Homework #1

1. “NYVVC” can be decrypted to “WHEELS” with encryption key J, and “DOLLS” with encryption key Q. I have found these solutions with coding in python, first I have find the number representation of the word “NYVVC” and then for all the numbers in the range from 0 to 25, I have tried all of them as keys and decrypt the ciphertext into plaintext using these keys. Out of 26 of them I have found 2 meaningful words which are “WHEEL” and “DOLLS” where “WHEEL” encrypted to “NYVVC” with encryption key J and “DOLLS” encrypted to “NYVVC” with encryption key Q. The corresponding python code is provided in the zip file.

2. The plaintext of that ciphertext is “Success is not final, failure is not fatal: it is the courage to continue that counts.”. For that question I have used the python and coded the steps to decrypt the ciphertext. For that I first find the most common letter in the ciphertext which is G with 10 repeats. As we have given the most common letter in the plaintext as T, and affine cipher is a substitution cipher, that means that the T is encrypted to G. Then I have found the possible alpha beta pairs for the affine cipher. To find the possible alpha beta pairs I have used the fact that alpha can take only the numbers that are less than 26 and are relatively prime to 26. So we have 12 possible alpha which are {1,3,5,7,9,11,15,17,19,21,23,25}. Then using that alpha values and the using the fact that T is encrypted to G I have found the corresponding beta values for the corresponding alpha values:

   Beta = (6 - alpha * 19) mod 26 where G is encoded as 6 and T encoded as 19.

   After finding all possible alpha beta values, I have tried all of them to decrypt the ciphertext. To decrypt the ciphertext I have used the code provided in hw01_helper.py. I have looked at all the decrypted texts and found the one which has meaning.

   In the end I have found that the key values that we are looking for is

   Encryption keys: alpha = 9 and beta = 17

   Decryption keys: gamma = 3 and theta = 1

   The plaintext is “Success is not final, failure is not fatal: it is the courage to continue that counts.”

   The corresponding python code is provided in the zip file.

3. The ciphertext send by server was “JĞRVĞZ PABMİAÖAZKG ŞİHI CAMGZİGDAZ RĞİZFL OGZKA JĞRVĞZİĞDFZF KGÖAİ PABMİAOİGDAZKG PĞİFSĞZ AZYĞZİĞDF KĞ GMOAİGRGCAİGÜGÖAZA KÇSÇZGDGO MGKADUAZ ŞİEHSİĞDKF ĞEĞ CH MÇD OHSOHİĞDFZ MÇEÇ KĞÖFİEFSMF ĞDMFO CHUÇZ OGZKAYA VG KŞYMİĞDF ŞDĞRĞ UGİGDGO JĞRVĞZ PABMİAÖAZAZ KNDM CAD RĞZFZF UGLAI AZÜGİGEASİGD VG RĞİZFLÜĞ GZ RGZA RNZMGEİGDİG KGÖAİ ĞRZF LĞEĞZKĞ CÇMÇZ PABMPAİGDG NDZGO ŞİEĞYF UGDGOGZ CAD KAYAIİAZ VG KÇLGZİG OĞDSFİĞSEFSİĞDKF JĞRVĞZ PABMİAÖAZKGOA ĞSĞÖF OGYAEİGDKGZ JĞRVĞZİĞDFZ ÇİOGZAZ CÇMÇZ JĞRVĞZİĞDFZKĞZ KĞJĞ PŞO PĞİFSFI KĞJĞ ĞL RGKAOİGDAZA YNRİGEGO JGDJĞİKG RĞZİFS ŞİEĞRĞÜĞOMF CHUÇZ UGDPGOMGZ KG OGZKAYA VG KŞYMİĞDF JĞRVĞZ PABMİAÖAZKG NRİG SGRİGD UNDEÇSİGDKA OA CHZİĞDF OGZKA PABMİAOİGDAZKG KG JGEGZ HRUHİĞEĞRĞ OŞREĞRF KÇSÇZÇRŞDİĞDKF YNLİGDAZA JĞRVĞZ PABMİAÖA AİG OŞESHİĞDF ĞDĞYFZKĞ VĞD ŞİĞZ VG YÇDEGYA UGDGOGZ KŞYMİHO KHRUHİĞDFZF CAD OGL KĞJĞ VHDUHİĞRĞDĞO CAMADEGO AYMARŞDKH KŞEHLİĞD AİG AZYĞZİĞD ĞDĞYFZKĞ GZ OÇPÇO CAD PFOĞD PĞMFSEĞYF RŞOMH ŞİEĞYF APAZ CAD ZGKGZ KG UNDGEARŞDKH VGDKAOİGDA HÖDĞSİĞD KĞ OĞDSFİĞSMFOİĞDF UÇPİÇOİGD KG CADKA” and the most common letter in the corresponding plaintext was A. As if I have done in question 2, I have found the most common letter in the ciphertext and since this is an affine cipher we can say that the most common letter in the plaintext is encrypted to the most common letter in the ciphertext. The most common letter in the ciphertext is Ğ that means that the plaintext letter A is encrypted to ciphertext letter Ğ. Then we need to find the possible alpha beta pairs. Possible alpha values that the key alpha can take is all the numbers from 0 to 29, 29 excluded. Because in Turkish alphabet there are 29 letters and sșnce 29 is a prime number, alpha can take all the values from 0 to 28. Then I have found the corresponding beta values using A, Ğ and possible alpha values.

