# Applied Cryptography (UE20CS314)

## Lab-2

**Name:** Vishwa Mehul Mehta

**SRN:** PES2UG20CS389

**Section:** F

**Date:** 08/09/2022

1.



2a.



2b.

```
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> f = open('PES2UG20CS389.txt', 'r')
>>> text = f.read()
>>> f.close()
>>> text
'excited  about  his  newly-earned  powers,  midas  started  touching every surr
ounding objectslike stones, grass, treesandcart, turning each item into pure gol
d.but soon, midas became hungry. as he picked up a piece of food, he found he co
uldnot eat it. it had turned to gold in his hand\n'
>>> #he
>>> text.count('he')
3
>>> text.count('h')
10
>>> text.count('ed')
5
>>> text.count('oo')
2
>>> text.count('a')
15
>>> text.count('as')
4
>>>
```

3.

```
[09/08/22]seed@VM:~/AC_Lab$ grep 'he' PES2UG20CS389.txt
excited  about  his  newly-earned  powers,  midas  started  touching every surro
unding objectslike stones, grass, treesandcart, turning each item into pure gold
.but soon, midas became hungry. as he picked up a piece of food, he found he cou
ldnot eat it. it had turned to gold in his hand
[09/08/22]seed@VM:~/AC_Lab$
```

```
[09/08/22]seed@VM:~/AC_Lab$ grep 'h' PES2UG20CS389.txt
excited  about  his  newly-earned  powers,  midas  started  touching every surroundin
g objectslike stones, grass, treesandcart, turning each item into pure gold.but soon,
 midas became hungry. as he picked up a piece of food, he found he couldnot eat it. i
t had turned to gold in his hand
[09/08/22]seed@VM:~/AC_Lab$ grep 'ed' PES2UG20CS389.txt
excited  about  his  newly-earned  powers,  midas  started  touching every surroundin
g objectslike stones, grass, treesandcart, turning each item into pure gold.but soon,
 midas became hungry. as he picked up a piece of food, he found he couldnot eat it. i
t had turned to gold in his hand
[09/08/22]seed@VM:~/AC_Lab$ grep 'oo' PES2UG20CS389.txt
excited  about  his  newly-earned  powers,  midas  started  touching every surroundin
g objectslike stones, grass, treesandcart, turning each item into pure gold.but soon,
 midas became hungry. as he picked up a piece of food, he found he couldnot eat it. i
t had turned to gold in his hand
[09/08/22]seed@VM:~/AC_Lab$ grep 'a' PES2UG20CS389.txt
excited  about  his  newly-earned  powers,  midas  started  touching every surroundin
g objectslike stones, grass, treesandcart, turning each item into pure gold.but soon,
 midas became hungry. as he picked up a piece of food, he found he couldnot eat it. i
t had turned to gold in his hand
[09/08/22]seed@VM:~/AC_Lab$ grep 'as' PES2UG20CS389.txt
excited  about  his  newly-earned  powers,  midas  started  touching every surroundin
g objectslike stones, grass, treesandcart, turning each item into pure gold.but soon,
 midas became hungry. as he picked up a piece of food, he found he couldnot eat it. i
t had turned to gold in his hand
[09/08/22]seed@VM:~/AC_Lab$
```

4.

```
[09/08/22]seed@VM:~/AC_Lab$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> from util import *
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'pyszhljwkcdrnibxeoqamgvtuf'
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'gapkyqefmrvnthiwubolsjdczx'
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'pmrlyvdnkztbqjcghwsxoaifeu'
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'vcyplkbwdufjhaigzxrmoteqsn'
>>> generate_key('abcdefghijklmnopqrstuvwxyz')
'tklvsqxdnejcrobyhuiwfagpmz'
>>>
```

```
[09/08/22]seed@VM:~/AC_Lab$ cat util.py
def check_key_validity(key, alphabet):
    if len(key) != len(alphabet):
        return False
    if len(list(key)) != len(set(key)):
        return False
    return True

def generate_key(alphabet_string):
    import random as r
    l = list(alphabet_string)
    r.shuffle(l)
    return ''.join(l)
```

5.

```
[09/08/22]seed@VM:~/AC_Lab$ vi encrypt.py
[09/08/22]seed@VM:~/AC_Lab$ python3 encrypt.py
splnwsv  tkbfw  dni  osgcm-stuosv  ybgsui,  rnvti  iwtuwsv  wbfldnox sasum ifuubfovno
x bkeslwicnjs iwbosi, xutii, wussitovltuw, wfuonox stld nwsr nowb yfus xbcv.kfw ibbo,
 rnvti ksltrs dfoxum. ti ds ynljsv fy t ynsls bq qbbv, ds qbfov ds lbfcvobw stw nw. n
w dtv wfuosv wb xbcv no dni dtov

[09/08/22]seed@VM:~/AC_Lab$
```

```
[09/08/22]seed@VM:~/AC_Lab$ python3 encrypt.py > PES2UG20CS389_encrypted.txt
[09/08/22]seed@VM:~/AC_Lab$ cat PES2UG20CS389_encrypted.txt
splnwsv  tkbfw  dni  osgcm-stuosv  ybgsui,  rnvti  iwtuwsv  wbfldnox sasum ifuubfovno
x bkeslwicnjs iwbosi, xutii, wussitovltuw, wfuonox stld nwsr nowb yfus xbcv.kfw ibbo,
 rnvti ksltrs dfoxum. ti ds ynljsv fy t ynsls bq qbbv, ds qbfov ds lbfcvobw stw nw. n
w dtv wfuosv wb xbcv no dni dtov

[09/08/22]seed@VM:~/AC_Lab$
```

```
[09/08/22]seed@VM:~/AC_Lab$ cat encrypt.py
f = open('PES2UG20CS389.txt', 'r')
plaintext = f.read()
f.close()
ct = ''
alpha = 'abcdefghijklmnopqrstuvwxyz'
key = 'tklvsqxdnejcrobyhuiwfagpmz'
for i in range(len(plaintext)):
    if plaintext[i] not in alpha:
        ct += plaintext[i]
    else:
        i1 = alpha.index(plaintext[i])
        ct += key[i1]
print(ct)
```

