

Intermediate Project Document

Course Title: CE 340 Cryptography & Network Security

Project Title: Affine Crypto System

Deadline: 2 November 2015

Project Member: Emre Övünç

Contents

PART ONE

1. Experiment description
 - 1.1 *How affine crypto system works*
 - 1.2 *How my codes work*
 - 1.3 *Explaining my codes*
 - 1.4 *Input & Output relations*
 - 1.5 *User guide (short)*

PART TWO

2. Outcomes
 - 2.1 *What did I achieve?*
 - 2.2 *Did the subject become clear to me?*

PART THREE

3. Codes

PART FOUR

4. Results
 - 4.1 *Screenshots of input & output files*
 - 4.2 *Screenshots of ranking files*
 - 4.3 *Download link (MD5 and SHA1 Sum)*

PART ONE

1.1 How affine crypto system works:

The form of the affine cipher is $E(x) = [a \cdot x + b] \bmod(m)$. Here, a and b are integers (keys); x is the plaintext number to be encrypted. m is 26, because of the use of a 26 character alphabet in English Alphabet.

Similarly, the decryption form is $D(y) = [a^{-1} \cdot (y-b)] \bmod(m)$. a^{-1} is the inverse of a.

For instance, let us encrypt the plain text "EMRE OVUNC", using the key a=3, b=8. First of all, we find the integer value of each letter in the plain text and perform the calculations on those values.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plain Text	E	M	R	E	O	V	U	N	C
x	4	12	17	4	14	21	20	13	2
3x+8	20	44	59	20	50	71	68	47	14
mod 26	20	18	7	20	24	19	16	21	14
Cipher Text	U	S	H	U	Y	T	Q	V	O

```
A=AffineCryptosystem(AlphabeticStrings())
P=A.encoding("EMREOVUNC")
a,b=(3,8)
C=A.enciphering(a,b,P)
A.deciphering(a,b,C)==P
print C
```

USHUYTQVO

1.2 How my codes work:

First of all, my codes create affine crypto system and read the plain text from the text file. Then, it generates two keys (key1, key2) and encrypts the plain text -called Cipher (encrypted text)- with using these keys. Next, it writes cipher into another text file.

After that, my codes also generates two keys, but these keys are inverse of the key1 and key2. After reading encrypted text, it decrypts all of text and again writes into a another text file, I called DecryptedMessage in my codes.

Lastly, I use ranking function to try bruteforce attack with different parameters and write results into another text file.

1.3 Explaining my codes:

def AffineCryptoSystem()

I tried to use it as a main function.

A=AffineCryptosystem(AlphabeticStrings())

Creates an affine cryptosystem.

PlainText=A.encoding(Read_TextFile())

In this line, I read the text file from my desktop with using Read_TextFile() function and encode it. In addition, Read_TextFile() function return lines of file.

key1,key2=GenerateKeys(A)

I generate key1 and key2 with using GenerateKeys() function. This function create key pairs like a,b=A.random_key() and return them.

Cipher=Encryption(A,PlainText,key1,key2)

In this line, I go to the Encryption() function to create cipher text and return Cipher. Also, we use key1 and key2 because of $E=A(\text{key1},\text{key2})$.

key1Inv,key2Inv=GenerateInverseKeys(A,key1,key2)

Like creating key1 and key2, I inverse key1 and key2 with using GenerateInverseKeys() function and this function return inverse of key1 and key2.

aInverse,bInverse=A.inverse_key(a,b)

I generate inverse key of the a and b.

Write_DeryptedText(A,Decryption(A,key1Inv,key2Inv))

This function allows me to write Cipher as a text file.

Ranking_None(A,Cipher)

Ranking_Chisquare(A,Cipher)

Ranking_Squared(A,Cipher)

These functions attempt a brute force cryptanalysis of the ciphertext Cipher.

with open ('path/to/my/file','r' or 'w') as TextFile

In this line, I can read or write a text file for my results. 'r' is read, 'w' is write and 'r+' is read and write.

TextFile.write(Cipher)

This command allows me to write Cipher into text file which I opened later.

1.4 Input & Output relations

On the one hand, when we take a look inputs, we see that inputs are the plain text like “Hello Cryptography” and it may be one sentence or more sentences. On the other hand, output is encrypted text which is “TWPPMYJCLHMUJALTC”. We see that the differences between inputs and outputs. This relationship shows us that the algorithm that we can use, works correctly. In addition, you can look the PART FOUR to compare results.

1.5 User Guide

You should change the directory of your plain text message to run this program properly. There are 7 directory path in my codes which you should change.

For Example:

with open ('/home/debian/Desktop/Message.txt','w') as TextFile

with open ('/Your/Message/Path/','w') as Text File

PART TWO

2.1 What did I achieve?

I learn affine crypto system and algorithm. Also, I want to draw attention to compare results and input&outputs file. These results show us how to encrypt & decrypt file with using create and read text file.

2.2 Did the subject become clear to me?

The subject become clear to me because of this project. I work on generating key, read&write text file functions and sage math. In addition, I understand that brute force attack is very important to see encryption schemes and key pairs..

