## Homework #1

Due date: 1/11/2020

**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.
- In the package is the file "hw01_helper.py", which may be useful for certain operations needed in the homework.

1. (**10 pts**) Consider the shift cipher. Show that the ciphertext "NYVVC" 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 'T'. Find the plaintext, the encryption and decryption keys. Show your work.

   "Xpjjbxx lx eng klerm, krlmpob lx eng krgrm: lg lx gcb jnportb gn jneglepb gcrg jnpegx."

3. (**20 pts**) Consider an affine cipher for the Turkish language, where alphabet 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}

   Use the Python code "**affine_client.py**" given in the assignment package to communicate with the server **'http://10.36.52.109:5000**'. 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**) Assume that you design a new affine cipher, where you encrypt three 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 trigrams (i.e., three-character words) and encrypt each trigram of the plaintext separately using this affine cipher. For example, if the first three letters of a plaintext is “THE” then it will be encoded as follows

THE → 19×31×31 + 7×31 + 4 = 18480.

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

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

"IDSEOYLTVVDO?PSAUEKZO?LQIILQMP?LQNP!YSFNGSDBJZRZYTZTPS?EVYF,?LQ ,SAXSWTFXFD"

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 3; plen = 3k+1 for an integer k)

6. (**20 pts**) The following ciphertext is encrypted using Vigènere cipher:

"JYPR LTAXTNM, SOGELBCONN IL TNY ZER TU VGIELOUCCX, EXEPY LABUH"

It is a message from me to you. Can you decrypt it?

Note that only the letter characters are encrypted.

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

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

"Fwg atax: P’tx oh li hvabawl jwgvmjs, nw fw tfiapqz lziym,
rqgv uuwfpxj wpbk jxlnlz fptf noqe wgw.
Qoifmowl P bdg mg xv qe ntlyk ba bnjh vcf ekghn
izl fq blidb eayz jgzbwx sqwm lgglbtqgy xlip.
Pho fvvs ktf C smf ur ecul ywndxlz uv mzcz xxivw?
Qomdmowl P bgzg, oblzqdxj C swas,
B kyl btm udujs dcbfm vn yg eazl, pqzx,
oblzq Q’ow mwmzb lg ghvk gxslz, emamwx apqu, wwmazagxv nomy bhlustk.”

Ghm qvv’f nbfx h vqe vgoubdg, pgh’a nuvw shvbtmk kbvzq.
Baam jqfg pafs ixetqm wcdanw svc.
Kwn’df dixs mzy ziym llllmfa, zjid wxl
bf nom eifw hlqspuglowall, loyv sztq cu btmlw mhuq phmmla.
Kwn’df htiirk yul gx bf noqe kbls. Kwz’b agjl naz mzcuoe mekydpqzx:
lblzq’a gg moqb nhj svc, fpxjy’z va zhsx.
Uwi basn fwg’dx ouzbql rgoy tunx zyym, uv mzcz ayied wvzzmk,
qib’dq lxknywkmw an ldqzroblzq qg lbl eazev."

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