6.

```
[09/08/22]seed@VM:~/AC_Lab$ vi decrypt.py
[09/08/22]seed@VM:~/AC_Lab$ python3 decrypt.py
enter the key: tklvsqxdnejcrobyhuiwfagpmz
excited  about  his  newly-earned  powers,  midas  started  touching every surroundin
g objectslike stones, grass, treesandcart, turning each item into pure gold.but soon,
 midas became hungry. as he picked up a piece of food, he found he couldnot eat it. i
t had turned to gold in his hand

[09/08/22]seed@VM:~/AC_Lab$
```

```
[09/08/22]seed@VM:~/AC_Lab$ cat decrypt.py
from util import check_key_validity
f = open('PES2UG20CS389.txt', 'r')
ct = f.read()
f.close()
pt = ''
alpha = 'abcdefghijklmnopqrstuvwxyz'
key = input('enter the key: ')
if not check_key_validity(key, alpha):
    print('key not valid')
else:
    for i in range(len(ct)):
        if ct[i] not in key:
            pt += ct[i]
        else:
            i1 = key.index(ct[i])
            pt += alpha[i1]
    print(pt)
```

7.

```
[09/08/22]seed@VM:~/AC_Lab$ vi encrypt.py
[09/08/22]seed@VM:~/AC_Lab$ python3 encrypt.py
Hfoxum, Mnvti xubtosv, "I'cc iwtuas! Psudtyi wdni gti obw ifld to splsccsow gnid tqws
u tcc!"...

[09/08/22]seed@VM:~/AC_Lab$
```

```
[09/08/22]seed@VM:~/AC_Lab$ python3 decrypt.py
enter the key: tklvsqxdnejcrobyhuiwfagpmz
Hungry, Midas groaned, "I'll starve! Perhaps this was not such an excellent wish afte
r all!"...

[09/08/22]seed@VM:~/AC_Lab$
```

```
[09/08/22]seed@VM:~/AC_Lab$ cat encrypt.py
f = open('new_input.txt', 'r')
plaintext = f.read()
f.close()
ct = ''
alpha = 'abcdefghijklmnopqrstuvwxyz'
key = 'tklvsqxdnejcrobyhuiwfagpmz'
for i in range(len(plaintext)):
    if plaintext[i] not in alpha:
        ct += plaintext[i]
    else:
        i1 = alpha.index(plaintext[i])
        ct += key[i1]
print(ct)
```

```
[09/08/22]seed@VM:~/AC_Lab$ cat decrypt.py
from util import check_key_validity
f = open('new_encrypt.txt', 'r')
ct = f.read()
f.close()
pt = ''
alpha = 'abcdefghijklmnopqrstuvwxyz'
key = input('enter the key: ')
if not check_key_validity(key, alpha):
    print('key not valid')
else:
    for i in range(len(ct)):
        if ct[i] not in key:
            pt += ct[i]
        else:
            i1 = key.index(ct[i])
            pt += alpha[i1]
    print(pt)
```

**notes.md:**

```
# Frequency Analysis
Letter Combination      Count
he                      3
h                       10
ed                      5
oo                      2
a                       15
as                      4

#Alphabet
`abcdefghijklmnopqrstuvwxyz`

#Plain Text
excited  about  his  newly-earned  powers,  midas  started  touching every surrounding objectslike stones,
 grass, treesandcart, turning each item into pure gold.but soon, midas became hungry. as he picked up a pi
ece of food, he found he couldnot eat it. it had turned to gold in his hand

#Substitution Text:
tklvsqxdnejcrobyhuiwfagpmz

#Cipher Text:
splnwsv  tkbfw  dni  osgcm-stuosv  ybgsui,  rnvti  iwtuwsv  wbfldnox sasum ifuubfovnox bkeslwicnjs iwbosi,
 xutii, wussitovltuw, wfuonox stld nwsr nowb yfus xbcv.kfw ibbo, rnvti ksltrs dfoxum. ti ds ynljsv fy t yn
sls bq qbbv, ds qbfov ds lbfcvobw stw nw. nw dtv wfuosv wb xbcv no dni dtov
```