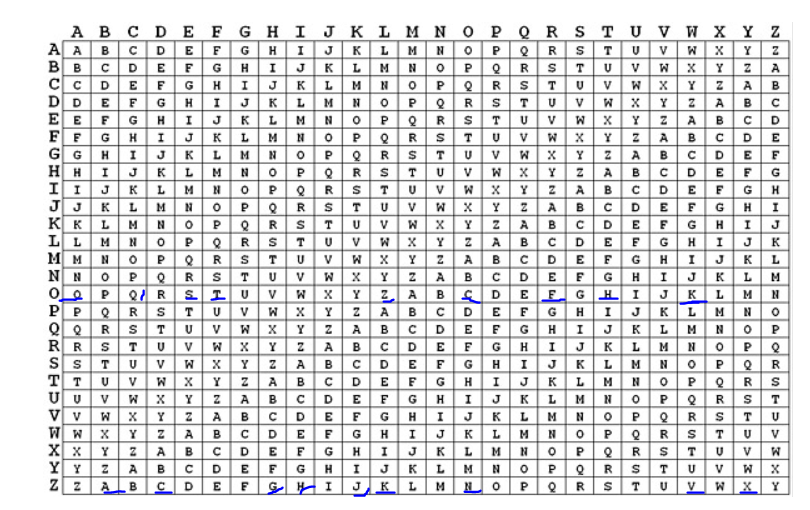
So we have the decryption of the message SKKZ NKXK is MEET HERE.

Source: “Caesar Shift Cipher”. *Crypto Corner*. <https://crypto.interactive-maths.com/caesar-shift-cipher.html#encrypt>

Exercise 2: Vignere cipher `

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

To do the encryption with vignere cipher, the first thing to do is creating the two-sided alphabet with column alphabet representing plaintext and row alphabet representing keyword.



We use every single letter of the words in the plaintext to tell us what column to look at the mapping while we use every single letter of the words in the keyword to tell us what row to look at mapping. The keyword is repeated after its last letter is pointed.

FOLLO WTHEY ELLOW BRICK ROAD: we divide this sentence into five sections

1) FOLLO: “F” is encrypted as “T”, “O” is encrypted as “N”, “L” is encrypted as “Z”, “L” is encrypted as “K”, “O” is encrypted as “C”. So, we have TNZKC.

2) WTHEY: “W” is encrypted as “V”, “T” is encrypted as “H”, “H” is encrypted as “G”, “E” is encrypted as “S”, “Y” is encrypted as “X”. So, we have VHGSX.

3) ELLOW: “E” is encrypted as “S”, “L” is encrypted as “K”, “L” is encrypted as “Z”, “O” is encrypted as “N”, “W” is encrypted as “K”. So, we have SKZNK.

4) BRICK: “B” is encrypted as “A”, “R” is encrypted as “F”, “I” is encrypted as “H”, “C” is encrypted as “Q”, “K” is encrypted as “J”. So, we have AFHQJ.

5) ROAD: “R” is encrypted as “F”, “O” is encrypted as “N”, “A” is encrypted as “O”, “D” is encrypted as “C”. So, we have FNOC.

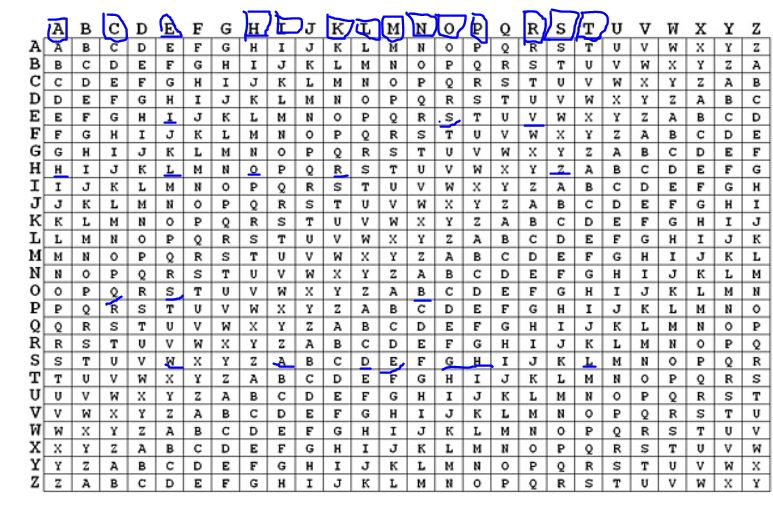
As a result, we have the encryption of FOLLO WTHEY ELLOW BRICK ROAD:

