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.

   COLD → XJGY (key = 21)
   FROG → XJGY (key = 18)

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 $\alpha \in \{A, B, \ldots, Z\}$. 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.

Assume that the ciphertext letter β encodes to $i \in \{0,1, \ldots, 25\}$. There are 26 different combinations of the shift amount and plaintext letter that will encrypts to β:

$$j + k \equiv i \bmod 26$$

where j encodes the plaintext letter and j = 0, 1, …, 25. Then p_β can be written as

$$p_\beta = (1/26)p_A + (1/26)p_B + \ldots + (1/26)p_Z = (1/26)(p_A + p_B + \ldots + p_Z) = 1/26$$

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"

   encryption key: (11, 19)

   the plaintext:
   "SO MANY BOOKS SO LITTLE TIME"

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.

Theoretically the number of bigrams are 26×26×26 = 17576
Then the modulus is 17576.
The size of the key space: $\phi(17576) \times 17576 = 8112 \times 17576 = 142576512$

5. (**10 pts**) Is the affine cipher defined in question (3) secure against the letter frequency analysis?

It is better than the original affine cipher. However, the language statistics is not totally removed. Note the following trigram frequencies of the English language.

THE : 1.81	ERE : 0.31	HES : 0.24
AND : 0.73	TIO : 0.31	VER : 0.24
ING : 0.72	TER : 0.30	HIS : 0.24
ENT : 0.42	EST : 0.28	OFT : 0.22
ION : 0.42	ERS : 0.28	ITH : 0.21
HER : 0.36	ATI : 0.26	FTH : 0.21
FOR : 0.34	HAT : 0.26	STH : 0.21
THA : 0.33	ATE : 0.25	OTH : 0.21
NTH : 0.33	ALL : 0.25	RES : 0.21
INT : 0.32	ETH : 0.24	ONT : 0.20

Check also the following link:
http://practicalcryptography.com/cryptanalysis/letter-frequencies-various-languages/english-letter-frequencies/

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.

"EVER TRIED EVER FAILED NO MATTER TRY AGAIN FAIL AGAIN FAIL BETTER"

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.

Key length is 6 and key vector is {18, 8, 12, 18, 8, 12}; i.e. SIMSIM. The ciphertext decrypts to following text:

“WHOSE WOODS THESE ARE I THINK I KNOW.
HIS HOUSE IS IN THE VILLAGE, THOUGH;
HE WILL NOT SEE ME STOPPING HERE
TO WATCH HIS WOODS FILL UP WITH SNOW.

MY LITTLE HORSE MUST THINK IT QUEER
TO STOP WITHOUT A FARMHOUSE NEAR
BETWEEN THE WOODS AND FROZEN LAKE
THE DARKEST EVENING OF THE YEAR.

HE GIVES HIS HARNESS BELLS A SHAKE
TO ASK IF THERE IS SOME MISTAKE.
THE ONLY OTHER SOUND'S THE SWEEP
OF EASY WIND AND DOWNY FLAKE.

THE WOODS ARE LOVELY, DARK AND DEEP,

BUT I HAVE PROMISES TO KEEP,
AND MILES TO GO BEFORE I SLEEP,
AND MILES TO GO BEFORE I SLEEP."