CS 411 Homework #1

Question 1:

There is 2 meaningful words which are SLEEP and BUNNY.

Keys are 5 and 14

Question 2:

One of the most used letters in plaintext is already given to us as “T” and in cipher text most used words are “Z” and “S”.

So, we have 2 options:

T -> Z (19,25)

T -> S (19,18)

We are 26 letters, so we are taking relatively prime numbers to 26 for alpha value.

Which are `[1,3,5,7,9,11,13,17,19,21,23,25]`

For encryption -> `key.beta = (ciphertextvalue) - (19 * alphavalue) % 26`

Ciphertext value either can be 25 (Z) or 18 (S).

I search for possible meaningful plaintext through them.

I got 24 possible plaintexts and meaningful one is.

```
THOUGH THIS BE MADNESS, YET THERE IS METHOD IN IT.

Alfa = 23

Beta = 4

Tetha = 10

Gamma = 17
```

Question 3:

AA, AB, AC, AD …. ZY,ZZ, .. , ,. …

There is 28^2 combinations of letters which is 784 -> Modulus

For calculating key space, we need to find the count of numbers that relatively prime to 784 which is 336.

Key space = 336 * 784 = 263424

Modulus = 784

Question 4:

As compared bigram option is more secure than one letter affine cipher because key space is larger, but it is still not completely secure.

Question 5:

The information given as length of the text is 2k+1 and finishing with ".". So, at the end of the plain text, we should see ".X"

According to the cipher text we have:

.X -> YT

As explained in Question 3 our key space is 784.

With this information I ran the function that I wrote which is affine_decription_loop_q5. (You can find function in attachment).

After looking at possible 336 outputs meaningful output is:

```
I HAVE COME TO BELIEVE THAT THE WHOLE WORLD IS AN ENIGMA.X
```

Question 6:

Plaintext to cipher text if shift amount is uniformly random (it means all letters ha ve equal chance to be shown).
There is 29^2 possible relations. For example
A -> A, A -> B, A -> C, ... Z -> Y, Z -> Z
Possibility that one occurring is 1/29^2
Chance that every letter exist in cipher text is 29 * 1/29^2 = 1 / 29

Question 7:

I used 4 different functions to solve Vigenère cipher.

First, I remove blank spaces, dots, commas etc.

Then, i shifted the text and find the key space as 6 because when I shifted the text every 6th iteration has more coincidences than others.

```
Iteration -> Coincidences
# 1 -> 33
# 2 -> 44
# 3 -> 29
# 4 -> 26
# 5 -> 35
# 6 -> 65
# 7 -> 22
# 8 -> 45
# 9 -> 42
# 10 -> 33
# 11 -> 46
# 12 -> 58
# 13 -> 38
# 14 -> 35
# 15 -> 43
# 16 -> 45
# 17 -> 43
# 18 -> 61
```

After frequency analysis key can be found as “CNAYSK”.

I convert the found key to list -> [2,13,0,24,18,10]

Then, I shift the cipher text according to these 6 numbers.

Meaningful text is:

HEWALKEDATTHEOTHERSHEELSWITHASWINGTOHISSHOULDERSANDHISLEGSSPRE
ADUNWITTINGLYASIFTHELEVELFLOORSWERETILTINGUPANDSINKINGDOWNTOTH
EHEAVEANDLUNGEOFTHESEATHEWIDEROOMSSEEMEDTOONARROWFORHISROLL
INGGAITANDTOHIMSELFHEWASINTERRORLESTHISBROADSHOULDERSSHOULDCOL
LIDEWITHTHEDOORWAYSORSWEEPTHEBRICABRACFROMTHELOWMANTELHEREC
OILEDFROMSIDETOSIDEBETWEENTHEVARIOUSOBJECTSANDMULTIPLIEDTHEHAZA
RDSTHATINREALITYLODGEDONLYINHISMINDBETWEENAGRANDPIANOANDACENT
RETABLEPILEDHIGHWITHBOOKSWASSPACEFORAHALFADOZENTOWALKABREASTY
ETHEESSAYEDITWITHTREPIDATIONHISHEAVYARMSHUNGLOOSELYATHISSIDESHED
IDNOTKNOWWHATTODOWITHTHOSEARMSANDHANDSANDWHENTOHISEXCITED
VISIONONEARMSEEMEDLIABLETOBRUSHAGAINSTTHEBOOKSONTHETABLEHELURC
HEDAWAYLIKEAFRIGHTENEDHORSEBARELYMISSINGTHEPIANOSTOOLHEWATCHED
THEEASYWALKOFTHEOTHERINFRONTOFHIMANDFORTHEFIRSTTIMEREALIZEDTHA
THISWALKWASDIFFERENTFROMTHATOFOTHERMENHEEXPERIENCEDAMOMENTA
RYPANGOFSHAMETHATHESHOULDWALKSOUNCOUTHLYTHESWEATBURSTTHROU
GHTHESKINOFHISFOREHEADINTINYBEADSANDHEPAUSEDANDMOPPEDHISBRONZ
EDFACEWITHHISHANDKERCHIEF