TNZKC VHGSX SKZNK AFHQJ FNOC.

Source: “Vignere Ciper”. *CRYPTO CORNER*. <https://crypto.interactive-maths.com/vigenegravere-cipher.html>

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

To do the decryption with vignere cipher, the first thing to do is creating the two-sided alphabet with column alphabet representing plaintext and row alphabet representing keyword.



we use every single letter of the words in the ciphertext to tell the position of the characters between columns and rows while we use every single letter of the words in the keyword to tell us what row to look at mapping. The keyword is repeated after its last letter is pointed.

LOSVW AZBSH DHQID ARSLG EL: we divide this code into five sections

1) LOSVW: “L” is decrypted as “T”, “O” is decrypted as “H”, “S” is decrypted as “E”, “V” is decrypted as “R”, “W” is encrypted as “E”. So, we have THERE.

2) AZBSH: “A” is decrypted as “I”, “Z” is decrypted as “S”, “B” is decrypted as “N”, “S” is decrypted as “O”, “H” is encrypted as “P”. So, we have IS NO P.

3) DHQID: “D” is decrypted as “L”, “H” is decrypted as “A”, “Q” is decrypted as “C”, “I” is decrypted as “E”, “D” is encrypted as “L”. So, we have LACE L.

4) ARSLG: “A” is decrypted as “I”, “R” is decrypted as “K”, “S” is decrypted as “E”, “L” is decrypted as “H”, “G” is encrypted as “O”. So, we have IKE HO.

5) EL: “E” is decrypted as “M”, “L” is decrypted as “E”. So, we have ME.

As a result, we have decryption of LOSVW AZBSH DHQID ARSLG EL:

THERE IS NO PLACE LIKE HOME.

Source: “Vignere Ciper”. *CRYPTO CORNER*. <https://crypto.interactive-maths.com/vigenegravere-cipher.html>

Exercise 3: Breaking the Caesar Cipher

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

Without knowing the shift keyword, we have 26 potential plaintext alphabets. I get the first four letters (PAXG) out and try them with every possible plaintext alphabet.

I have tried those alphabets (1-26) with the encrypted messages and found the most possible plaintext with 19 as the key. The alphabet is below:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ciphertext Alphabet | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Plaintext Alphabet | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g |

PAXG LAHNEW B KXMNKG has 17 characters. “P” is decrypted as “W”, “A” is decrypted as “H”, “X” is decrypted as “E”, “G” is decrypted as “N”, “L” is decrypted as “S”, “A” is decrypted as “H”, “H” is decrypted as “O”, “N” is decrypted as “U”, “E” is decrypted as “L”, “W” is decrypted as “D”, “B” is decrypted as “I”, “K” is decrypted as “R”, “X” is decrypted as “E”, “M” is decrypted as “T”, “N” is decrypted as “U”, “K” is decrypted as “R”, and “G” is decrypted as “N”, So we have the decryption of the message PAXG LAHNEW B KXMNKG is WHEN SHOULD I RETURN.

Source: “Caesar Shift Cipher”. *Crypto Corner*. <https://crypto.interactive-maths.com/caesar-shift-cipher.html#encrypt>

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

Without knowing the shift keyword, we have 26 potential plaintext alphabets. I get the first four letters (QUCN) out and try them with every possible plaintext alphabet.

