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**

**In the alphabetical letters, I counted letter B as 1 and E as 4 and went along till Z.**

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

**IXEVZU**

**In the alphabetical letters, I counted letter B as 1 and G as 6 and went along till Z.**

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

**MEET LATER**

**When we count A through Q; Q=22. Decrypt with 4 as a key=22-4=18. Counting A through M, M=18. Therefore, Q=M. When it ends on Z, keep going repeating A again and assign the value accordingly.**

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

**MEET HERE**

**Just for the try, I used the website** [**https://www.xarg.org/tools/caesar-cipher/**](https://www.xarg.org/tools/caesar-cipher/) **mentioned in the Cyber\_Princip\_5-Cryptography.pptx. I used the key guess.**

Exercise 2: Vignere cipher `

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

**TNZKC VHGSX SKZNK AFHQJ FNOC**

**Counting A= 0 to Z=25, O=14. O Z=2 digits. TO ENCRYPT ADD 3. Which is 14+2+3=19. In normal alphbetical order, 19=T. Thus, F is encrypted as T.**

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

**THERE IS NO PLACE LIKE HOME**

**Counting A= 0 to Z=25, L=11. SHOES**=**5 digits. TO ENCRYPT ADD 3. Which is 11+5+3=19. In normal alphbetical order, 19=T. Thus, L is encrypted as T.**

Exercise 3: Breaking the Caesar Cipher

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

**WHEN SHOULD I RETURN?**

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

**WAIT FOR A PHONE CALL!**

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

**THE RABBIT CRAWLED OUT OF ITS HOLE.**

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.**

**THIS EXERCISE WAS HARD TO UNDERSTAND; USED THIS WEBSITE FOR SOLUTION:** [**https://www.dcode.fr/caesar-cipher**](https://www.dcode.fr/caesar-cipher)

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?**

**Here, Assuming A=0 to Z=25, B=1. Ecrypting a Vignere cipher of length 4, 4-1=3, which is 3=D. Therefore, B is decrypted as D.**

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 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.**

Same process applies as 1.

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

**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-TIS SOME VISITER I MUTTERED TAPPING AT MY CHAMBER DOOR, ONLY THIS AND NOTHING MORE.**

**COUNTING A=0 TO Z=25, L=11. ADD 3 TO 11= 14. 14= O. ETC.**