PART THREE

3. Codes

```
def AffineCryptoSystem():
    A=AffineCryptosystem(AlphabeticStrings())
    PlainText=A.encoding(Read_TextFile())

    key1,key2=GenerateKeys(A)
    Cipher=Encryption(A,PlainText,key1,key2)
    Write_EncryptedText(Cipher)

    EncryptText=A.encoding(Read_TextFile())

    key1Inv,key2Inv=GenerateInverseKeys(A,key1,key2)
    Write_DecryptedText(A,Decryption(A,key1Inv,key2Inv))

    Ranking_None(A,Cipher)
    Ranking_Chisquare(A,Cipher)
    Ranking_Squared(A,Cipher)

def GenerateKeys(self):
    a,b=self.random_key()
    return a,b

def GenerateInverseKeys(self,a,b):
    aInverse,bInverse=self.inverse_key(a,b)
    return aInverse,bInverse

def Encryption(self,P,a,b):
    E=self(a,b)
    C=E(P)
    return C

def Decryption(self,aInverse,bInverse):
    D=self(aInverse,bInverse)
    return D

def Read_TextFile():
    with open("/home/EmreOvunc/Desktop/Message.txt", 'r') as TextFile:
        lines=TextFile.read()
    TextFile.close()
    return lines
```

```

def Write_EncryptedText(Cipher):
    with open("/home/EmreOvunc/Desktop/EncryptedMessage.txt", "w") as
EncryptedText:
        EncryptedText.write(str(Cipher))
        EncryptedText.close()

def Write_DecryptedText(self,D):
    with open('/home/EmreOvunc/Desktop/EncryptedMessage.txt', 'r') as
ReadEncryptedFile:
        line=ReadEncryptedFile.read()
        line=self.encoding(line)

        DecryptedText= open("/home/EmreOvunc/Desktop//DecryptedMessage.txt", "w")
        DecryptedText.write(str(D(line)))
        DecryptedText.close()

def Ranking_Squared(self,Cipher):
    Rank = self.brute_force(Cipher, ranking="squared_differences")
    with open("/home/EmreOvunc/Desktop/Ranking_Squared.txt", "w") as
Ranking_Squared:
        Ranking_Squared.write(str(Rank))
        Ranking_Squared.close()

def Ranking_Chisquare(self,Cipher):
    Rank = self.brute_force(Cipher, ranking="chisquare")
    with open("/home/EmreOvunc/Desktop/Ranking_Chisquare.txt", "w") as
Ranking_Chisquare:
        Ranking_Chisquare.write(str(Rank))
        Ranking_Chisquare.close()

def Ranking_None(self,Cipher):
    L=self.brute_force(Cipher)
    with open("/home/EmreOvunc/Desktop/Ranking_None.txt", "w") as
Ranking_None:
        Ranking_None.write(str(L))
        Ranking_None.close()

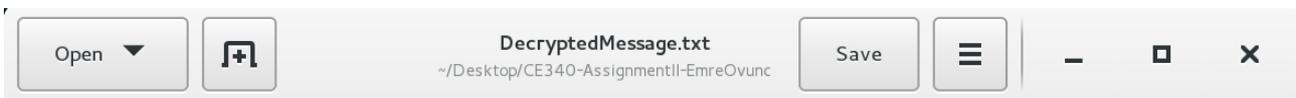
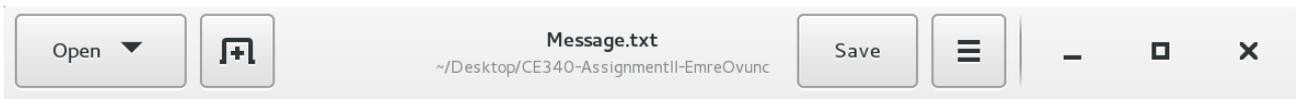
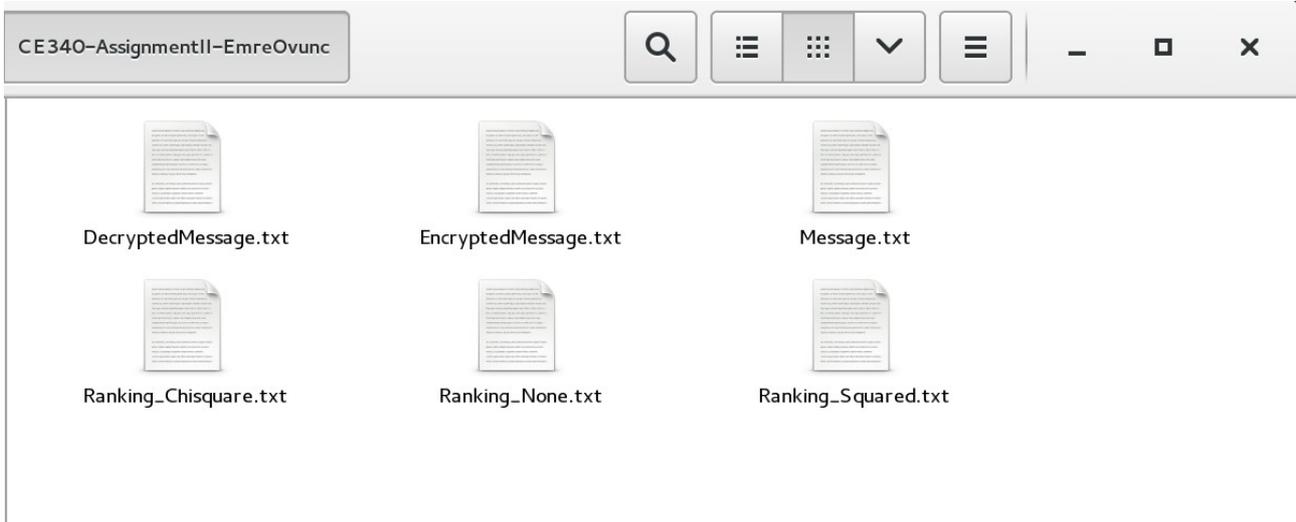
if __name__ == "__main__":
    main()

def main():
    AffineCryptoSystem()