   Beta = (8 - alpha * 0) mod 26 where Ğ is encoded as 8 and A encoded as 0. Then we can observe that since we are multiplying alpha with 0, the only possible beta value is 8.

   After trying all the alpha beta pairs which are 29 of them, with alpha = 23 and beta = 8 we can get the plaintext “HAYVAN ÇİFTLİĞİNDE OLUP BİTENLERİN YALNIZ KENDİ HAYVANLARINI DEĞİL ÇİFTLİKLERİNDE ÇALIŞAN İNSANLARI DA ETKİLEYEBİLECEĞİNİ DÜŞÜNEREK TEDİRGİN OLMUŞLARDI AMA BU TÜR KUŞKULARIN TÜMÜ DAĞILMIŞTI ARTIK BUGÜN KENDİSİ VE DOSTLARI ORAYA GELEREK HAYVAN ÇİFTLİĞİNİN DÖRT BİR YANINI GEZİP İNCELEMİŞLER VE YALNIZCA EN YENİ YÖNTEMLERLE DEĞİL AYNI ZAMANDA BÜTÜN ÇİFTÇİLERE ÖRNEK OLMASI GEREKEN BİR DİSİPLİN VE DÜZENLE KARŞILAŞMIŞLARDI HAYVAN ÇİFTLİĞİNDEKİ AŞAĞI KESİMLERDEN HAYVANLARIN ÜLKENİN BÜTÜN HAYVANLARINDAN DAHA ÇOK ÇALIŞIP DAHA AZ YEDİKLERİNİ SÖYLEMEK HERHALDE YANLIŞ OLMAYACAKTI BUGÜN GERÇEKTEN DE KENDİSİ VE

DOSTLARI HAYVAN ÇİFTLİĞİNDE ÖYLE ŞEYLER GÖRMÜŞLERDİ Kİ BUNLARI KENDİ ÇİFTLİKLERİNDE DE HEMEN UYGULAMAYA KOYMAYI DÜŞÜNÜYORLARDI SÖZLERİNİ HAYVAN ÇİFTLİĞİ İLE KOMŞULARI ARASINDA VAR OLAN VE SÜRMESİ GEREKEN DOSTLUK DUYGULARINI BİR KEZ DAHA VURGULAYARAK BİTİRMEK İSTİYORDU DOMUZLAR İLE İNSANLAR ARASINDA EN KÜÇÜK BİR ÇIKAR ÇATIŞMASI YOKTU OLMASI İÇİN BİR NEDEN DE GÖREMİYORDU VERDİKLERİ UĞRAŞLAR DA KARŞILAŞTIKLARI GÜÇLÜKLER DE BİRDİ".

Encryption keys: alpha= 23, beta=8

Decryption keys: gamma= 24, theta= 11

The corresponding python code is provided in the zip file.

4. The modulus for this new affine cipher is $31^3 = 29791$ because we are encoding a triagram which has 3 letters in it and we have 31 possibilities for each of the letter in the given alphabet. The first letter may take 31 possibilities from the alphabet, second letter may take 31 possibilities from the alphabet and the third letter may take 31 possibilities from the alphabet. When we calculate the Euler's function we have the alpha can take 28830 different possibilities because the alpha values should be relatively prime to the modulus and we have 28830 different possibilities for alpha can take between [1, 29791). Beta can take any value between [1, 29791] then beta can take values 29791 different values. So the key space is the number of different alpha values * number of different beta values and it's equal to $28830 \cdot 29791 = 858874530$. Then the modulus is 29791 and key space is 858874530.

