

CS 5413: Cryptography and network security

Hardil Mehta (0898141)



2019

CONTENTS

Specifications:	2
Assignment Task 1:.....	3
Explanation of code (Encryption program).....	4
Explanation of code (Decryption program)	4
Output(encryption):.....	4
Output(decryption)	5
Assignment Task 2:.....	5
Explanation of code (Encryption program).....	5
Explanation of code (Decryption program)	5
Output (Encryption)	6
Output(Decryption)	7
Assignment Task 3:.....	7
Idea of Program	7
Ouput:	8

SPECIFICATIONS:

Language used: Python 3.6.8

Software used for compilation: IDLE (Python 3.4 GUI 64 bit)

Operating System: Windows 10

ASSIGNMENT TASK 1:

Write computer programs for the Substitution Cipher based on Z29 which is corresponding to 26 alphabetic characters (0 - 25), space (26), and “,” (27) “.”(28). The key is a random permutation π on Z29. Write down encryption and decryption programs. Select a paragraph of text (I don't think any two people will choose a same paragraph if they choose independently) and encrypt it using your encryption algorithm. Then use your decryption program to check the correctness. You can use Java, C or other computer languages. Record your plaintext, ciphertext and the key π in your answer sheet

ANSWER:

Alphabet represents the z29 space corresponding to the all the characters and space and comma and full-stop.

alphabet = " ABCDEFGHIJKLMNOPQESTUVWXYZ.,"

The π is also in Z29 space and the key for encryption of data is as the following:

key = "FPJVRKDWAEZ,BSGMTYICXQOLHU.N "

Plaintext:

“During the first part of your life, you only become aware of happiness once you have lost it. Then an age comes, a second one, in which you already know, now when you begin to experience true happiness, that you are, at the end of the day, going to lose it. When I met Belle, I understood that I had just entered this second age. I also understood that I hadn't reached the third age, in which anticipation of the loss of happiness prevents you from living.

CipherText:

Rqregwfxakfdercxftprxfmdfumqrfbedkfumqfmgbufjkmvskfplprkfmdfaptteggkccfmvgkfumqfapokfbmcxfe
xnfXakgfpwkvmskcfpfckvmgrfmgkfegflaevafumqfprkpruf,gmlfpxfxakfsmkgxflakgfumqfjkwegfxmfk
htkrekgvxfxrqkfaptteggkccfxapxfumqfprkfpfxakfkgrfmdfxakfrpufwmegwfxmfbmckfexnfLakgfEfskxfJkbbk
EfqgrkrxmmrxfapxfEfaprfzqcxfgkxkrkrfxaecfckvmgrfpwknfEfpbcmfqqgrkrxmmrxfapxfEfaprg'xfrkpvakrfx
akfxaerrfpwkvfegflaevafpgxevetpxemgmdfxakfbmccfmdfaptteggkccftrkokgxcfumqfdrmsfboegwn

EXPLANATION OF CODE (ENCRYPTION PROGRAM)

As shown in the code, both alphabet and key space are defined.

NOTE: For simplicity all the text is converted to uppercase for simplified encryption program.

def encrypt function: Takes an argument "Message". The translated variable is initialized as empty which stores the encrypted message. A For loop is used to traverse through the whole string of message. It takes individual character and searches its index value in alphabet. After getting the index from alphabet the same index value is used and the value from KEY is stored in variable "translated". At the end encrypted value is returned by the function

- ⇒ User input i.e. message is taken from terminal and is encrypted using the above-mentioned function.
- ⇒ This encrypted message is stored in a file for decryption by decrypting file