```

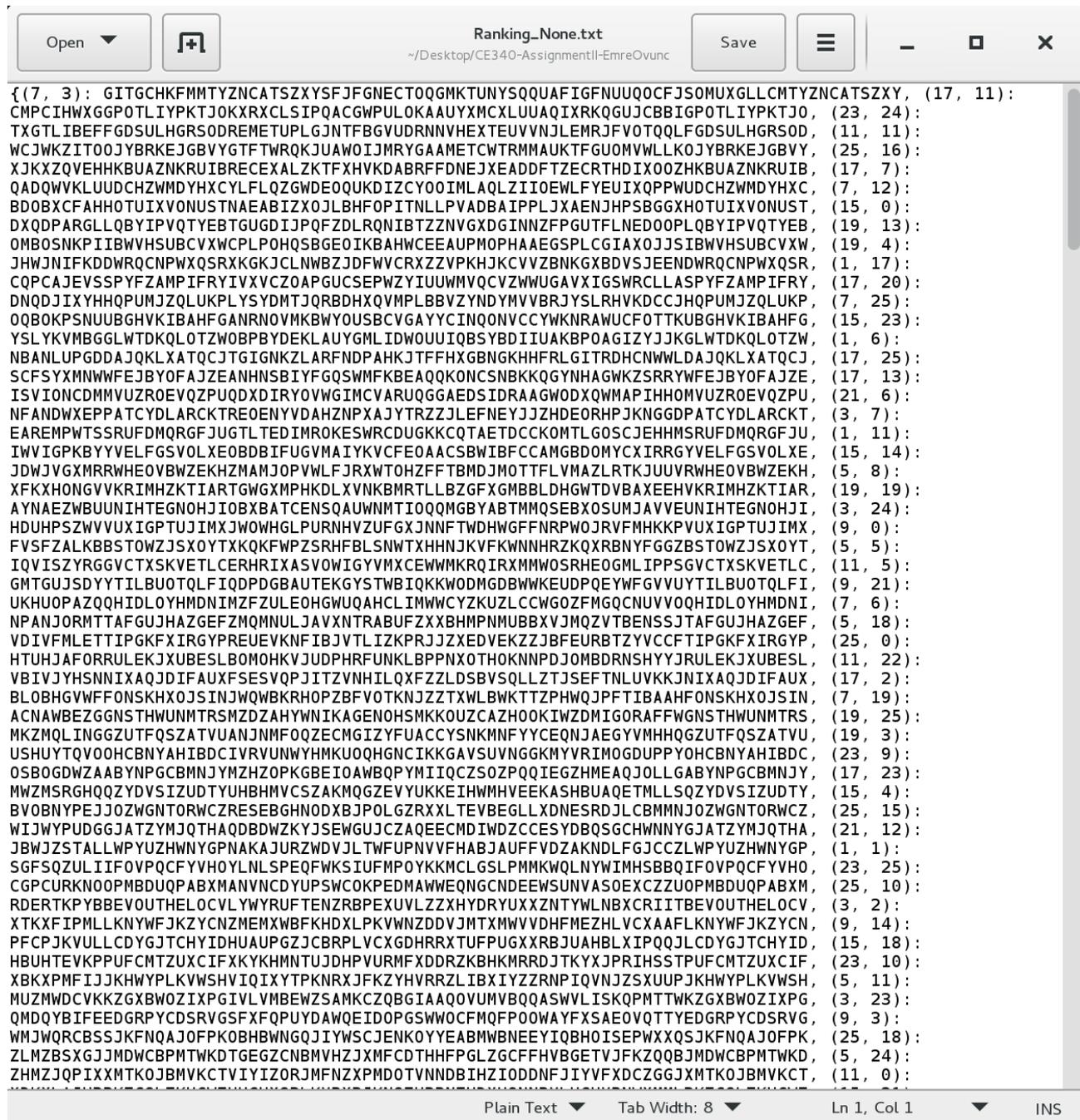
PART FOUR

4.1 Screenshots of input & output files



4.2 Screenshots of ranking files

Ranking_None(self,Cipher):



