

Cryptography with Python - Quick Guide

Cryptography with Python - Overview

Cryptography is the art of communication between two users via coded messages. The science of cryptography emerged with the basic motive of providing security to the confidential messages transferred from one party to another.

Cryptography is defined as the art and science of concealing the message to introduce privacy and secrecy as recognized in information security.

Terminologies of Cryptography

The frequently used terms in cryptography are explained here –

Plain Text

The plain text message is the text which is readable and can be understood by all users. The plain text is the message which undergoes cryptography.

Cipher Text

Cipher text is the message obtained after applying cryptography on plain text.

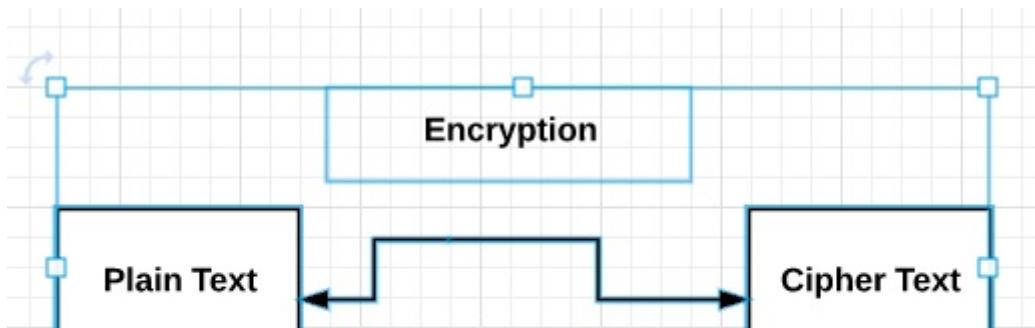
Encryption

The process of converting plain text to cipher text is called encryption. It is also called as encoding.

Decryption

The process of converting cipher text to plain text is called decryption. It is also termed as decoding.

The diagram given below shows an illustration of the complete process of cryptography –





Characteristics of Modern Cryptography

The basic characteristics of modern cryptography are as follows –

- It operates on bit sequences.
- It uses mathematical algorithms for securing the information.
- It requires parties interested in secure communication channel to achieve privacy.

Double Strength Encryption

Double strength encryption, also called as multiple encryption, is the process of encrypting an already encrypted text one or more times, either with the same or different algorithm/pattern.

The other names for double strength encryption include cascade encryption or cascade ciphering.

Levels of Double Strength Encryption

Double strength encryption includes various levels of encryption that are explained here under –

First layer of encryption

The cipher text is generated from the original readable message using hash algorithms and symmetric keys. Later symmetric keys are encrypted with the help of asymmetric keys. The best illustration for this pattern is combining the hash digest of the cipher text into a capsule. The receiver will compute the digest first and later decrypt the text in order to verify that text is not tampered in between.

Second layer of encryption

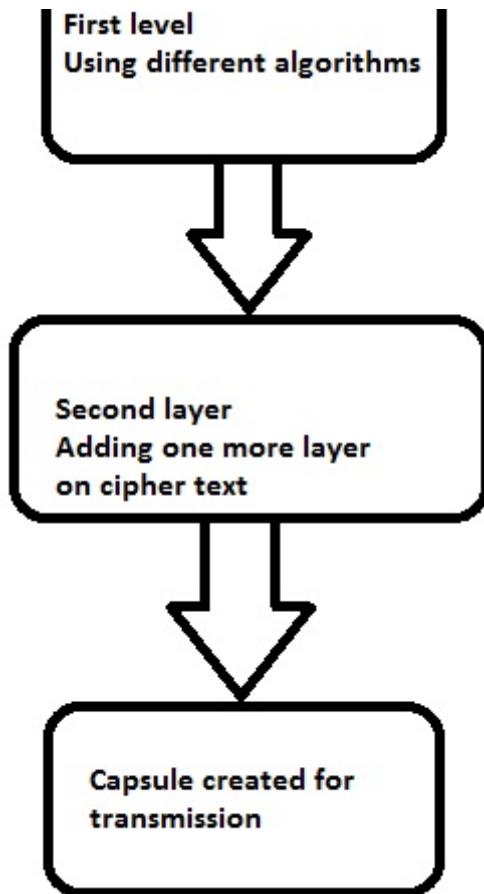
Second layer of encryption is the process of adding one more layer to cipher text with same or different algorithm. Usually, a 32-bit character long symmetric password is used for the same.