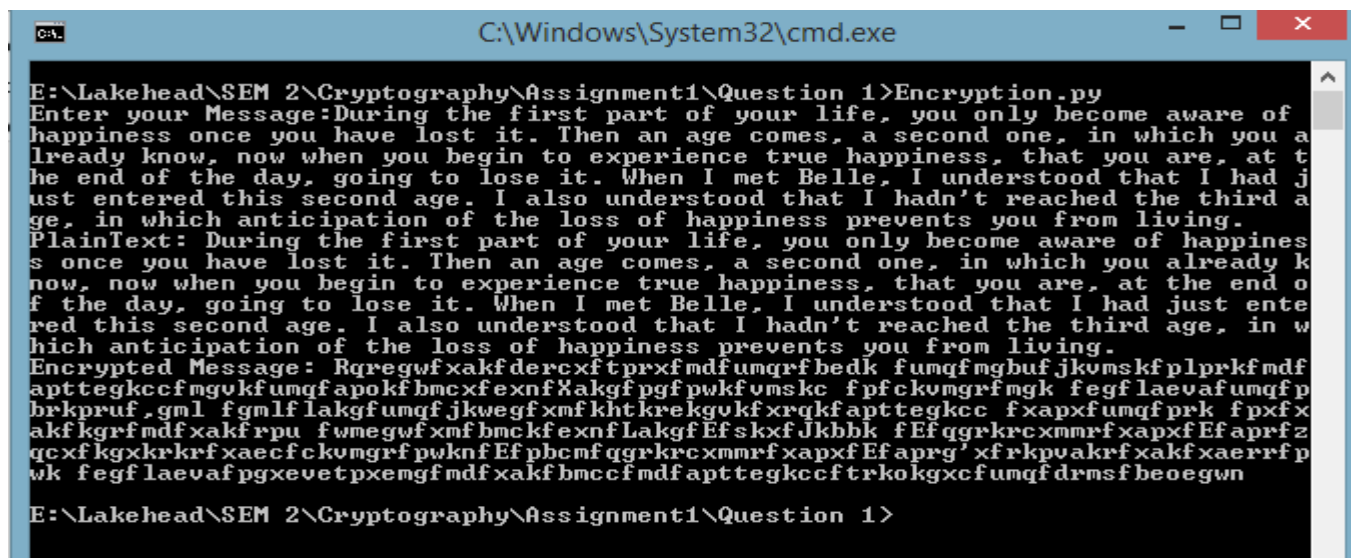
EXPLANATION OF CODE (DECRYPTION PROGRAM)

The decryption Program uses the key for decrypting the encrypted text.

Def decrypt function: Decrypt function takes an argument "Message". Its reverse engineers the encrypt function. It searches for the index value of the character in key and uses that index value to find the real character in alphabet.

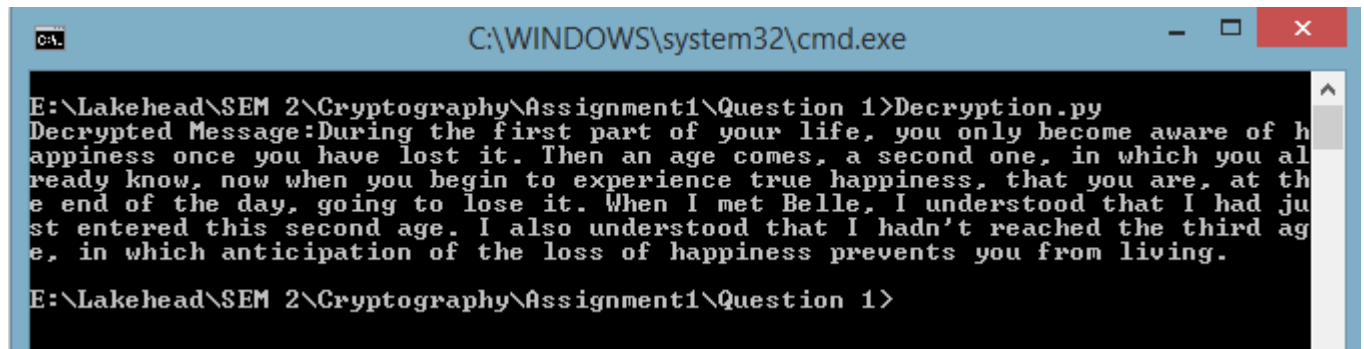
- ⇒ The decrypting program get the encrypted message from the file and uses decrypting function to decrypt the message.
- ⇒ The decrypt function decrypts the message and its printed out on the terminal.