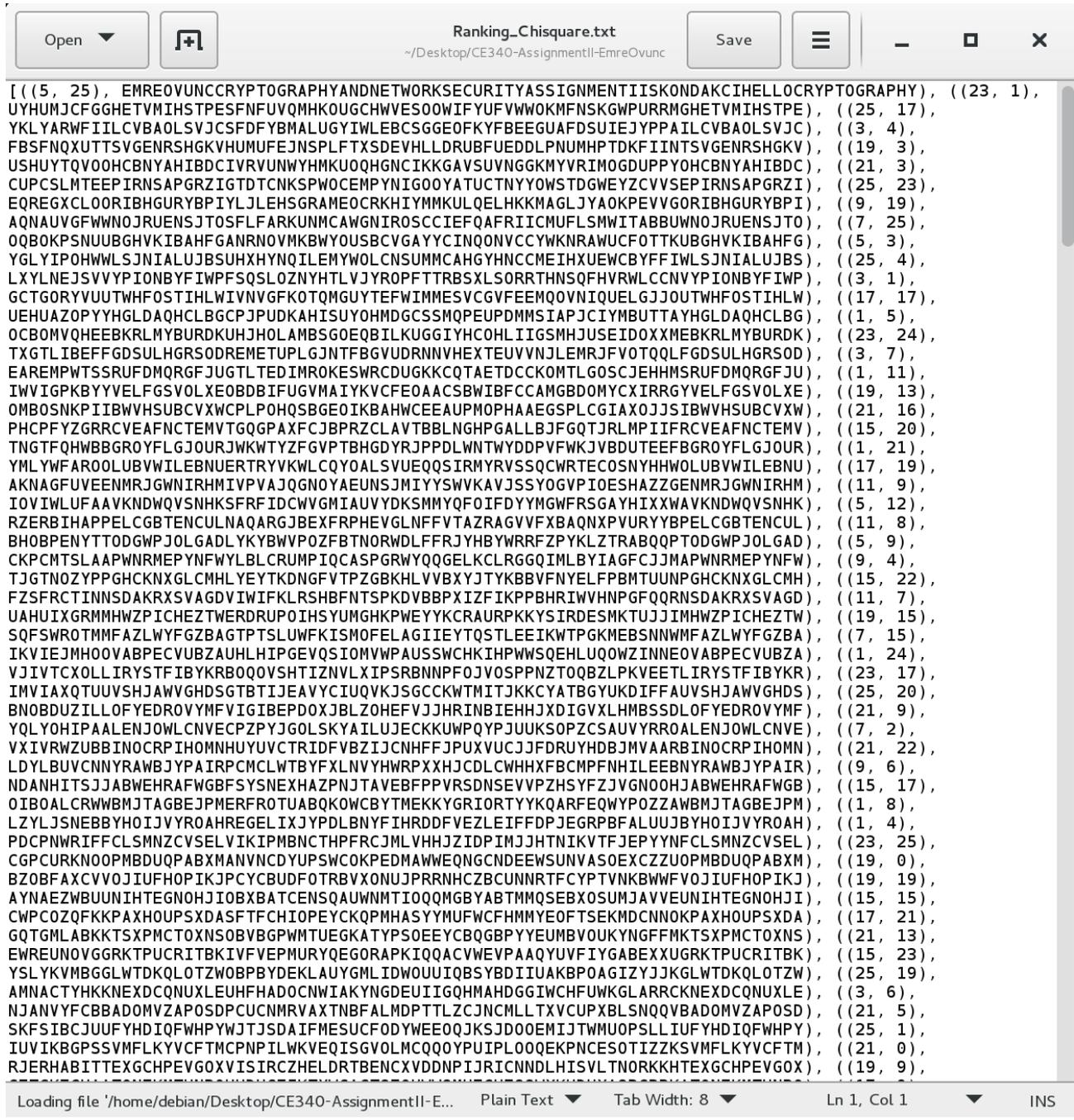
```
{(7, 3): GITGCHKFMPTYZNCATSZXYSFJGNECTOQGMKTUNYSQUAFIGFNUUQOCFJSMUXGLLCMTYZNCATSZXY, (17, 11):
CMPCIHXXGGPOTLIYPKTJOKXRXCLSIPOACGWPULOKAAUYXMCXLUUAQIXRKGQGUJCBIGPOTLIYPKTJO, (23, 24):
TXGTLIBEFFGDSULHGRSODREMETUPLGJNTFBGVUDRNNVHEXTEUVVNJLEMRJFVOTQQLFGDSULHGRSOD, (11, 11):
WCJWKZITOOJYBRKEJGBVYGTFTWRQKJUAWOIJMRYGAAMETCWTRMMAUKTFGUOMVWLLKOJYBRKEJGBVY, (25, 16):
XJKXZQVEHHKBUAZNRKUIBRECEXALZKTFXHVKDABRFFDNEJXEADDFTECERTHDIX00ZHKBUAZNRKUIB, (17, 7):
QADQWKLUDCHZMWDYHXYLFLQZGWDEOQKDIYZCYOIMLAQLZIIOWELFYEUIXQPPWUDCHZMWDYHXC, (7, 12):
BDOBXCFAHHOTUIXVONUSTNAEABIZXOJLBHFOPITNLLPVADBAIPPLJXAENJHPSBGGXHOTUIXVONUST, (15, 0):
DXQDPARGLLQBYIPVQTYEBTGUGDIJPOFZDLRQNBIBTZNVGXDGINNFPUGUFTLNEDOOPLQBYIPVQTYEB, (19, 13):
OMBOSNKPIBWBVHUBCVXWCLPOHQSBGEOIKBAHWCEEAUPMOPHAAEGSPLCGIAXOJJSIBWBVHUBCVXW, (19, 4):
JHWJNIFKDDWRQCNPNWQSRXKXGKJCLNWBZJDFWVCRXZVVPKHJKCVVZBNKGXBDVSEENDWRQCNPNWQSR, (1, 17):
CQPCAJEVSSPYFZAMPFRYIVXVCZOAPGUCSEPZYIUUWVQCVZWWUGAVXIGSWRCLLSPYFZAMPFRY, (17, 20):
DNQDJIXYHHQPUMJZQLUKPLYSYDMTJQRBDHXQVMPVBBVZYNDYVMBRBJYSLRHVKDCCJHQPUMJZQLUKP, (7, 25):
OQBOKPSNUUBGHVKBIAHFGANRNOVMKBWYOUSBCVGAYYCINQONVCCYWKNRWUCFOTTKUBGHVKBIAHFG, (15, 23):
YSLYKVMGGGLWTDKQLOTZWOBBYDEKLAUYGMLIDWOUUIQBSYBDIIUAKBPOAGIZYJJKGLWTDKQLOTZW, (1, 6):
NBANLUPGDDAJQKLXATQCJTGIGNKZLARFNDAHJKJTFHXGBNGKHHFRLGITRDHCNWWLDAJQKLXATQCJ, (17, 25):
SCFSYXMMNWFEBYOFBJZEANHSBIYFGQSWMFKBEAQKONCSNBKQGYNHAGWKZSRRYWFEBYOFBJZE, (17, 13):
ISVIONCMMVUZROEVQZPUQDXDIRYOVWGMICVARUQGGAEEDSJDRAAGWODXQWMAPIHHOMVUZROEVQZPU, (21, 6):
NFANDWXEPPATCYDLARCKTREOENYVDAAHZNPAJYTRZZJLEFNEYJZHDEORHPJKNGGDPATCYDLARCKT, (3, 7):
EAREMPWTSSRUFDMQRGFJUGTLTEDIMROKESWRCDUGKKCQTAETDCCOMTLGOSCEJHHSRUFDMQRGFJU, (1, 11):
IWWIGPKBYVELFGSVOLXE0BDBIFUGVMAIYKVCFE0AACSBWIBFCCAMGBDOMYXCIRRGYVELFGSVOLXE, (15, 14):
JDWJVGXMRWHEOVWBZEKHZMAMJOPVWLFJRXWTOHZFFTBMDJMOITFLVMAZLRTKJUUVRWHEOVWBZEK, (5, 8):
XFKXHGONVVKRIMHZKTIARTGWGMPHKDLXVNBKMRLLBZGFXGMBBLDHGWTDBAXEEHVKRIMHZKTIAR, (19, 19):
AYNAEZBUUNIHTEGNOHJIOBXBATCENSQAUNMTIOQQMGBYABTMMQSEBXOSUMJAVVEUNIHTEGNOHJ, (3, 24):
HDUHPSZWWVUXIGPTUJIMXJWOWHGLPURNHVZUFGXJNNFTWDHWGFFNRPWJRVFMHKKPVUXIGPTUJIMX, (9, 0):
FVSFZALKBBSZTOWZJXSXYTKQKFWPZSRHFBLSNWTXHHNJKVFKWNNHRZKQXRBNYFGGZBSTOWZJXSXY, (5, 5):
IQVISZYRGGVCTXSKVETLCERHRIXASVOWIGYVMXCEWMMKQIRXMMWOSRHEOGLIPPSGVCTXSKVETLC, (11, 5):