I have tried those alphabets (1-26) with the encrypted message and found the most possible plaintext with 20 as the key. The alphabet is below:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ciphertext Alphabet | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Plaintext Alphabet | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f |

QUCN ZIL U JBIHY WUFF has 17 characters. “Q” is decrypted as “W”, “U” is decrypted as “A”, “C” is decrypted as “I”, “N” is decrypted as “T”, “Z” is decrypted as “F”, “I” is decrypted as “O”, “L” is decrypted as “R”, “U” is decrypted as “A”, “J” is decrypted as “P”, “B” is decrypted as “H”, “I” is decrypted as “O”, “H” is decrypted as “N”, “Y” is decrypted as “E”, “W” is decrypted as “C”, “U” is decrypted as “A”, “F” is decrypted as “L” and “F” is decrypted as “L”, So we have the decryption of the message QUCN ZIL U JBIHY WUFF is WAIT FOR A PHONE CALL.

Source: “Caesar Shift Cipher”. *Crypto Corner*. <https://crypto.interactive-maths.com/caesar-shift-cipher.html#encrypt>

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

Without knowing the shift keyword, we have 26 potential plaintext alphabets. I get the first four letters (GURE) out and try them with every possible plaintext alphabet.

I have tried those alphabets (1-26) with the encrypted message and found the most possible plaintext with 13 as the key. The alphabet is below:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ciphertext Alphabet | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Plaintext Alphabet | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m |

GUR ENOOVG PENJYRQ BHG BS VGF UBYR has 28 characters. “G” is decrypted as “T”, “U” is decrypted as “H”, “R” is decrypted as “E”, “E” is decrypted as “R”, “N” is decrypted as “A”, “O” is decrypted as “B”, “O” is decrypted as “B”, “V” is decrypted as “I”, “G” is decrypted as “T”, “P” is decrypted as “C”, “E” is decrypted as “R”, “N” is decrypted as “A”, “J” is decrypted as “W”, “Y” is decrypted as “L”, “R” is decrypted as “E”, “Q” is decrypted as “D”, and keep doing the decryption until the last character. So we have the decryption of the message GUR ENOOVG PENJYRQ BHG BS VGF UBYR is   
 THE RABBIT CRAWLED OUT OF ITS HOLE.

Source: “Caesar Shift Cipher”. *Crypto Corner*. <https://crypto.interactive-maths.com/caesar-shift-cipher.html#encrypt>

4. Decrypt the message encrypted with a Caesar cipher:

MAXLX TKXGM MAXWK HBWLR HNKXE HHDBG ZYHK Without knowing the shift keyword, we have 26 potential plaintext alphabets. I get the first four letters (MAXL) out and try them with every possible plaintext alphabet.

I have tried those alphabets (1-26) with the encrypted message and found the most possible plaintext with 19 as the key. The alphabet is below:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ciphertext Alphabet | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Plaintext Alphabet | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g |

MAXLX TKXGM MAXWK HBWLR HNKXE HHDBG ZYHK has 34 characters. “M” is decrypted as “T”, “A” is decrypted as “H”, “X” is decrypted as “E”, “L” is decrypted as “S”, “X” is decrypted as “E”, and keep doing the decryption until the last character. So we have the decryption of the message MAXLX TKXGM MAXWK HBWLR HNKXE HHDBG ZYHKis:

**these aren’t the droids you’re looking for.**

Source: “Caesar Shift Cipher”. *Crypto Corner*. <https://crypto.interactive-maths.com/caesar-shift-cipher.html#encrypt>

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.

To decrypt a message encrypted with a Vignere cipher without knowing the keyword, the popular way to do that is using the Kasiski test. However, we have already known the length of the code (4). So, our work will be less complex.

Since the keyword has 4 letters, it means that they are repeated after every four words are mapped. So, we divide the message into groups, one of which matches every letter of the keyword. Then find the letter has the most frequency in each group.