5. For this question I've written a python code which is available in the zip file. We know from the hints that the last three characters of the plaintext is ".XX" and it's equivalent to "XFD" in the ciphertext. First I've found the possible alpha values where alpha values are relatively prime to the modulus 29791. We have 28830 different alpha values. Then I've encoded the part of the plaintext ".XX" and part of the ciphertext "XFD" using the formula given in the 4th question. Then using the encoded numbers and possible alpha values I've found the corresponding beta values for the alpha values. I've found the beta values as:

Beta = (encode("XFD") - alpha * encode(".XX")) mod 29791

I've kept the alpha beta pairs that ensure the above equation in the tuples of list where at each tuple we have a possible alpha value and it's correspondent beta value. Then I've changed the Affine_Dec function that is given in the hw01_helper.py with the new affine cipher. For every alpha beta values I've called the Affine_Dec function. In Affine_Dec function for every triagram in the ciphertext it encodes the triagram, calculate the gamma and theta values for the the corresponding alpha beta value. Then we calculate the encoded number of the corresponding plaintext which is calculated as:

Encode[plaintext] = (gamma * encode[ciphertext] + theta) mod 29791

To decode this big number of encode[plaintext], first we take the mod 31 and get the last letter of the triagram. Then we subtract the first letter from the encode[plaintext], get the mod $31^2 = 961$ and then divide it by 31 and get the second letter. Then we subtract the second letter from encode[plaintext], get mod 29791 and divide it by $31^2 = 961$ and get the first letter of the triagram:

position_firstletter = encode[plaintext] mod 31

position_secondletter =((encode[plaintext] - position_firstletter) mod 961)/31

position_thirdletter= ((encode[plaintext] - position_firstletter - positionsecondletter) mod 29791)/961.

Then for every alpha beta values we have called the decryption function where we encode the ciphertext triagrams and decode them into decrypted triagrams and find the corresponding decrypted texts for each pair. Then we have 28830 different decrypted texts since we have 28830 different alpha beta pairs. To find the meaningful one among all of these decrypted text, I've imported enchant and created a dictionary of all the English alphabet. Wherever I decrypt the ciphertext, I've put all the words of the decrypted texts into a function check where it checks in the dictionary that this word is meaningful in English or not. If all the words in the decrypted text is meaningful in English then I've found the plaintext that we are looking for. The plaintext in the end is "TO LIVE IS THE RAREST THING IN THE WORLD. MOST PEOPLE EXIST, THAT IS ALL.XX".

The keys that are used to encrypt the plaintext is alpha = 129 and beta = 6119

The keys that are used to decrypt the ciphertext is gamma = 26096 and theta = 28127

6. Since this message is from you to us, I've thought that the last 2 words would be ERKAY SAVAS. For this question I've written a python code too. First I've find the difference between encoded ciphertext letters and encoded plaintext letters where ciphertext is "EXEPY LABUH" and plaintext that I've thought it would be "ERKAY SAVAS". Then I've got the list of keys which is [0, 6, 20, 15, 0, 19, 0, 6, 20, 15]. There are 10 numbers since the length of EXEPY LABUH and ERKAY SAVAS is 10 but the key might be less than 10 and might be repeating itself in these 10 numbers which is the case. Then I've observed that in this list numbers 6, 20 and 15 are repeating twice and the difference between the two repeating indices is 6. 0 is repeating itself 3 times and the difference of the indices between first and second is 4, first and third is 6 and second and third is 2 which shows that 0 might be repeating itself in the key too. So the possible key length is 6 from the observations. Then I've counted the letters in the ciphertext that is given to us which is 51, when we take mod 6 of 51 it's equal to 3. We know that in the vigenere cipher we are repeating the key and after finishing the encrypting 6 letters of the plaintext we move onto the next 6 letters. Since mod 6 of 51 is 3, the last numbers of the list should be the first numbers of the key since it's repeating itself. So we know that the first three numbers of the key is 6, 20,15 and the key length is 6, then the last three numbers of the key should be 0, 19, 0 because there's a pattern in the list. Then the key is [6, 20, 15, 0, 19, 0] which is equal to word **"GUPATA"**.

Then I've found the encoded number of each plaintext letter using the equation:

If i is the index of ciphertext letter and key = [6,20,15,0,19,0]

encoded[plaintext_letter] = (encoded[ciphertext_letter] - key[i mod(6)]) mod 26

After that decoded all the numbers into letters and find the plaintext as "DEAR STUDENT, SIMPLICITY IS THE KEY TO BRILLIANCE, ERKAY SAVAS".

