Homework #1

Due date: **22/10/2021**
Notes:

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

1. (**10 pts**) Consider the shift cipher. Show that the ciphertext "NKWZ" can be decrypted into two meaningful English words. Find out those words and corresponding encryption keys.

2. (**15 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 'A'. Find the plaintext, the encryption and decryption keys. Show your work.

"REZANSZ JRE VRDB CLXGNOZ. NEMZ R TOBRG VRE JRE HOLGB LG."

3. **(15 pts)** Consider an affine cipher for the Turkish language, where alphabet and some punctuation marks can be encoded as follows:

{'A':0, 'B':1, 'C':2, 'Ç':3, 'D':4, 'E':5, 'F':6, 'G':7, 'Ğ':8, 'H':9, 'I':10, 'İ': 11, 'J':12, 'K':13, 'L':14, 'M':15, 'N':16, 'O':17, 'Ö':18, 'P':19, 'R':20, 'S':21, 'Ş':22, 'T':23, 'U':24, 'Ü':25, 'V':26, 'Y':27, 'Z':28, '.':29, ',':30}

Use the Python code "affine_client.py" given in the assignment package to communicate with the server 'cryptlygos.pythonanywhere.com/'. The server will send you a ciphertext and the most frequent letter in the corresponding plaintext. You are expected to complete the Python code ("affine_client.py"), which should decrypt the ciphertext and send it back to the server with your student number.

4. **(10 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, where $\alpha \in \{A, B, \ldots, Z\}$. Suppose also that p_β is the probability of the ciphertext letter β, where $\beta \in \{A, B, \ldots, Z\}$. Demonstrate that $p_\beta = 1/26$ for every $\beta \in \{A, B, \ldots, Z\}$ independent of the values of p_α.

5. (**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}

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 19x28 + 7 = 539.

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.

6. (**15 pts**) Is the affine cipher defined in question (5) secure against the letter frequency analysis?

7. **(20 pts)** Consider the following ciphertext that is encrypted with the affine cipher defined in question (5):

"RYHUHBCMNHLMHHUYWMNXDIXMR.HUGB RCMD.HMZHOTJYUYWMZJOBBE"

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)

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

"Iur tvlrc ig vnc wof il tvps aoiutpy wu wfiqo ajl aln yrs jrcahld cqihl-rhsye gs cue fuahn gngairuhpol tvht kayls y pobpcr hoe cqihl mf o Yoaksmejlsy, tfe gaunir tal tvl eouos od ab Lilshlil, abk tfe wnnmrout kab ahc eebaj ot hnw ccslcgs wrcswkelt. Hoar ibztgtiaimn, ulnrlstel, ig h cmufa. Ir cou bc tvl Sspflmc Ccbrr ot ahc Ubptcd Saareg vr rhs oukbzlsr J.D josrh pn rhs sald, cy tfig oolofhbje qvupt koiah mvu qefce. Muf josrhz hyvs ahcif maslhz, aq dcls ynm oukab pnqtwauricu, bst wu tfig josnhyy muf josrhz ape hoe ersht jejllcrg, hnb ib vup ccbrrs osl keb hrc cflarer lqsaz.

P'm lo wkeylwzt ro pllgejl fgrasy gn hoe gnhlgpihf od oiy cmufas ynr pn rhs qupy-gfsrea ahyt wz nm irlaj tc te, gt wz a jijpne, wcykgnu yeylway. Eebalcmsu, a aoiyt gs bv bcthlr rhou eycv tal ot fos swatgnu iedofl mc ob ahgs xbrw. A qvupt wz ollm hs qoiud ys was huff, ald o qupy wz ollm hs qoiud ys hoe keb dhm more gt iw. I ym qvndirlnr tvht woi neltzlmcn kplj rscicw kptfoia pysgpol tvl etirlnae mvu fajl hcafk, cmms ao y dsjiqicu, ald flsrofl tfig kedebkalt hv hgs thmglm. Pn rhs uake cm Gmd, rv ymuf kury."

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