OUTPUT(ENCRYPTION):



```
E:\Lakehead\SEM 2\Cryptography\Assignment1\Question 1>Encryption.py
Enter your Message:During the first part of your life, you only become aware of
happiness once you have lost it. Then an age comes, a second one, in which you a
lready know, now when you begin to experience true happiness, that you are, at t
he end of the day, going to lose it. When I met Belle, I understood that I had j
ust entered this second age. I also understood that I hadn't reached the third a
ge, in which anticipation of the loss of happiness prevents you from living.
PlainText: During the first part of your life, you only become aware of happines
s once you have lost it. Then an age comes, a second one, in which you already k
now, now when you begin to experience true happiness, that you are, at the end o
f the day, going to lose it. When I met Belle, I understood that I had just ente
red this second age. I also understood that I hadn't reached the third age, in w
hich anticipation of the loss of happiness prevents you from living.
Encrypted Message: Rqregwfxakfdercxftprxfmdfumqrfbedk fumqfmgbuf jkvmkskplprkfmf
aptteggkccfmvgkfumqfapokfbmcxfexnfXakgfpfgfwkfvmksk fpfckvmgrfmgk fegflaevafumqfp
brkpruf,gml fgmfl lakgfumqf jkwegfxmflkhtkrekgykfxrqqkaptteggkcc fxapxfumqfprk fpxfx
akflgrfmdfxakfrpu fvmegwfxmfbmckfexnflakgfEfskoxfJkbbk fEfqqrkrcxmmrfxapxfEfaprfz
qcxflkgxkrkrfxaecfckvmgrfpwknfEfpbcmfqqrkrcxmmrfxapxfEfaprg'xfrkpvakrfxakfxaerrfp
wk fegflaevafpgxevetpxengfmdfxakfbmccfmdfaptteggkccftrkoikgxcfumqfdrmsfboegwn
E:\Lakehead\SEM 2\Cryptography\Assignment1\Question 1>
```

OUTPUT(DECRYPTION)



```
C:\WINDOWS\system32\cmd.exe

E:\Lakehead\SEM 2\Cryptography\Assignment1\Question 1>Decryption.py
Decrypted Message:During the first part of your life, you only become aware of happiness once you have lost it. Then an age comes, a second one, in which you already know, now when you begin to experience true happiness, that you are, at the end of the day, going to lose it. When I met Belle, I understood that I had just entered this second age. I also understood that I hadn't reached the third age, in which anticipation of the loss of happiness prevents you from living.

E:\Lakehead\SEM 2\Cryptography\Assignment1\Question 1>
```

ASSIGNMENT TASK 2:

Write computer programs for the Permutation Cipher based on Z29 as in Problem 1. In encryption program, the inputs are a value of m (the size of permutation), a permutation as the key and the plaintext, and the output is the ciphertext. Write the decryption program accordingly. Try your programs by some text. Note that since m and the length of plaintext is not fixed, paddings might be added to the end of plaintext by the program. You may think about what kind padding is better for the security and design your paddings.

ANSWER:

In permutation cipher an input of permutation size is taken.

EXPLANATION OF CODE (ENCRYPTION PROGRAM)

def GenerateKey(m) function: The function takes “ m ” the permutation size as input. The function generates an array of range (m) i.e. if m is 5 then key is generated [1,2,3,4,5]. And Then the key is randomly shuffled.

The code takes user input and stores it as plaintext.

- ⇒ $Y = (m - \text{len}(\text{plaintext}) \% m)$ is used to know if padding is required or not.
- ⇒ Then \$ is added as padding.
- ⇒ Next the string is divided and blocks are generated where each block is of length m .
- ⇒ Each block is encrypted using the key generated by the encryption program.
- ⇒ A for loop is used and the index value of key is used to encrypt the message.
- ⇒ This encrypted message is stored on the file and key is stored in a different file to be sent via the secure channel as discussed in the lecture notes.