Third layer of encryption

In this process, the encrypted capsule is transmitted via SSL/TLS connection to the communication partner.

The following diagram shows double encryption process pictorially –





Hybrid Cryptography

Hybrid cryptography is the process of using multiple ciphers of different types together by including benefits of each of the cipher. There is one common approach which is usually followed to generate a random secret key for a symmetric cipher and then encrypt this key via asymmetric key cryptography.

Due to this pattern, the original message itself is encrypted using the symmetric cipher and then using secret key. The receiver after receiving the message decrypts the message using secret key first, using his/her own private key and then uses the specified key to decrypt the message.

Python Overview and Installation

Python is an open source scripting language which is high-level, interpreted, interactive and object-oriented. It is designed to be highly readable. The syntax of Python language is easy to understand and uses English keywords frequently.

Features of Python Language

Python provides the following major features –

Interpreted

Python is processed at runtime using the interpreter. There is no need to compile a program before execution. It is similar to PERL and PHP.

Object-Oriented

Python follows object-oriented style and design patterns. It includes class definition with various features like encapsulation and polymorphism.

Key Points of Python Language

The key points of Python programming language are as follows –

- It includes functional and structured programming and methods as well as object oriented programming methods.
- It can be used as a scripting language or as a programming language.
- It includes automatic garbage collection.
- It includes high-level dynamic data types and supports various dynamic type checking.
- Python includes a feature of integration with C, C++ and languages like Java.

The download link for Python language is as follows – www.python.org/downloads It includes packages for various operating systems like Windows, MacOS and Linux distributions.



Python Strings

The basic declaration of strings is shown below –

```
str = 'Hello World!'
```

Python Lists

The lists of python can be declared as compound data types, separated by commas and

enclosed within square brackets ([]).

```
list = [ 'abcd' , 786 , 2.23, 'john' , 70.2 ]
tinylist = [123, 'john']
```

Python Tuples

A tuple is dynamic data type of Python which consists of number of values separated by commas. Tuples are enclosed with parentheses.

```
tinytuple = (123, 'john')
```

Python Dictionary

Python dictionary is a type of hash table. A dictionary key can be almost any data type of Python, which are usually numbers or strings.

```
tinydict = {'name': 'omkar','code':6734, 'dept': 'sales'}
```

Cryptography Packages

Python includes a package called `cryptography` which provides cryptographic recipes and primitives. It supports Python 2.7, Python 3.4+, and PyPy 5.3+. The basic installation of `cryptography` package is achieved through following command –

```
pip install cryptography
```

There are various packages with both high level recipes and low level interfaces to common cryptographic algorithms such as **symmetric ciphers**, **message digests** and **key derivation functions**.

Throughout this tutorial, we will be using various packages of Python for implementation of cryptographic algorithms.

Cryptography with Python - Reverse Cipher

The previous chapter gave you an overview of installation of Python on your local computer. In this chapter you will learn in detail about reverse cipher and its coding.

