Homework #1

Due date: **27/10/2023**
Notes:

- Your work (code + written answers) must be submitted through SUcourse+.
- Winzip your programs and add a readme.txt document (**if necessary**) to explain the programs and how to use them.
- Name your winzip file as **"cs411_507_hw01_yourname.zip"**

1. (**15 pts**) Consider the shift cipher. Show that the ciphertext "NLPDLC" can be decrypted into a meaningful word. Find out this word and the corresponding encryption key.

2. (**20 pts**) Consider the ciphertext generated by Affine Cipher over $Z_{26.}$ As a hint, you are told that the most frequent letter in the plaintext is 'T'. Find the plaintext, the encryption and decryption keys. Show your work.

"J gjg mxa czjq ayr arpa. J ulpa cxlmg ayerr ylmgerg rqrwrm hzdp ax gx ja hexmn."

3. **(15 pts)** Assume that you design a new affine cipher where you encrypt two letters at a time, where your alphabet is

{'A':0, 'B':1, 'C':2, 'D':3, 'E':4, 'F':5, 'G':6, 'H':7, 'I':8, 'J':9, 'K':10, 'L':11, 'M':12, 'N':13, 'O':14, 'P':15, 'Q':16, 'R':17, 'S':18, 'T':19, 'U':20, 'V':21, 'W':22, 'X':23, 'Y':24, 'Z':25, '.':26, ' ':27, ',':28, '!':29}.

In other words, you group your plaintext message in bigrams (i.e., two-character words) and encrypt each bigram of the plaintext separately using this affine cipher. For example, if the first two letters of a plaintext is "TH" then it will be encoded as follows

TH $\Rightarrow$ $19 \times 30 + 7 = 577$.

If the number of letters in the plaintext is not a multiple of two, you pad it with the letter "X" at the end. Determine the modulus and the size of the key space.

4. (**15 pts**) Is the affine cipher defined in question (3) secure against the letter frequency analysis?

5. **(20 pts**) Consider the following ciphertext that is encrypted with the affine cipher defined in question (3):

   "ZHOFC.BNZCLRZ WNJ.XGI.WMBDV.MEJ!GGYKGDZ ERGMWNJ.KDGD RSW"

   Find the key and decrypt the ciphertext.

   (**Hint 1:** The plaintext is a sentence that ends with a dot.)
   (**Hint 2:** The length of the plaintext (plen) is not a multiple of 2; plen = 2k+1 for an integer k.)

6. **(15 pts)** If we select a different shift amount for every letter in the plaintext uniformly randomly, the shift cipher becomes a one-time-pad with perfect security. Suppose p_α is the probability of the plaintext letter α from the Turkish alphabet, where $\alpha \in$ {A, B, C, Ç, …, Z}. Suppose also that p_β is the probability of the ciphertext letter β, where $\beta \in$ {A, B, C, Ç, …, Z}. Demonstrate that $p_\beta = 1/29$ for every $\beta \in$ {A, B, C, Ç, …, Z} independent of the values of p_α.

7. **BONUS (20 pts)** The following was encrypted using the Vigènere cipher:

   “FNZ FFZZMLQQZVO GAXXH PZ UPU QXGIHU UY NWJXR AHBDLPOMK YOUPZM, VOZAYCD. J TGQH B XUIJJZM ARS XOAH, BZJ D JP AT GLWUTB LO EVDWF AL GRHUI. OKPGMC L NME IRU NKGLFHK DQ UTK JUEQX JI UTK PQJHKMVF, KKO L MABZ WIQ YOLDWE GLUFRZ OFMBZV BE ZCHZ AVZQ JZ YKUJZM. D OPHK OKF NRPH TWE, D OPHK NRNQ VZRQXK, RKPY UIH MABZV ZAA FQPI YJPFFOHHT IOOKPGZ FQPIOIJ XTE. D OPHK NRNQ MMHBF JZHEE JJQF NE HHO, FNJXHT O’QH MATB FFMYZG QQXCDQE ZJ KBHK ADJFN DQ UTKH, BFF LMRN ARY KBNOO ROQ’Y CHBDZ KUJLKN WIQS. CHSQ ZCHZ TGQH CDUPJIF ZCH TAAK IPD EJX, FMZ DW, JF CDOM PU TRV SUJG. JF’Y ALSEZ-MDUQ YJXQ, FNZB LZUR KPI ZJ PBWK DW IQXZ. L XMTO WP FXVYFX OI HVDUKH, BXEJVIM, O NKBXR NHU ALA ISAS CHSQ. GIG ZQZ D NOAC OKBF O VP PZRT JPUTB WP M MMDWQEVUE, NAO LU’E G HRTF VMHDUUPV HDGQHZMXY, WIMZ’N ZIMZ DW JE. VMHDUUPV BDK OKF PKVG UTGO OJQ ZCHSQ, KQHSK YOROQ UQHS FNZP TBKVNT AL NXDT HPUOUTB OJRK DQ UTK KDTF, UA VVON KDTEOJQBFK ADJFN DQ UTKDU XAXF, WIQOM WSGZC, WIQOM VUDABJMQ GIG UTKDU TOOZQDQ, ZCDU

U QIRX U YCDMX LVOM AT OKF SXJXOP GIG LUYN WIAYZ VUATZV BZJ RHFB UQHS FNZP; UTUPJI U'S XROHOIFFP OI PZ TKVUU FNVW JF'Y GROS HZHO ZUOKJZM WXU M MMDWQEVUE. MTY L TTGGO OAZ RHFB LMRN PKNSBUX, WXU EOHSMK HZFBGYZ L TTGGO CQ NVSQK OI PZ FKVUT, U YCDMX YOHFB ST VPGR DQ FYUOLPZ. O GRWQ ZCH TFOXNZ XKVYFE OI VQDOIJ, UTK WOVQ YFB - UTGO'V BXR DW JE. OO'V OAZ V PBFZZU PR OIWFXRZFU AX GRHUI, DW'T XUQLOS CDWI ATZ'V JZYDGF, IOOK PZK'N VUASVFI."

Attack it and find the key length and the key. Note that only the letter characters are encrypted.