EXPLANATION OF CODE (DECRYPTION PROGRAM)

Def getKey() function: gets the key from the stored file.

Def getencryptedmessage() function: gets the message from the file and stores it in encrypted_message variable.

- ⇒ Key variable has the key and encrypted message is stored in Encrypted_message.
- ⇒ We find no of blocks to make and permutation number from length of key and size of encrypted message.
- ⇒ We divided the encrypted message in blocks of size m which is the permutation number using
`"block = [encrypted_message[i:i+permutation_number] for i in range(0, len(encrypted_message), permutation_number)]"`
- ⇒ Then each block is decrypted using the index value and finding its permutation in the key.

Lastly the plaintext is printed after decryption.

Output (Encryption)

```
E:\Lakehead\SEM 2\Cryptography\Assignment1\Question 2>Encryption.py
Enter the permutation Size:5
[0, 1, 2, 3, 4]
[0, 3, 2, 1, 4]
Enter your Message:During the first part of your life, you only become aware of
happiness once you have lost it. Then an age comes, a second one, in which you a
lready know, now when you begin to experience true happiness, that you are, at t
he end of the day, going to lose it. When I met Belle, I understood that I had j
ust entered this second age. I also understood that I hadn't reached the third a
ge, in which anticipation of the loss of happiness prevents you from living.
Duringthefirstpartofyourlife,youonlybecomeawareofhappinesonceyouhave lost it.Then
anagecomes,asecondone,inwhichyoualreadknow,nowwhenyoubegintoexperiencetruehappi
ness,thatyouare,attheendoftheday,goingt lose it.WhenImetBelle,IunderstoodthatIhad
justenteredthissecondage.Ialso understoodthatIhadn't reachedthethirdage,inwhichant
icipationofthelossofhappinesspreventsyoufromliving.
Duringthefirstpartofyourlife,youonlybecomeawareofhappinesonceyouhave lost it.Then
anagecomes,asecondone,inwhichyoualreadknow,nowwhenyoubegintoexperiencetruehappi
ness,thatyouare,attheendoftheday,goingt lose it.WhenImetBelle,IunderstoodthatIhad
justenteredthissecondage.Ialso understoodthatIhadn't reachedthethirdage,inwhichant
icipationofthelossofhappinesspreventsyoufromliving.
['Durin', 'gthe', 'irstp', 'artof', 'yourl', 'ife,y', 'ouonl', 'ybeco', 'meawa',
'reofh', 'appin', 'esson', 'ceyou', 'havel', 'ostit', 'Then', 'anage', 'comes',
'asec', 'ondon', 'e.inw', 'hichy', 'oualr', 'eadyk', 'now,n', 'owwhe', 'nyou',
'b', 'egint', 'oexpe', 'rienc', 'etrue', 'happi', 'ness', 'thaty', 'ouare', 'at',
'th', 'eendo', 'fthed', 'ay.go', 'ingto', 'losei', 't.Whe', 'nImet', 'Belle', 'I',
'und', 'ersto', 'odtha', 'tlhad', 'juste', 'ntere', 'dthis', 'secon', 'dage', 'I',
'also', 'under', 'stood', 'thatI', 'hadn', 'treac', 'hedth', 'ethir', 'dage', 'I',
'inwhi', 'chant', 'icipa', 'tiono', 'fthel', 'ossof', 'happi', 'nessp', 'reven',
'tsyou', 'froml', 'iving', '.$$$$']
Dirungehtfitsrpaotrfrfyrul,efyonoulycebomwaeafoeaippneossncoyeuhevaloist.ehIn
aganecemos,esacoodnneni,whhciyolaureydakn,wonohwenuoybenigtopxeerneiceurtehppai
nsse,ttahyoraue,ttahedneofehtdag,yoitgnolesoithW.enemItBllee,nuldetsroohtdatahId
jtsuenretedihtssocendega.Islaouednrsootdttahlhnda'taerchtdeheihtrdega,iwhnicnaht
ipicatnoiofehtloosfhhppainssepreventoyufmorlinivg.
$$$$$
```