GMTGUJSDYITILBUOTQLFIQDPDGBAUTEKGYSTWBIQKKWODMGBWKEUDPQYWFVGVUUTILBUOTQLFI, (9, 21):
UKHUOPAZQQHIDLOYHMDNIMZFUZLEOHGWUQAHLIMWYCYZKUZLCCWGOZFMGQCNUVVOQHIDLOYHMDNI, (7, 6):
NPANJORMTAFGUJHAZGEFZMQMNLJAVXNTRABUFZXXBHMNPMBBXXVJMZVTBENSSJAFGUJHAZGEF, (5, 18):
VDIVFMLETTIPGKFIRGYPREUEVKNFIBJVTLIZKPRJZJXEDVEKZJBFEURBTZYVCCFTIPGKFIRGY, (25, 0):
HTUJHAFORRULEKJXUBESLBOMOHKVJUDPHRFUNKLBPPNXOTHOKNPNJOMBDNRSHYYJRULEKJXUBESL, (11, 22):
VBIVJYHSNNIXAQJDIFAUXFSESVPJITZVNHILQXFZLDSBYSQLLZTJSEFTNLUVKKJNIXAQJDIFAUX, (17, 2):
BLOBHGWFVONSKHXOJSINJWQWBKRHOPZBFVOTKNJZZTXLWBLWKTZTTPHWQJPTIBAAHFONSKHXOJSIN, (7, 19):
ACNAWBEZGGNSTHWUNMTRSMZDAHYWNKIKAGENOHSMMKOUZCAZHOOIKWZDMIGORAFFWGNSTHWUNMTR, (19, 25):
MKZMQLINGGZUTFQSZATVUANJNMFQZECMGIZYFUACCSYKMNFFYCEQNJAEGYVMHHQZUTFQSZATVU, (19, 3):
USHUYTQV00HCBNYAHIBDCIVRVUNWYHMKUOQHGNCKIKKAVSUVVNGGKMYVRIMOGDUPPYOHCBNYAHIBDC, (23, 9):
OSBODGWAABYNPGCBMNJYMZHZOPKGBEIOAWBQPYMIICQZSOZPQIEGZHMEDIAJOLLGABYNPGCBMNJY, (17, 23):
MWZMSRGHQZYZDVSIZUDTYUHBHVMVCSZAKMQGZEVYUKKEIHWMHVEEKASHBUAQETMLLSQZYZDVSIZUDTY, (15, 4):
BVOBNYPEJJOZWNRTORWCZRESEBGNODXBJPOLGZRXXLTEVBEGLLXDNESRDJLCBMMNJJOZWNRTORWCZ, (25, 15):
WIJWYPUJGGJATZYMJQTHAQDBDZKYZSEWGUJCAZAECEMDIWDZCCESYDBQSGCHWNNYGTATZYMJQTHA, (21, 12):
JBWJZSTALLWPUYZHWNYPNAKAJURZWDVJLTFWUPNVVFHABJAUFFVDZAKNDLFGJCCZLWPUYZHWNYP, (1, 1):
SGFSQZULIIFOVPOCFYVHOYLNLSPEQFWSIUFMPOYKKNCLGSLPMMKWLNYWIMHSBBQIFOVPOCFYVHO, (23, 25):
CGPCURKNOOPMBDUQAPABXMANVNCYUPSWCOKPEDMAWWEQNGCNDDEESUNVASOEXCZUOPMBDUQAPABX, (25, 10):
RDERTKPYBBEVOUTHLOCVLYYRUF TENZRBPEXUVLZXXHYDRYUXXZNTYWLNBXCRIITBEVOUTHLOCV, (3, 2):
XTKXFIPMLLKNYWFJKZCYNMEMXWBFKDXLPKVWVNDZDVJMTXWVVDHFMEZHLVCAAFLLKNYWFJKZCYN, (9, 14):
PFPCJKVULLCDYGTJCHYIDHUAUPGZJCBRPLVXGDRRXTUFPUGXRBJUABHLXIPQQJLCDYGTJCHYID, (15, 18):
HBUHTEVKKPUFCMTZUXCIFXKYKHMNTUJDHPVURMFDDRZKBKMRDJKYXJPRIHSSTPUFCMTZUXCIF, (23, 10):
XBKXPMFIJJKHWYPLKVWVSHVIXYTPKNRXJFKZYHVRRLIBXIZZRNPQVNVJZSXUUPJKHWYPLKVWVSH, (5, 11):
MUZMWDVCKKZGXWBOZIXPGIVLVBWZSAMKZQBGIQAQVUMVVBQASWVLISKQPMTTWKZGXWBOZIXPG, (3, 23):
QMDQYBIFEEDGRPYCDSRVGSFXFPUYDAWQEIIDOPGSSWOCFMQFP00WAYFXSAEQVQTTIEDGRPYCDSRVG, (9, 3):
WMJWQRCBSSJKFNQAJOFKPBHBNWQJJIYWSCJENKOYYEABMWBNEEYIQBH0ISEPWXXQSJKFNQAJOFK, (25, 18):
ZLMZBSXGJMDWCBPMTWKDTGEGZCNBMVHZJXMFCDTHFFPLZGCFHVBGETVJFKZQ0BJMDWCBPMTWKD, (5, 24):
ZHMZJQPIXXMTKOJBMVKCTVIYIZORJMFNZXPMDOTVNNDBIHZIODDNFJIIYVFXDCZGGJXMTKOJBMVKCT, (11, 0):
```