Next, I will find the Index of Coincidence (IC).

On the two-sided alphabet, the task is to find the row alphabet that can contain all the characters of every letter group above.

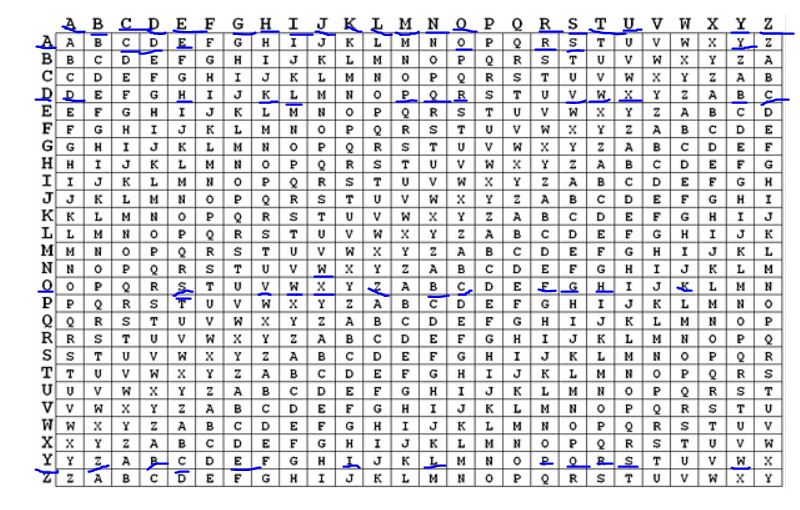
After many triads, I figure four letters could be part of the keyword.

Besides, I use an online software to find the possible keyword.

Knowing the length of Vigere cipher key, I figure out that the keyword is YODA.

Source: “Vigenere Solver”. *Guballa*. <https://www.guballa.de/vigenere-solver>

To do the decryption with vignere cipher, the first thing to do is creating the two-sided alphabet with column alphabet representing plaintext and row alphabet representing keyword. we use every single letter of the words in the ciphertext to tell the position of the characters between columns and rows while we use every single letter of the words in the keyword to tell us what row to look at mapping. The keyword is repeated after its last letter is pointed.



BCRR BCQO RHKE PSLS LCWR WXXD ESPE ZMPY QWCE BCBO SFHC IZHS QWVH CBRW RVLN EGDR CKRR QS.: we divide this code into 18 sections

1) BCRR: “B” is decrypted as “D”, “C” is decrypted as “O”, “R” is decrypted as “O”, “R” is decrypted as “R”. So, we have DO OR.

2) BCQO: “B” is decrypted as “D”, “C” is decrypted as “O”, “Q” is decrypted as “N”, “O” is decrypted as “O”. So, we have DONO.

3) RHKE: “R” is decrypted as “T”, “H” is decrypted as “T”, “K” is decrypted as “H”, “E” is decrypted as “E”. So, we have T THE.

4) PSLS: “P” is decrypted as “R”, “S” is decrypted as “E”, “L” is decrypted as “I”, “S” is decrypted as “S”. So, we have RE IS.

5) LCWR: “L” is decrypted as “N”, “C” is decrypted as “O”, “W” is decrypted as “T”, “R” is decrypted as “R”. So, we have NO TR.

6) WXXD: “W” is decrypted as “Y”, “X” is decrypted as “J”, “X” is decrypted as “U”, “D” is decrypted as “D”. So, we have Y JUD.

7) ESPE: “E” is decrypted as “G”, “S” is decrypted as “E”, “P” is decrypted as “M”, “E” is decrypted as “E”. So, we have GE ME.

8) ZMPY: “Z” is decrypted as “B”, “M” is decrypted as “Y”, “P” is decrypted as “M”, “Y” is decrypted as “Y”. So, we have BY MY.