Algorithm of Reverse Cipher

The algorithm of reverse cipher holds the following features –

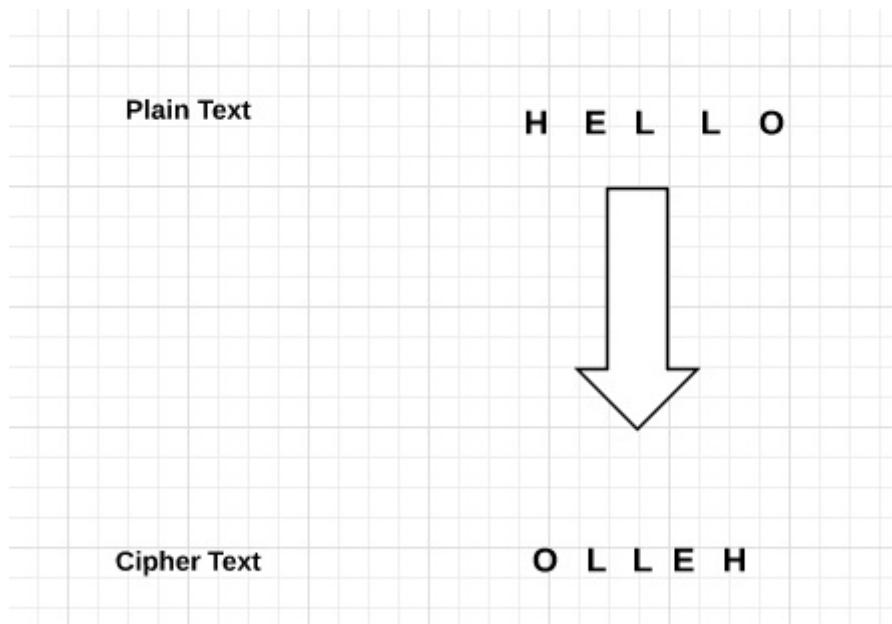
- Reverse Cipher uses a pattern of reversing the string of plain text to convert as

cipher text.

- The process of encryption and decryption is same.
- To decrypt cipher text, the user simply needs to reverse the cipher text to get the plain text.

Drawback

The major drawback of reverse cipher is that it is very weak. A hacker can easily break the cipher text to get the original message. Hence, reverse cipher is not considered as good option to maintain secure communication channel.,



Example

Consider an example where the statement **This is program to explain reverse cipher** is to be implemented with reverse cipher algorithm. The following python code uses the algorithm to obtain the output.

```
message = 'This is program to explain reverse cipher.'
translated = '' #cipher text is stored in this variable
i = len(message) - 1

while i >= 0:
    translated = translated + message[i]
    i = i - 1
print("The cipher text is : ", translated)
```

Output

You can see the reversed text, that is the output as shown in the following image –



```
E:\Cryptography- Python>python reversecipher.py
('The cipher text is : ', '.rehpic esrever nialpxe ot margorp si sihT')
E:\Cryptography- Python>
```

Explanation

- Plain text is stored in the variable message and the translated variable is used to store the cipher text created.
- The length of plain text is calculated using **for** loop and with help of **index number**. The characters are stored in cipher text variable **translated** which is printed in the last line.

Cryptography with Python - Caesar Cipher

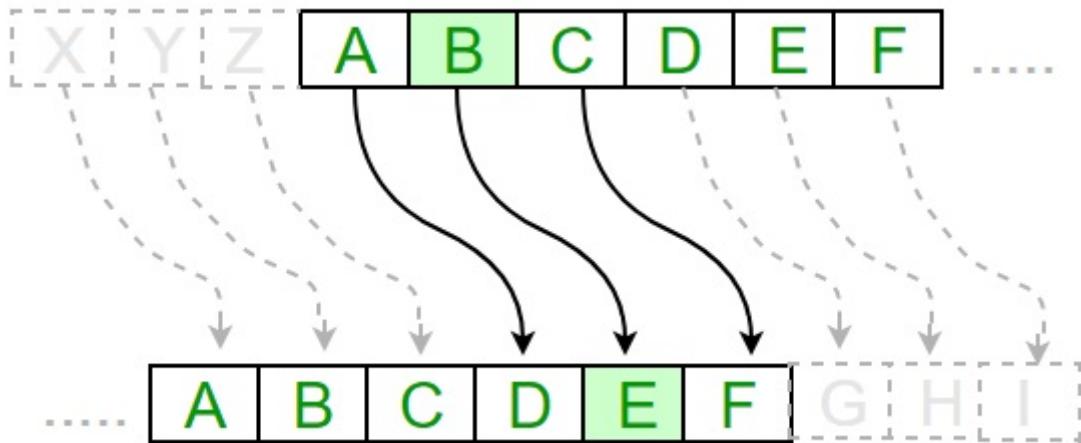
In the last chapter, we have dealt with reverse cipher. This chapter talks about Caesar cipher in detail.

Algorithm of Caesar Cipher

The algorithm of Caesar cipher holds the following features –

- Caesar Cipher Technique is the simple and easy method of encryption technique.
- It is simple type of substitution cipher.
- Each letter of plain text is replaced by a letter with some fixed number of positions down with alphabet.