Ranking_Squared(self,Cipher):

```
Ranking_Squared.txt
~/Desktop/CE340-AssignmentII-EmreOvunc

[ ( ( 5, 25), EMREOVUNCCRYPTOGRAPHYANDNETWORKSECURITYASSIGNMENTIISKONDAKCIHELLOCRYPTOGRAPHY), ( ( 21, 0),
RJRERHABITTEXGCHPEVGOXVISIRZHELDRTBENCXVDDNPIJRICNNDLHISVL TNORKKHTXGCHPEVGOX), ( ( 19, 19),
AYNAEZWBUNIHTEGNOHJIOBXBATCENSQAUWNMTIOQQMGBYABTMMQSEBXOSUMJAVVEUNIHTEGNOHJI), ( ( 21, 3),
CUPCSLMTEEP IRNSAPGRZIGTDTCKNKSPOCEMPYNIIGOOYATUCTNYYOWSTDGWEYZCVVSEPIRNSAPGRZI), ( ( 23, 11),
GKTGYVORSS TQFHYUTEFBQERZRGHCYTWAGSOTIHQEA AIURKGRHIIAWYRZEWSIBGDDYSTQFHYUTEFBQ), ( ( 9, 19),
AQNAUVGFWWNOJRUENSJTOSFLFARKUNMCAWGNIROSCCIEFQAFRIICMUFLSMWITABBUWNOJRUENSJTO), ( ( 21, 6),
NFANDWXEPPA TCYDLARCKTREOENYVD AHZNPXAJYTRZZJLEFNEYJZJHDEORHPJKNGGDPATCYDLARCKT), ( ( 7, 19),
ACNAWBEZGGNSTHWUNMTRSMZDZAHYWN IKA GENOHS MKKOUZCAZH00KIWZDMIGORAFFWGNSTHWUNMTRS), ( ( 17, 6),
NXANTSHIRRAZEW TJAVEUZVICINWDTABLNRHAFWZVLLFJIXNIWFFLBTICVBRFUNMMTRAZEW TJAVEUZ), ( ( 9, 22),
RHERL MXWNNEFA I LVEJAKFJWCWRIBLEDTRNXEZIFJTZVWHRWIZZTDLWCJDNZKRSSLNEFA I LVEJAKF), ( ( 3, 7),
EAREMPWTSSRUFDMQRGFJUGTLTEDIMROKESWRCDUGKKCQTAETDCCKOMTLGOSCEJHHMSRUFDMQRGFJU), ( ( 23, 24),
TXGTLIBEFFGDSULHGRSDREMETUPLGJNTFBGVUDRNNVHEXTEUUVVNJLEMRFVOTQQLFGDSULHGRSD), ( ( 7, 12),
BDOBXCFAHHTU I X VONUSTNAEABIZXOJLBHFOPITNLLPVADBAIPPLJXAENJHPSBGGXHOTU I X VONUST), ( ( 11, 25),
QWDQETCNIIIDSVLEYDAVPSANZNLKEDOUQICDGLSAUUGYNWQLGGUOENZA OIGPQFFEDSVLEYDAVPS), ( ( 3, 1),
GCTGORYVUUTWHFOSTIHLWIVNVGFKOTQMGUYTEFWIMMESVCGVFEEMQOVNIQUELGJJOUTWHFOSTIHLW), ( ( 7, 9),
UWHUQYVYTA AHMNBQOHGNLMGTXTUBSQCEUAYHIBMGEEIOTWUTBIIECQTXGCAILUZZQAHMNBQOHGNLM), ( ( 7, 13),
MOZMINQLSSZEFTIGZYFDEYLP LMTKIZUWMSQZATEYWWAGLOMLTAAWU I L P YUSADMRRISZEFTIGZYFDE), ( ( 9, 2),
ZPMZTUFEVVMNIQTDMRISNREKEZQJTLMBZVFMHQNRBBHDEPZEQHHLTEKRLVHSZAA TVMNIQTDMRISN), ( ( 9, 6),
NDANHITSJJABWEHRAFWGBFYSYNEXHAZPNJTAVEBFPPVRSDNSEVVPZHSYFZJVGNOOHJABWEHRAFWGB), ( ( 3, 4),
FBSFNQXUTTSVGENRSHGVHUMUFEJNSPLFTXSDEVHLLDRUBFUEDDLPNUMHPTDKFIINTSVGENRSHGV), ( ( 25, 19),
ANNACTYHKKNE XDCQNULXLEUHFHADOCNWI AKYNGDEUIIGQMAHDGGIWCHEFWKGLARRCKNE XDCQNULXLE), ( ( 1, 21),
YMLYWFAR00LUBVWILEBNUERTRYVKKWLCQYOALSVUEQQSIRMYRVSSQCWRTECOSNYHHWOLUBVWILEBNU), ( ( 15, 7),
GATGSDUJ00TEBLSYTWBHEWJXJGLMSTICGOUTLEWCCQYJAGJLQQCISJXWIOQHGRRSOTEBLSYTWBHE), ( ( 1, 15),
ESRECLGXUURAHBCORKHTAKXZXEBCRIWEUGRYBAKWYXSEXBYWICXZKIUYTENNCURAHBCORKHTA), ( ( 19, 15),
SQFSWRO TMMFAZLWYFGZBAGTPTSLUWFKISMOFELAGIIEYTQSTLEEIKWTPGKMEBSNNWMAZLWYFGZBA), ( ( 17, 19),
AKNAGFUVEENMRJGWNIRHMI V PVAJQGN OYAEUN SJMIYYSWVKAVJSSYOGVPI OESH AZZGENMRJGWNIRHM), ( ( 15, 24),