9) QWCE: “Q” is decrypted as “S”, “W” is decrypted as “I”, “C” is decrypted as “Z”, “E” is decrypted as “E”. So, we have SIZE.

10) BCBO: “B” is decrypted as “D”, “C” is decrypted as “O”, “B” is decrypted as “Y”, “O” is decrypted as “O”. So, we have DO YO.

So far, we have DO OR DONOT. THERE IS NO TRY. JUDGE ME BY MY SIZE. DO YO.

Keep doing this step with the rest of code, we have:

DO OR DONOT. THERE IS NO TRY. JUDGE ME BY MY SIZE, DO YOU? RECKLESS IS HE. NOW THINGS ARE WORSE.

Source: “Vigenere Solver”. *Guballa*. <https://www.guballa.de/vigenere-solver>.

<https://en.wikipedia.org/wiki/Kasiski_examination>

“Vignere Ciper”. *CRYPTO CORNER*. <https://crypto.interactive-maths.com/vigenegravere-cipher.html>

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

To decrypt a message encrypted with a Vignere cipher without knowing the keyword, the popular way to do that is using the Kasiski test. However, we have already known the length of the code (4). So, our work will be less complex.

Since the keyword has 4 letters, it means that they are repeated after every four words are mapped. So, we divide the message into groups, one of which matches every letter of the keyword. Then find the letter has the most frequency in each group.

Next, I will find the Index of Coincidence (IC).

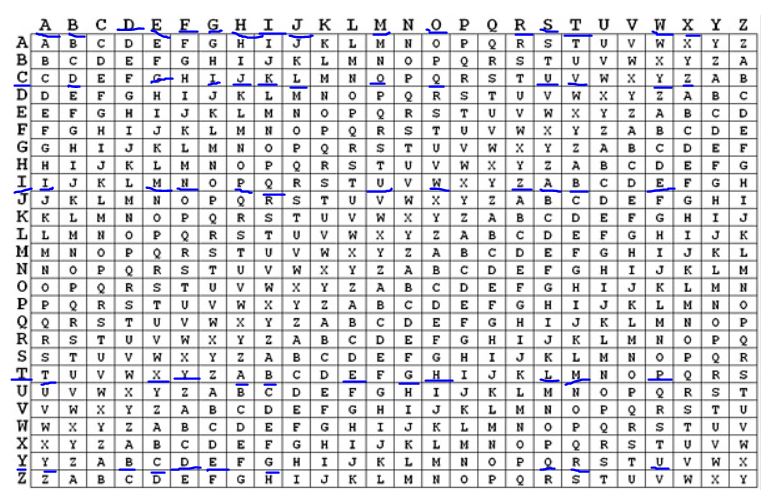
On the two-sided alphabet, the task is to find the row alphabet that can contain all the characters of every letter group above.

After many triads, I figure four letters could be part of the keyword.

Besides, I use an online software to find the possible keyword.

Knowing the length of Vigere cipher key, I figure out that the keyword is CITY

To do the decryption with vignere cipher, the first thing to do is creating the two-sided alphabet with column alphabet representing plaintext and row alphabet representing keyword. we use every single letter of the words in the ciphertext to tell the position of the characters between columns and rows while we use every single letter of the words in the keyword to tell us what row to look at mapping. The keyword is repeated after its last letter is pointed.



By groups of 5, we divide this code into 44 sections:

1) KBPYU: “K” is decrypted as “I”, “B” is decrypted as “T”, “P” is decrypted as “W”, “Y” is decrypted as “A”, “U” is decrypted as “S”. So, we have IT WAS.

2) BACDM: “B” is decrypted as “T”, “A” is decrypted as “H”, “C” is decrypted as “E”, “D” is decrypted as “B”, “M” is decrypted as “E”. So, we have THE BE.

3) LRQNM: “L” is decrypted as “S”, “R” is decrypted as “T”, “Q” is decrypted as “O”, “N” is decrypted as “F”, “M” is decrypted as “T”. So, we have ST OF T.