The following diagram depicts the working of Caesar cipher algorithm implementation –



The program implementation of Caesar cipher algorithm is as follows –

```
def encrypt(text,s):
result = ""
# transverse the plain text
```

```

for i in range(len(text)):
    char = text[i]
    # Encrypt uppercase characters in plain text

    if (char.isupper()):
        result += chr((ord(char) + s-65) % 26 + 65)
    # Encrypt lowercase characters in plain text
    else:
        result += chr((ord(char) + s - 97) % 26 + 97)
return result

#check the above function
text = "CEASER CIPHER DEMO"
s = 4

print "Plain Text : " + text
print "Shift pattern : " + str(s)
print "Cipher: " + encrypt(text,s)

```

Output

You can see the Caesar cipher, that is the output as shown in the following image –

```

E:\Cryptography- Python>python caeserCipher.py
Plain Text : CEASER CIPHER DEMO
Shift pattern : 4
Cipher: GIEWIVrGMTLIVrHIQS
E:\Cryptography- Python>

```

Explanation

The plain text character is traversed one at a time.

- For each character in the given plain text, transform the given character as per the rule depending on the procedure of encryption and decryption of text.
- After the steps is followed, a new string is generated which is referred as cipher text.

Hacking of Caesar Cipher Algorithm

The cipher text can be hacked with various possibilities. One of such possibility is **Brute Force Technique**, which involves trying every possible decryption key. This technique does not demand much effort and is relatively simple for a hacker.

The program implementation for hacking Caesar cipher algorithm is as follows –

```

message = 'GIEWIVrGMTLIVrHIQS' #encrypted message
LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

```

```

for key in range(len(LETTERS)):
    translated = ''
    for symbol in message:
        if symbol in LETTERS:
            num = LETTERS.find(symbol)
            num = num - key
            if num < 0:
                num = num + len(LETTERS)
            translated = translated + LETTERS[num]
        else:
            translated = translated + symbol
print('Hacking key #%-s: %s' % (key, translated))

```

Consider the cipher text encrypted in the previous example. Then, the output with possible hacking methods with the key and using brute force attack technique is as follows –

```

Git CMD
Key #25: HJFXJWrHNUMJWrIjRT
E:\Cryptography- Python>python caesarHacker.py
Key #0: GIEWIVrGMTLIVrHIQS
Key #1: FHDVHUrFLSKHUrGHPR
Key #2: EGCUGTrEKRjGTrFGOQ
Key #3: DFBTFSrDjQIFSrEFNP
Key #4: CEASERrCIPHERrDEMO
Key #5: BDZRDQrBHOGDQrCDLN
Key #6: ACYQCPrAGNFCPrBCKM
Key #7: ZBXPBOrZFMEBOrABJL
Key #8: YAWOANrYELDANrZAIK
Key #9: XZVNZMrXDKCZMrYZHJ
Key #10: WYUMYLrWCjBYLrXYGI
Key #11: VXTLXKrVBIAXKrWFH
Key #12: UWSKWJrUAHZWJrVWEG
Key #13: TVRjVjIrTZGYVjIrUVDF
Key #14: SUQIUHrSYFXUHrTUCE
Key #15: RTPHTGrRXEWTGrSTBD
Key #16: QSOGSFrQWDVSFrRSAC
Key #17: PRNFRErPVCURErQRZB
Key #18: OQMEQDrOUBTQDrPQYA
Key #19: NPLDPCrNTASPCr0PXZ
Key #20: MOKCOBrMSZROBrNOWY
Key #21: LNjBNArLRYQNArMNvx
Key #22: KMIAMZrKQXPMZrLMUw
Key #23: JLHZLYrJPWOLYrKLTV
Key #24: IKGYKXrIOVNKXrJKSU
Key #25: HJFXJWrHNUMJWrIjRT

E:\Cryptography- Python>