RLERDOFUZZEPMDJEHMSPHUIURWXDETNRZFEWBPHNNBJULRUWBN TDU IHTZBSRCCDZEPMDJEHMSP), ( ( 25, 10),
RDERTKPYBBEVOU THELOCVLWYWRUF TENZRBPEXUVLZZXHYDRYUXXZNTYWLNBXCRIITBEVOU THELOCV), ( ( 23, 21),
SWFSKHAD EEF CRTKGFQRNCQDL DSTOKFIMSEAFUTCQMMUGDWSDTUUMIKDLQIEUNSPKFCRTKGFQRNC), ( ( 19, 9),
GETGKFC HAAATONZKMTUNPOUHDHGZIKTYWGACTS ZOUWWSMHEGHZSSWKHDUYASPGBBKATONZKMTUNPO), ( ( 17, 9),
WGJWC BQRAAJINFC SJENDIERLRFWMCJKUWAQJOFTEUUSRGWRFOOUKCRLEKAODVVC AJINFC SJENDI), ( ( 25, 25),
GSTGIZENQQTKDJ IWTADRKANLNGJUITCOGQETMJKAO0MWN SGNJMMOCINLACQMRGXXIQTKDJ IWTADRK), ( ( 7, 15),
IKVIEJMH00VABPECVUBZAUHLHIPGEVQSIOMVWPAUSSWCHKIHPWWSQEHLUQOWZINNEOVABPECVUBZ), ( ( 5, 23),
UCHUELKDSSHOFJEW HQFXOQD TDUJMEHAIUSKHYJQOIIYWD CUDJYYIAEDTQAS YXUBBESHOFJEW HQFXO), ( ( 3, 17),
SOF SADKHGGF ITRAEFUTXIUHZHSRWAFCYS GKFR IUYQEHOSH RQYCAHZUCGQXSVVAGFITRAEFUTXI), ( ( 15, 9),
SMFSEPGVA AFQNXEKFINTQIVJVSXYEFUOSAGFCXQIOOCKVMSVXCCOUEVJ IUA CTSDDEAFQNXEKFINTQ), ( ( 7, 17),
EGREAFIDKKRWXLA YRQXVWQDDEL CARMOEKIRSLWQ00SYDGEDLSSOMADHQMKSV EJJAKRWXLA YRQXVW), ( ( 19, 11),
KIXK0JGLEEXSRDQX YRTSYLHLKDMOXCAKEGXWDSYAAWQLIKLDWWACOLHYCEWTKFFOEXSRDQX YRTS), ( ( 5, 2),
TBGTDKJCRRGNEIDVGPENPCSCITLDGZHTRJGXINPHXVCBCTCIXXHZDCSPZRXTAADRNEIDVGPENW), ( ( 5, 12),
RZERBIHAPPELCGBTENCULNAQARGJBEXFRPHEVGLNFFVTAZRAGVVF XBAQNXPVURYYPPELCGBTENCUL), ( ( 15, 13),
QKDQCNETYYDOLVCIDGLROGHTQVWCDSMQYEDAVOGMMAITKQTVAAAMSC THGSYARQBBCYDOLVCIDGLRO), ( ( 25, 23),
EQREGXCL00RIBHGURYBPIYLJLEHSGRAMEOCRKHIMMKULQELHKKMAGLJYAOKPEVVGORIBHGURYBPI), ( ( 1, 25),
UIHUSBWNKKHQXRSEHAXJQANPNURGSHYMUUKWHORQAMOENIUNROOMYSNPA YK0JUDDSKHQXRSEHAXJQ), ( ( 1, 8),
LZYLJSNEBBYHOIJVYROAHREGELIXJYDPLBNYFIHRDDFVEZLEIFFDPJEGRPBFALUUBJYHOIJVYROAH), ( ( 23, 1),
UYHUMJCFGGHETVMIHSTPESFN FUVQMHKOUGCHWVES00WIF YUFVWVWOKMFSKGPURRMGHETVMIHSTPE), ( ( 1, 2),
RFERP YTKHHENUOPBEXUGNXMKKRODPEVJRHTELONXJL B KFRKOLLJVPKMXVHLGRAAPHENUOPBEXUGN), ( ( 11, 16),
FLSFTIRCCXSHKATNSPKEHPCOCAFZTSDJFXRSVAHPJJVNLCLFC AVVJDT COPDXVEFUUTXSHKATNSPKEH), ( ( 11, 7),
UAHUIXGRMMHWZPICHEZTWERDRUPOIHSYUMGHKPWEYKCR AURPKKYSIRDESMKTUJJIMHWZPICHEZTW), ( ( 11, 1),
EKRESHQBWRGJZSMROJ DGOBNBEZYSRCIEWQRUZGOI IUMBKEBZUUCSBNOCWUDETTSWRGJZSMROJ D G), ( ( 17, 3),
EOREKJYZIIRQV NKARMVLQMTZTZENUKRSC E IYRW NQMCWA ZOEZNNWCSKZTMSIWL EDDKIRQV NKARMVLQ), ( ( 17, 12),
FPSFLKZAJJSRWOLBSNWMR NAUAF0VLSDFJZSXORNDDXBAPFAOXD TLAUNTJXMFEELJSRWOLBSNWMR), ( ( 11, 14),
RXERFUD0JJETW MFZEBWQTB0AORMLFEPVRJDEHMTBVVHZOXROMHHVFPF0ABPJHQRGGFJETW MFZEBWQT), ( ( 23, 18),
RVERJGZCDDEBQ SJFEPQMBPCKCRSNJEHLRDZETSBLLTFCVRCSTTLHJCKPHDTMR00JDEBQ SJFEPQMB), ( ( 5, 5),
```

