Homework #1

Due date: 06/10/2017
Notes:

- Computer programs and other soft material 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. (**15 pts**) Consider the shift cipher. Show that the ciphertext "XJGY" can be decrypted into two meaningful English words. Find out those words and corresponding encryption keys.

2. (**10 pts**) If we select a different shift amount for every letter in the plaintext at 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, …, Z}. Suppose also that p_β is the probability of the ciphertext letter β, where $\beta \in$ {A, B, …, Z}. Demonstrate that $p_\beta = 1/26$ for every $\beta \in$ {A, B, …, Z} independent of the values of p_α.

3. (**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 O. Find the plaintext and the encryption keys. Show your work.

   "HR JNAF ERRBH HR STYYSD YTJD"

4. (**20 pts**) Assume that you design a new affine cipher where you encrypt three letters at a time. In other words, you group your plaintext message in trigrams (three-letter words) and encrypt each trigram of the plaintext separately using this affine cipher. If the number of letters in the plaintext is not multiple of three, you pad it with the letter "X". Determine the modulus and the size of the key space.

5. (**10 pts**) Is the affine cipher defined in question (4) secure against the letter frequency analysis?

6. (**10 pts**) Decrypt the following plaintext using Vigenere cipher where the secret key is "SESAME":

   "WZWR FVAIV EHIJ JSIXIV RG MMXLIJ TDC SKSIZ JSMD ASEAR XAUP TILTQV"

   Note that space characters are not encrypted.

7. (**20 pts**) The following was encrypted using the Vigenere method:

"OPAKM IGWPK BTWAQ SZQ A BTAVW A SZGE.
TAA TGCEW QE AV FZM HATXSOQ, LPAMOT;
ZM IATX FWF KMQ EM ELWBHQZY PQJM
FG EMLKT ZQE OWAVA RATX MX IABT KVAO.

UK DQFLTQ ZWDKM YMAF LPUFS UL YGWMD
LW ELWB OQFZWGL I RSZYZWGKM ZWID
TMFOMQF BTW EAGLE SVP XZARMZ DIWW
BTW LMJSQKB QNMZAVS GN FZM KWID.

ZM SADQK PUK PMJVQKA NWTXK I EZIWW
BA SAW AN FZMDW QE KWYW UUKBMCM.
FZM AFTK GBTWZ EGCZV'A FZM EOMQH
WR WIEQ EUFL MFL PGEZQ NXSSQ.

LPQ OWAVA MJM XGDQDG, PSZW SVP VMQH,
JGL Q TSDQ HZAEQEWA FG SQWX,
MFL YATQK BA YW NWNAJM U KTQWX,
MFL YATQK BA YW NWNAJM U KTQWX."

Attack it and find the key length and the key. Note that the punctuation marks and space characters are not encrypted.