4) GOMLG: “G” is decrypted as “I”, “O” is decrypted as “M”, “M” is decrypted as “E”, “L” is decrypted as “S”, “G” is decrypted as “I”. So, we have IMES I.

5) VETQV: “V” is decrypted as “T”, “E” is decrypted as “W”, “T” is decrypted as “A”, “N” is decrypted as “S”, “M” is decrypted as “T”. So, we have T WAS T.

6) PXUQZ: “P” is decrypted as “H”, “X” is decrypted as “E”, “U” is decrypted as “W”, “Q” is decrypted as “O”, “Z” is decrypted as “R”. So, we have HE WOR.

7) LRZNM: “L” is decrypted as “S”, “R” is decrypted as “T”, “Z” is decrypted as “X”, “N” is decrypted as “F”, “M” is decrypted as “T”. So, we have ST XF T.

8) GOMLG: “G” is decrypted as “I”, “O” is decrypted as “M”, “M” is decrypted as “E”, “L” is decrypted as “S”, “G” is decrypted as “I”. So, we have IMES I.

9) VETQV: “G” is decrypted as “T”, “O” is decrypted as “W”, “M” is decrypted as “A”, “L” is decrypted as “S”, “G” is decrypted as “T”. So, we have T WAS T.

10) PXYIM: “P” is decrypted as “H”, “X” is decrypted as “E”, “Y” is decrypted as “A”, “I” is decrypted as “G”, “M” is decrypted as “E”. So, we have HE AGE.

11) HDYQL: “H” is decrypted as “O”, “D” is decrypted as “F”, “Y” is decrypted as “W”, “Q” is decrypted as “I”, “L” is decrypted as “S”. So, we have OF WIS.

12) BQUBR: “B” is decrypted as “D”, “Q” is decrypted as “O”, “U” is decrypted as “M”, “B” is decrypted as “I”, “R” is decrypted as “T”. So, we have DOM IT.

13) YILRJ: “Y” is decrypted as “W”, “I” is decrypted as “A”, “L” is decrypted as “S”, “R” is decrypted as “T”, “J” is decrypted as “H”. So, we have WAS TH.

14)MTEGW: “M” is decrypted as “E”, “T” is decrypted as “A”, “E” is decrypted as “G”, “G” is decrypted as “E”, “W” is decrypted as “O”. So, we have E AGE O.

15) YDQWE: “Y” is decrypted as “F”, “D” is decrypted as “F”, “Q” is decrypted as “O”, “W” is decrypted as “O”, “E” is decrypted as “L”. So, we have F FOOL.

16) GUPGC: “G” is decrypted as “I”, “U” is decrypted as “S”, “P” is decrypted as “H”, “G” is decrypted as “N”, “C” is decrypted as “E”. So, we have ISHNE.

17) UABRY: “U” is decrypted as “S”, “A” is decrypted as “S”, “B” is decrypted as “I”, “R” is decrypted as “T”, “Y” is decrypted as “W”. So, we have SS IT W.

18) ILRJM: “I” is decrypted as “A”, “L” is decrypted as “S”, “R” is decrypted as “T”, “J” is decrypted as “H”, “M” is decrypted as “E”. So, we have AS THE.

So far, we have: IT WAS THE BEST OF TIMES, IT WAS THE WORST XF TIMES. IT WAS THE AGE OF WISDOM. IT WAS THE AGE OF FOOLISHNESS. IT WAS THE.

Keep doing this step with the rest of the code, we have:

IT WAS THE BEST OF TIMES. IT WAS THE WORST XF 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.

Source: “Vigenere Solver”. *Guballa*. <https://www.guballa.de/vigenere-solver>.

“Vignere Ciper”. *CRYPTO CORNER*. <https://crypto.interactive-maths.com/vigenegravere-cipher.html>

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 Without knowing the shift keyword, we have 26 potential plaintext alphabets.

