## Homework #1

Due date: 12/10/2019

**Notes:**

- Your answers and any other soft material such as Python codes must be zipped and submitted through SUCourse.
- Name your winzip file as "cs411_507_hw01_yourname.zip"
- You must show your work to explain how you obtained the result. Otherwise, you will get no credit.

1. (**20 pts**) Consider the shift cipher. Show that the ciphertext "NZWO" can be decrypted into two meaningful English words. Find out those words and the corresponding encryption keys.

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 "A". Find the plaintext and the encryption keys. Show your work.

   "H fzbbvffsza xhu jf ruv tmr bhu ahn h sjix srzuyhcjru tjcm cmv eijbdf rcmvif mhwv cmirtu hc mjx."

3. (**20 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, '?':30}.

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

4. (**20 pts**) Consider the following ciphertext that is encrypted with the affine cipher defined in question (3):

   "? RCYYP FYYK?VISYY?.J,HGQL?. ,HU!O,HXVBKMBRY??EPYT"

   Find the key and decrypt by exhaustive search it.

5. (**20 pts**) Decrypt the following plaintext using Vigènere cipher where the secret key is "SANITY":

"A RRNNQW TB IGQOEE BAYL QHMLRAOA WG RZE TZHSFDF BAYL I QWG'R CNBE MFW AAAPCJ. "s

Note that only the letter characters are encrypted.

**BONUS QUESTION**
**==========**

**6.** (**20 pts**) The following was encrypted using the Vigènere cipher:

"Gsoom onyos ppwro lra Q lgsyk E sfng.
Sio pgtcp io qf srp vetdzqp, tdwmfr;
Se sqdk xzt omw lo dtkxhhxr hazw
Sy hapkz gsd wkwvr ptlh ch vseh ovgv.
Wj leblko sonaw ledt ppamu tt mcwdb
Eo obgo gttdwms k qanuznede jmsq
Lptsmwm dse swgcc lnz njnjpn hicd
Dse zijjodt adwmsyg kn lgo jewz.

Zd qtvaa zhc sanvwrc mehtk z csagm
Ln kdk en lgoce ea knwp mealzup.
Tdm gmvj oppwq czujl'k srp ssmwo
Yq ewaq vsyd wvv cyhnu ndzup.
Tdm onyos wzw kygehg, vzbv ajl vdoa,
Bqb A gkge lzglsdeo bg jopp,
Wvv lsweo bg fy mebwjd S dlamh,
Zxo metwr dz gk jweyce E addoa."

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