7. To find the key I've written a python code that is available in the zip file. First I take the ciphertext and shift it 1 letter and count the coincidences, the same letters. Then I shift the ciphertext 2 letters and count the coincidences and so on. I've shifted the ciphertext for [1,15] and count the coincidences at each shift. The maximum number of coincidences happened when I shifted the ciphertext for 7 letters to the right. So the possible key length is 7 since it gives the highest number of coincidences was 38. Then I've obtained 7 different subciphertexts from the ciphertext and found the number of each letter in these subciphertexts and ordered them in decreasing order.

For the first subciphertext the most common letters were ‘L, V, O, U, Z’. We know that letter ‘E’ is the most frequent letter in the English alphabet. If E is encrypted to L then the first key would be 7. Then O is encrypted into V, H is encrypted to O, N is encrypted to U and S encrypted to Z:

E → L, O → V, H → O, N→ U, S → Z. We know from the frequency of the letters in English that O, N and S are frequent letters in English so first key can be 7 which is equal to H. k1 = 7 = ‘H’

For the second subciphertext the most common letters were ‘W, B, Z, M, I, Q, V’. If E is encrypted to W then key is 18 and

J → B H → Z U → M Q → I Y → Q D → V

But we know that J, U, Q, Y are not frequent letters in English so E might not be encrypted to W.

If we try the second most frequent letter in English alphabet T → W then the key is 3 and

Y → B W→ Z J→ M F → I N→ Q S→ V

But we know that Y, W, J and F are not frequent letters in English so it’s not likely that key is 3.

If we try to encode the third most frequent letter in English A → W then the key is 22 and

F → B D → Z Q → M M → I U → Q Z → V

But we know that F, Q , Z, M are not frequent letters so it’s not likely that key is 22.

Finally if we try to encode the fourth most frequent letter O → W then the key is 8 and

T → B R → Z E → M A → I I → Q N → V

And we know that all of them are frequent letters in English so k2 = 8 = ‘I’

For the third subciphertext the most frequent letters are ‘Q, F, A, D, G, K’. If we encrypt

E → Q then the key is 12 and

T → F O→ A R→ D U→ G Y → K

We know that T, O, R are very frequent letters so k3 might 12. k3= 12 = ‘M’

For the fourth subciphertext most frequent letters are ‘M, Z, B, G, P. If we encrypt

E → M then the key is 8 and

R → Z T → B Y → G H → P

We know that R, T and H are frequent letters so fourth key might be 8. k4= 8 =’I’

For the fifth subciphertext the most frequent letters are ‘X, B, H, M, T, G’. If we encrypt E→ X then the key is 19 and

I → B O→ H T→ M A→ T N→ G

We know that I, O, T, A and N are very frequent letters in English alphabet so the key is most probably 19. k5= 19 = ‘T’

For the sixth subciphertext the most frequent letters are ‘W, G, L, F, J’. If we encrypt E→ W then the key is 18 and

O → G T→ L N→ F R → J

We know that O, T, N, R are very frequent letters in English alphabet so the key is most probably 18. k6= 18 = ‘S’

For the seventh subciphertext most frequent letters are ‘M,N,X,Y,B,C,L’. As I’ve done in the previous ciphertexts I first try to encrypt E → M but when I’ve done it the most frequent letters in the decrypted text would be ‘P,Q,T,U,D,Z’ and except for T none of them are frequent letters in the alphabet. Then I’ve tried T, A, O, I, N and S in order since these are the most frequent letters in the alphabet and it’s likely that the most frequent letter in the subciphertext was encrypted from one of them. When I tried the letters T, A, O, I and N thenI’ve realized that the most frequent letters in decrypted texts are not frequent letters in English. But when I encrypt S → M and key would be 20 and

T → N D → X E → Y H→ B I→ C R → L

And we know that T, E, H, I, R are all frequent letters in English alphabet so the last key is likely to be 20. k7= 20 = ‘U’

Then when we combine k1, k2, k3, k4, k5, k6, k7 and decode them the key would be a 7 letter word ‘HIMITSU’.

I’ve tried to decrypt the ciphertext with key **‘HIMITSU’** and got the plaintext:

I’ll go to another country, go to another shore, find another city better than this one. Whatever I try to do is fated to turn out wrong and my heart lies buried like something dead. How long can I let my mind moulder in this place? Wherever I turn, wherever I look, I see the black ruins of my life, here, where I’ve spent so many years, wasted them, destroyed them totally. You won’t find a new country, won’t find another shore. This city will always pursue you. You’ll walk the same streets, grow old in the same neighborhoods, turn gray in these same houses. You’ll always end up in this city. Don’t hope for things elsewhere: there’s no ship for you, there’s no road. Now that you’ve wasted your life here, in this small corner, you’ve destroyed it everywhere in the world.