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

Used Crypto Club’s Caesar Cipher tool, set the key to 4, put in the plain text “MATH” hit encrypt and quick answer

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

IXEVZU

Used Crypto Club’s Caesar Cipher tool, set the key to 6, put in the plain text “CRYPTO” hit encrypt and quick answer

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

meet later

Used Crypto Club’s Caesar Cipher tool, set the key to 4, put in the plain text “QIIZ PEXIV” hit decrypt and quick answer

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

meet here

E is the most common letter in English, so I figured K in the cipher text was most likely E, and it takes 6 shifts to get from E to K so I put it in the Caesar Cipher tool on Crypto Club with a key of 6, hit decrypt and quick answer

Exercise 2: Vignere cipher `

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

TNZKC VHGSX SKZNK AFHQJ FNOC

Used Crypto Club’s Vignere cipher tool and replaced the letters corresponding with O with the letters matched with them on the cipher wheel with O as the key and then did the same thing with letters corresponding to Z with Z as the key

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

there isnop lacel ikeho me (there is no place like home)

Used Crypto Club’s Vignere cipher tool and replaced the letters corresponding with S with the letters matched with them on the cipher wheel with S as the key and then did the same thing with the rest of the letters in SHOES

Exercise 3: Breaking the Caesar Cipher

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

when should I return

I first assumed that B was A as A is the most common single letter word in English, so I tried first by decrypting the message with a shift of 1, that gave me gibberish so then I tried if B were I which gave me a shift of 19 so I put it in the Caesar Cipher tool on Crypto Club with a key of 19, hit decrypt and quick answer

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

wait for a phone call

I assumed U was a giving me a shift of 20 so I put it in the Caesar Cipher tool on Crypto Club with a key of 20, hit decrypt and quick answer

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

the rabbit crawled out of its hole

The most common three letter word in English is “the” and to turn ‘t’ into ‘g’ you shift 13 so I put it in the Caesar Cipher tool on Crypto Club with a key of 13, hit decrypt and quick answer

4. Decrypt the message encrypted with a Caesar cipher:

MAXLX TKXGM MAXWK HBWLR HNKXE HHDBG ZYHKthese arent thedr oidsy ourel ookin for (these arent the droids youre looking for)

E is the most common letter in English, so I figured X in the cipher text might be E in plaintext, and it takes 19 shifts to get from E to X so I put it in the Caesar Cipher tool on Crypto Club with a key of 19, hit decrypt and quick answer

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

I used <https://www.dcode.fr/vigenere-cipher> and put the ciphertext in the decoder, selected the decryption method of knowing the key-length/size and input 4 as the number of letters

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 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 IN CREDULITY IT WAS THE SEASON OF LIGHT IT WAS THE SEASON OF DARKNESS IT WAS THE SPRING OF HOPE IT WAS THE WINTER OF DESPAIR |

I used <https://www.dcode.fr/vigenere-cipher> and put the ciphertext in the decoder, selected the decryption method of knowing the key-length/size and input 4 as the number of letters

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 JLOBonce upon a midnight dreary while i pondered weak and weary over many a quaintand curious volume of forgotten lore while i nodded nearly napping suddenlythere came a tapping as of some one gently rapping rapping at my chamberdoor t is some visiter i muttered tapping at my chamber door only this and nothing more

I first assumed that X was A as A is the most common single letter word in English, so I tried first by decrypting the message with a shift of 23 using Crypto Club’s Caesar cipher tool