I have tried those alphabets with the keys (1-26) and found the most possible plaintext with 23 as the key. The alphabet is below:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ciphertext Alphabet | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Plaintext Alphabet | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c |

We divide the following message into groups as shown in the original word spacing:

1) LKZB: “L” is decrypted as “O”, “K” is decrypted as “N”, “Z” is decrypted as “C”, “B” is decrypted “E”. So, we have ONCE.

2) RMLK: “R” is decrypted as “U”, “M” is decrypted as “P”, “L” is decrypted as “O”, “K” is decrypted “N”. So, we have UPON.

3) X: “X” is decrypted as “A”

4) JFAKFDEQ: “J” is decrypted as “M”, “F” is decrypted as “I”, “A” is decrypted as “D”, “K” is decrypted “N”, “F” is decrypted as “I”, “D” is decrypted as “G”, “E” is decrypted as “H”, “Q” is decrypted “T”. So, we have MIDNIGHT.

5) AOBXOV: “A” is decrypted as “D”, “O” is decrypted as “R”, “B” is decrypted as “E”, “X” is decrypted “A”, “O” is decrypted as “R”, “V” is decrypted as “Y”. So, we have DREARY.

6) TEFIB: “T” is decrypted as “W”, “E” is decrypted as “H”, “F” is decrypted as “I”, “I” is decrypted as “L”, “B” is decrypted “E”. So, we have WHILE.

7) F: “F” is decrypted as “I”.

8) MLKABOBA: “M” is decrypted as “P”, “L” is decrypted as “O”, “K” is decrypted as “N”, “A” is decrypted “D”, “B” is decrypted as “E”, “O” is decrypted as “R”, “B” is decrypted as “E”, “A” is decrypted “D”. So, we have PONDERED.

9) TBXH: “T” is decrypted as “W”, “B” is decrypted as “E”, “X” is decrypted as “A”, “H” is decrypted “K”. So, we have WEAK.

10) XKA: “X” is decrypted as “A”, “K” is decrypted as “N”, “A” is decrypted as “D”. So, we have AND.

11) TBXOV: “T” is decrypted as “W”, “B” is decrypted as “E”, “X” is decrypted as “A”, “O” is decrypted “R”, “V” is decrypted as “Y”. So, we have WEARY.

12) LSBO: “L” is decrypted as “O”, “S” is decrypted as “V”, “B” is decrypted as “E”, “O” is decrypted “R”. So, we have OVER.

13) JXKV: “J” is decrypted as “M”, “X” is decrypted as “A”, “K” is decrypted as “N”, “V” is decrypted “Y”. So, we have MANY.

14) X: “X” is decrypted as “A”.

15) NRXFKQ: “N” is decrypted as “Q”, “R” is decrypted as “U”, “X” is decrypted as “A”, “F” is decrypted “I”, “K” is decrypted as “N”, “Q” is decrypted as “T”. So, we have QUAINT.

16) XKA: “X” is decrypted as “A”, “K” is decrypted as “N”, “A” is decrypted as “D”. So, we have AND.

17) ZROFLRP: “Z” is decrypted as “C”, “R” is decrypted as “U”, “O” is decrypted as “R”, “F” is decrypted “I”, “L” is decrypted as “O”, “R” is decrypted as “U”, “P” is encrypted as “S”. So, we have CURIOUS.

The first line is ONCE UPON A MIDNIGHT DREARY, WHILE I PONDERED, WEAK AND WEARY, OVER MANY A QUIANT AND CURIOUS.

Keep doing this step with the rest of following message. As a result, we have:

ONCE UPON A MIDNIGHT DREARY, WHILE I PONDERED, WEAK AND WEARY, OVER MANY A QUIANT 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.

Source: “Caesar Shift Cipher”. *Crypto Corner*. <https://crypto.interactive-maths.com/caesar-shift-cipher.html#encrypt>