```

Cryptography with Python - ROT13 Algorithm

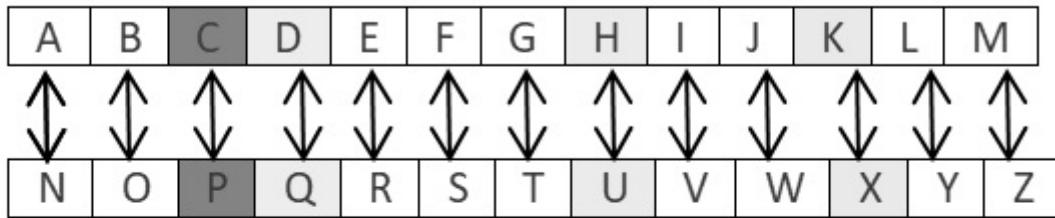
Till now, you have learnt about reverse cipher and Caesar cipher algorithms. Now, let us discuss the ROT13 algorithm and its implementation.

Explanation of ROT13 Algorithm

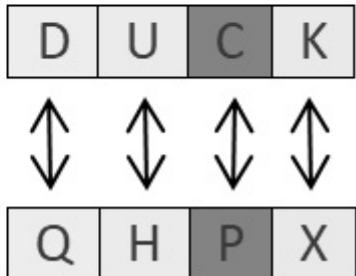
ROT13 cipher refers to the abbreviated form **Rotate by 13 places**. It is a special case of Caesar Cipher in which shift is always 13. Every letter is shifted by 13 places to encrypt or decrypt the message.

Example

The following diagram explains the ROT13 algorithm process pictorially –



ROT13



Program Code

The program implementation of ROT13 algorithm is as follows –

```
from string import maketrans

rot13trans = maketrans('ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz'
                      'NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm')

# Function to translate plain text
def rot13(text):
    return text.translate(rot13trans)
def main():
    txt = "ROT13 Algorithm"
    print rot13(txt)

if __name__ == "__main__":
    main()
```

You can see the ROT13 output as shown in the following image –



```
E:\Cryptography- Python>python rot13.py
EBG13 Nytbevguz
E:\Cryptography- Python>
```

Drawback

The ROT13 algorithm uses 13 shifts. Therefore, it is very easy to shift the characters in the reverse manner to decrypt the cipher text.

Analysis of ROT13 Algorithm

ROT13 cipher algorithm is considered as special case of Caesar Cipher. It is not a very secure algorithm and can be broken easily with frequency analysis or by just trying possible 25 keys whereas ROT13 can be broken by shifting 13 places. Therefore, it does not include any practical use.

Transposition Cipher

Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

Example

A simple example for a transposition cipher is **columnar transposition cipher** where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.

Consider the plain text **hello world**, and let us apply the simple columnar transposition technique as shown below

| | | | |
|---|---|---|---|
| h | e | I | I |
| o | w | o | r |
| l | d | | |

The plain text characters are placed horizontally and the cipher text is created with vertical format as : **holewdlo lr**. Now, the receiver has to use the same table to decrypt the cipher text to plain text.

Code

The following program code demonstrates the basic implementation of columnar transposition technique –

```
def split_len(seq, length):
```

```

    return [seq[i:i + length] for i in range(0, len(seq), length)]
def encode(key, plaintext):
    order = {
        int(val): num for num, val in enumerate(key)
    }
    ciphertext = ''

    for index in sorted(order.keys()):
        for part in split_len(plaintext, len(key)):
            try:ciphertext += part[order[index]]
            except IndexError:
                continue
    return ciphertext
print(encode('3214', 'HELLO'))

```

Explanation

- Using the function **split_len()**, we can split the plain text characters, which can be placed in columnar or row format.
- **encode** method helps to create cipher text with key specifying the number of columns and prints the cipher text by reading characters through each column.

Output

The program code for the basic implementation of columnar transposition technique gives the following output –

```

Git CMD
E:\Cryptography- Python>python columnarTransposition.py
LARPT HUONTSINCQCM NSOEIURAOITNE
E:\Cryptography- Python>

```

Note – Cryptanalysts observed a significant improvement in crypto security when transposition technique is performed. They also noted that re-encrypting the cipher text using same transposition cipher creates better security.