Encrypted Data - Notepad

```
File Edit Format View Help
Dirungehtfitsrpaotrfrfyrul,efyonoulycebomwaeafoeaippneossncoyeuhevaloist.ehInaganecemos,esacoodnneni,whhciyolaureydakn,wonohwenuoybenigtopxeerneiceurtehppainsse,ttahyoraue,ttahedneofehtdag,yoitgnolesoithW.enemItBllee,nuldetsroohtdatahIdjtsuenretedihtssocendega.Islaouednrsootdttahlhnda'taerchtdeheihtrdega,iwhnicnahtipicatnoiofehtloosfhhppainssepreventoyufmorlinivg.
$$$$$
```

Output(Decryption)

```
E:\Lakehead\SEM 2\Cryptography\Assignment1\Question 2>Decryption.py
['0', '3', '2', '1', '4']
Dirungehtfitsrpaotrfyruoli,efyonoulycebomwaeearfoehaippneossncoyeuhevaloistst.ehIn
aganecemos,esacoodnneni,whhciyolaureydakn,wonohwwenuoybenigtopxeerneiceurtehppai
nsse,ttahyoraue,ttahedneofehtdag,yoitgnolesoithW.enemItBlee,nuldetsroohtdatahId
jtsuenretedihssocendega.IslaouednrsootdtthahIhnda'taerchtdeheihtrdega,ihwnicnaht
ipicatnoiofehtloosffhppainssepreventoyusufmorlinivg.$$$$
75
['Dirun', 'gehtf', 'itsrp', 'aotrf', 'yruol', 'i,efy', 'onoul', 'ycebo', 'mwaea',
 'rfoeh', 'aippn', 'eossn', 'coyeu', 'heval', 'oitst', 'ehIn', 'agane', 'cemos',
 'esac', 'oodnn', 'eni,w', 'hhciy', 'olaur', 'eydak', 'n,won', 'ohwwe', 'nuoy',
 'benigt', 'opxee', 'rneic', 'eurte', 'hppai', 'nsse', 'ttahy', 'oraue', 'tt',
 'ah', 'edneo', 'fehtd', 'ag,yo', 'itgno', 'lesoi', 'thW.e', 'nemIt', 'Blee', 'n',
 'uld', 'etsro', 'ohtda', 'tahId', 'jtsue', 'nrete', 'dihts', 'socen', 'dega', 'I',
 'slao', 'uednr', 'sootd', 'ttahI', 'hnda', 'taerc', 'htdeh', 'eihtr', 'dega', 'I',
 'ihwni', 'cnaht', 'ipica', 'tnoio', 'fehtl', 'oosff', 'hppai', 'nssep', 'reven',
 'toysu', 'fmorl', 'inivg', '.$$$$']
Duringthefirstpartofyourlife,youonlybecomeawareofhappinessonceyouhave lost it.Then
anagecomes,asecondone,inwhichyoualreadyknow,nowwhenyoubegintoexperiencetruehappi
ness,thatyouare,attheendoftheday,goingtoloseit.WhenImetBelle,IunderstoodthatIhad
justenteredthissecondage.IalsounderstoodthatIhadn'treachedthethirdage,inwhichant
icipationofthelossofhappinesspreventsyoufromliving.$$$$
E:\Lakehead\SEM 2\Cryptography\Assignment1\Question 2>
```

ASSIGNMENT TASK 3:

Read “2.5 The Vegene`re Cipher” of the lecture notes posted in course web carefully and try to understand the materials in this subsection. Then solve the following problem: The following is a piece of ciphertext which is encrypted by Vegene`re Cipher.