Ranking_Chisquare(self,Cipher):



```
[((5, 25), EMREOVUNCCRYPTOGRAPHYANDNETWORKSECURITYASSIGNMENTIISKONDAKHELLOCRYPTOGRAPHY), ((23, 1),
UYHUMJCFGGHETVMIHSTPESFNFUVMHKOUGCHWVESOOWIFYUVVWOKMFNSKGPURRMGHETVMIHSTPE), ((25, 17),
YKLYARWFIILCVBAOLSVJCSDFYBMLUGYIWLBEBCSGGEOFKYFBEEGUAFDSUIEJYPPAILCVBAOLSVJCS), ((3, 4),
FBSFNQUTTSVGENRSHGKVHUMUFEJNSPLFTXSDEVHLLDRUBFUEDDLPNUMHPTDKFIINTSVGENRSHGKV), ((19, 3),
USHUYTQVOOHCBNYAHIBDCIVRVUNWYHMKUOQHGNCIKKGAVSUUVGGKMYVRIMOGDUPPYOHCBNYAHIBDC), ((21, 3),
CUPCSLMTEEPIRNSAPGRZIGTDTCNKSPWOCEMPYNIIGOOYATUCNTNYOWSTDGWEYZCVVSEPIRNSAPGRZI), ((25, 23),
EQREGXCLORIBHGURYBPIYLJLEHSGRAMEOCRKHIIYMMKULQELHKKMAGLJYAOKPEVVGORIBHGURYBPI), ((9, 19),
AQNAUVGFVWNOJRUENSJTOSFLFARKUNMCAWGNIROSCIEFQAFRIICMUFLSMWITABBUWNOJRUENSJTO), ((7, 25),
OQBOKPSNUUBGHVIBAHFGANRNOVMKBWYOUSBCVGAAYCINQONVCCYWKNAWUCFOTTKUBGHVIBAHFG), ((5, 3),
YGLYIPOHWWLSJNIALUJBSUFXHYNQILEMYWOLCNSUMMCAHGYNCCMEIHUEWCYFFIWLJSJNIALUJBS), ((25, 4),
LXYLNEJSVVYPIONBYFIWPFSLQZNYHTLVJYROPFTTRBSXLSORRTHNSQFHVRWLCNPNYPIONBYFIW), ((3, 1),
GCTGORYVUUTWHFOSTIHLWIVNVGFKOTQMGUYTEFWIMMESVCGVFEEMQOVNIQUELGJJOUTWHFOSTIHLW), ((17, 17),
UEHUAZOPYYYHGLDAQHCLBGCPJPUKHAHISUYOHMDGSSMQPEUPDMMSIAPJCIYMBUTTAHYHGLDAQHCLBG), ((1, 5),
OCBOMVQHEEBKRLMYBURDKUHJHOLAMBSGOEQBILKUGGIYHCOHLIIGSMHJUSEIDOXMEBKRLMYBURDK), ((23, 24),
TXGTLIBEFFGDSULHGRSODREMETUPLGJNTFBGVUDRNNVHEXTEUVVJLEMRJFVOTQQLFGDSULHGRSOD), ((3, 7),
EAREMPWTSSRUFDMQRGFJUGTLTEDIMROKESWRCDUGKCKQTAETDCCKOMTLGOSCEJHMSRUFDMQRGFJU), ((1, 11),
IWWIGPKBYVELFGSVOLXEODBIUGVMAIYKVCFEOAACSBBWIBFCAMGBDOMYCXIRRGYVELFGSVOLXE), ((19, 13),
OMBOSNKPIIBWVHSUBCVXWCLPQHQSGBGEOIKBAHWCEEAUPMOPHAAEGSPLCGIAXOJJSIBWVHSUBCVXW), ((21, 16),
PHCPFYZGRRCVEAFNCTEMVTGGQPAFCJBPZCLAVTBBLNGHFGALLBJFGQJRLMPJIFRCVEAFNCTEMV), ((15, 20),
TNGTFQHWBBGROYFLGJOURJWKWYTFZGVPFBHGDYRJPDLWNTWYDDPVFWKJVBDUTEFBBGROYFLGJOUR), ((1, 21),
YMLYWAROOLUBVWILEBNUERTRYVKWLQYOALSVEUQSIIRMYRVSQCRWTECOSNYHHWOLUBVWILEBNU), ((17, 19),
AKNAGFUVENMRJGWNIRHMIVPAJQGNQYAEUNSMJIYYSWVKAVJSSYOGVPIOSHAZZGENMRJGWNIRHM), ((11, 9),
IOVWLUFUAAVKNQDVSNHKSFRFIDCWVGMIAUVYDKSMYQFOFDYIMGWFRSGAYHIXXWAVKNDWQVSNHK), ((5, 12),
RZERBIHAPPELGBTENCULNAQARGJBEXFRPEVGLNFFVTAZRAVGFVXBAQNXPVURYBPELGBTENCUL), ((11, 8),
BHOBPENYSTTODGWPJOLGADLYKYBWVPOZFBTNRWDLFFRJJYHBYWRRFZPKLZTRABQQPTODGWPJOLGAD), ((5, 9),
CKPCMTSLAAPWNRMEPYNFWYLBLCRUMPIQCAASPRGWYQQGELKCLRGGQIMLBYIAGFCJJMAPWNRMEPYNFW), ((9, 4),
TJGTNOZYPHGCKNXGLCMHLYEYTKDNGFVTPZGBKHLVVBXYJTYKBBVFNELFPBMTUUNPGHCKNXGLCMH), ((15, 22),
FZSFRCTINNSDAKRXSVAAGDVIIWIFKLRSHBNTSPKDVBBPZIFIKPPBHRHIVWHPGFQQRNSDAKRXSVAAG), ((11, 7),
UAHUIXGRMMHWZPICHEZTWERDRUPOIHSYUMGHKPWEYKCAURPKKYSIRDESMKTUJJIMHWZPICHEZTW), ((19, 15),
SQFSWROTMFAZLWYFGZBAGTPSLUWFKISMOFELAGIIEYTSLEEKWTPGKMEBSNNWMAZLWYFGZBA), ((7, 15),
IKVIEJMHOOVABPECVUBZAUHLHIPGEVQSIOMVWPAUSSWCHKIHPWWSQEHUQUOWZINNEOVABPECVUBZ), ((1, 24),
VJIVTCXOLLIRYSTFIBYKRBOQVSHITZNVLXIPSRBNPNFQJVOVSPNZTQOZBLPKVEETLIRYSTFIBYKR), ((23, 17),
IMVIAIXQTUUVSHJAWVGHDSGTBTIJEAVYCIUQVKJSGCCKWTMTIJKKCYATBGYUKDIFFAUVSHJAWVGHDS), ((25, 20),
BNOBDUZILLOFYEDROVYMFVIGIBEPDOXJBLZOHFVJJHRINBIEHHJXDIGVXLHMBSSDLOFYEDROVYMF), ((21, 9),
YQLYOHIPAALENJOWL CNVECPZPYJGOLSKYAILUJJECKKUWPQYPUUKSOPZCSAUVYRROALENJOWL CNVE), ((7, 2),
VXIVRWZUBBINOCRPIHOMNHUYVCTRIDFVBIJCNHFFJPUXVUCJFDRUYHDBJMVAAARBINOCRPIHOMN), ((21, 22),
LDYLBUCVNNYRAWBJYPAIRPCMCLWTFYXNLNVYHWRPXXHJCDLWXXXFBCEMFPNHILEEBNRAWBJYPAIR), ((9, 6),
NDANHITSJJABWEHRAFVGBFYSYNEXHAZPNJTAVEBFPPVRSDNSEVVPZHSYFZJVGNOOHJABWEHRAFVGB), ((15, 17),
OIBOALCRWWMJTAGBEJPMERFROTUABQKOWCBYTHEKKYGRIORTYKQARFEQWYPOZZAWBMJTAGBEJPM), ((1, 8),
LZYLJSNEBBYHOIJVYROAHREGELIXJYDPLBNYFTHRDDFVEZLEIFFDPJEGRPBFALUJBYHOIJVYROAH), ((1, 4),
PDCPNWRIFCLSMNZCVSELVIKIPMBNCTHPFRCLMHHJZIDPIMJHTNIKVTFJEPYFNCLSMNZCVSEL), ((23, 25),
CGPCURKNOPMBDUQPABXMANVNCYUPSWCOKPEDMAWWEQNSUNVASOEXCZUOPMBDUQPABXM), ((19, 0),
BZOBFAACVVOJUIFHOPIKJPCYCBUDFOTRBYXONUJPRNRHCZBUNNRTFCYPTVNBKWWFVOJUIFHOPIKJ), ((19, 19),
AYNAEZBUUNIHTEGNOHJIOBXBATCENSQAUNWMTIOQQMGYABTMMQSEBXOSUMJAVVEUNIHTEGNOHJI), ((15, 15),
CWPQZQFKKPAKHOUPSXDAFTECHIOPEYCKQPMHASYYMUFWCFHMYEOTSEKMDCNNOKPAXHOUPSXDA), ((17, 21),
GQTGLMABKKTSPMCTOXNSOVBGPWMTUEGKATYPSOEEYCBQGBPYEUMBOUKYNGFFMKTSPMCTOXNS), ((21, 13),
EWREUNOVGGRKTPUCRITBKIVFVEMURYQEGORAPKIQACVWEVPAAYUVFIYGABEXXUGRKTUCRITBK), ((15, 23),
YSLYKVMGGGLWTDKQLOTZWBOPBYDEKLAUYGMLIDWOUUIQBSYBDIIUAKBPOAGIZYJJKGLWTDKQLOTZW), ((25, 19),
AMNACTYHKKNEXDCQNUXLEUHFHADOCNWIAYNGDEUIIGQMAHDDGGIWFHUKGLARRCKNEXDCQNUXLE), ((3, 6),
NJANVYFCBBADOMVZAPOSDDPCUCNMVAXTNBFALMDPTTLZCJNCMLLTXVCUPXBLSNQVBBADOMVZAPOS), ((21, 5),
SKFISBCJUUFIYHDIQFWHPYJWJTJSDAIFMESUCFODYWEEOQJKSDO0EMIJTWMUOPLLUIFYHDIQFWHPY), ((25, 1),
IUVIKBGPSSVMFLKYVCFMCPNPIWVVEQISGVOLMCQQYUPLI00QEKPNCEOTIZZKSSVMFLKYVCFM), ((21, 0),
RJRERHABITTEXGCHPEVGOXVISIRCZHELDRTBENCXVDDNPIJRICNNDLHISVLTNRKKHTTEXGCHPEVGOX), ((19, 9),
```

4.3 Download link

www.emreovunc.com/CE340/EmreOvunc-Assignment2.zip

MD5: 9ba2db1f3f0f5ba7780e2b79ad1d9075

SHA1: 7ffa0f5b7ee53c84ed11042bf6e9fb8eea196395