cjnpkgrlilqawbnuptgkerwxuzviaiysxckwdntjawhqcutttvpewtrpgvcwlkkkgczafsihrimixukrwxrfmgfgkfxgukpjvvzmc
mjvawbnuptgcicvxxvgczkekgcbchvnrqhhwiadfrcyxgvzqqtvubdguvttkccdpvvpfphftamzxqwertgukcelqlrxgvycwtncbjk
keerecjihvrjzpkkfexqgjtjpfupemswwxjxqzpjtxkvlvyaemwhovudkmnfxegfrwxtद्याiecyhlgjfpogymbxyfpzxxvpngk
xfitnkfdniyrwxukssxpqabmvkgcbciagpadfrcyxgvvyimjvwpgkscwbpurwxqkftkorrrwvnrqhxurllsgvjxmvmccraceathhtf
pmeygczwguttvtv katmcvgiltwscmjmvgyghitfazodkbf

IDEA OF PROGRAM

The code first reads the encrypted message and stores it in word. The code uses 4 function.

1. **Def getfrequency(word):** This function gets the frequency of each word in the string given in the argument. This function is used to calculate the frequency for index of coincidence.
2. **Def frequency(word):** This function calculates the frequency value for Mutual index of coincidence.
3. **Def function correlation(word):** This function matches the frequency pattern of the word and uses it to calculate the mutual index of correlation.
4. **Def function calculateindex(y):** This function gets the value for calculating the value of index of coincidence for the argument y.

After defining the functions, the code runs as follows:

- ⇒ New variable joins the encrypted text together. i.e. it converts it to a string from list. (line 41)
- ⇒ This variable is now converted to single vector so that It can be converted to matrix format.
- ⇒ This tuple is now converted to a matrix
- ⇒ The matrix is reshaped and value (-1, m) is used to find the value of m.
- ⇒ After iterating m, we find that the value of m is 5.
- ⇒ The matrix is transposed to convert it to an column and then using the calculate index function each index of coincidence is calculated for each row of the column.
- ⇒ Here, we found out the value of m is 5.
- ⇒ We use this value to find the mutual index of coincidence using the function frequency().
- ⇒ A single for loop is used calculate the maximum coincidence factor for each value of l and j where the value is equivalent to ~0.065
- ⇒ The plaintext is generated using this equations generated from the maximum coincidence factor.
- ⇒ This decrypted value is stored onto a file.

OUTPUT:

```

C:\WINDOWS\system32\cmd.exe
E:\Lakehead\SEM 2\Cryptography\Assignment1\Question 3>question3.py
confidence Index of sentence1: 0.07155067155067155
confidence Index of sentence2: 0.07008547008547009
confidence Index of sentence3: 0.05299145299145299
confidence Index of sentence4: 0.059096459096459095
confidence Index of sentence5: 0.060073260073260075
Hence, The key length is 5
Equation 1: k<0>
Equation 2: k<1> = k<0> - 11
Equation 3: k<2> = k<0> - 4
Equation 4: k<3> = k<0> - 13
Equation 5: k<4> = k<0> - 9
Deciphered key is: CRYPT
PlainText:
a s p a r e a n t s o f c h i l d r e n i n t h e s i x t h g r a d e a t y o u
r s c h o o l w e a r e r e l u c t a n t l y w r i t i n g y o u t o p r o t e
s t t h e p o o r m e t h i n s t r u c t i o n t h e c h i l d r e n a r e g e
t t i n g i n m r j o k e s c l a s s o u r c o m p l a i n t i s b a s e d o n
s e v e r a l f a c t o r s m r j o k e o f t e n s t e p s o u t i n t h e h a
l l d u r i n g c l a s s t o t a l k w i t h p e o p l e w h o w a l k b y h e
a s s i g n s v i r t u a l l y n o h o m e w o r k w h i l e o t h e r m a t h
c l a s s e s h a v e h o m e w o r k e v e r y n i g h t a l t h o u g h t h e
s t u d e n t s l i k e m r j o k e t h e y c o m p l a i n t h a t t h e y a r
e b e h i n d t h e o t h e r m a t h c l a s s e s a n d s e e l i t t l e c h
a n c e o f c h a t c h i n g u p w e a r e v e r y c o n c e r n e d a b o u t
t h i s p r o b l e m m m m m
E:\Lakehead\SEM 2\Cryptography\Assignment1\Question 3>

```