Encryption of Transposition Cipher

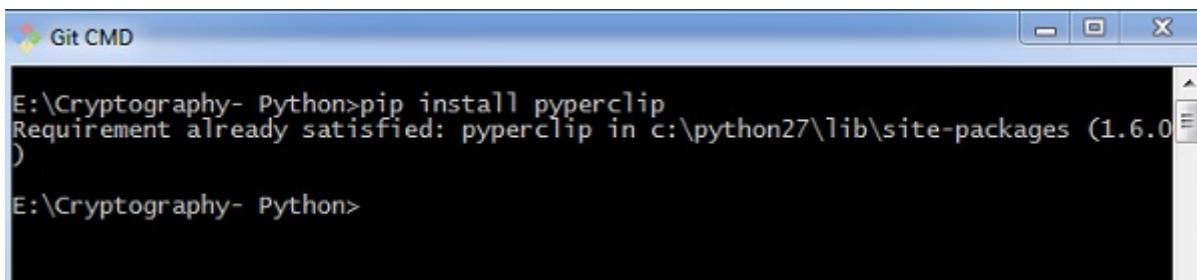
In the previous chapter, we have learnt about Transposition Cipher. In this chapter, let us discuss its encryption.

Pyperclip

The main usage of **pyperclip** plugin in Python programming language is to perform cross platform module for copying and pasting text to the clipboard. You can install python **pyperclip** module using the command as shown

```
pip install pyperclip
```

If the requirement already exists in the system, you can see the following output –



```
E:\Cryptography- Python>pip install pyperclip
Requirement already satisfied: pyperclip in c:\python27\lib\site-packages (1.6.0)
)
E:\Cryptography- Python>
```

Code

The python code for encrypting transposition cipher in which **pyperclip** is the main module is as shown below –

```
import pyperclip
def main():
    myMessage = 'Transposition Cipher'
    myKey = 10
    ciphertext = encryptMessage(myKey, myMessage)

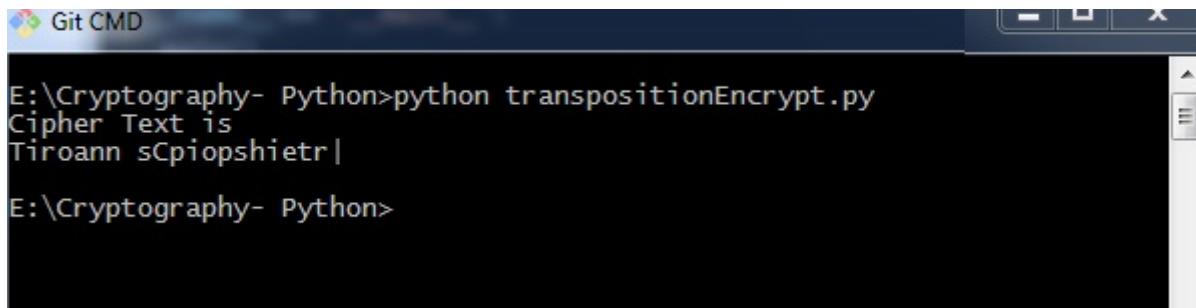
    print("Cipher Text is")
    print(ciphertext + '|')
    pyperclip.copy(ciphertext)

def encryptMessage(key, message):
    ciphertext = [''] * key

    for col in range(key):
        position = col
        while position < len(message):
            ciphertext[col] += message[position]
            position += key
    return ''.join(ciphertext) #Cipher text
if __name__ == '__main__':
    main()
```

Output

The program code for encrypting transposition cipher in which **pyperclip** is the main module gives the following output –



The screenshot shows a Windows Command Prompt window titled "Git CMD". The command entered is "python transpositionEncrypt.py". The output displays the cipher text "Tiroann sCpiopshietr|", which is the result of encrypting the message "Transposition Cipher" with a key of 6. The command prompt then returns to the directory "E:\Cryptography- Python>".

Explanation

- The function **main()** calls the **encryptMessage()** which includes the procedure for splitting the characters using **len** function and iterating them in a columnar format.
- The main function is initialized at the end to get the appropriate output.

Decryption of Transposition Cipher

In this chapter, you will learn the procedure for decrypting the transposition cipher.

Code

Observe the following code for a better understanding of decrypting a transposition cipher. The cipher text for message **Transposition Cipher** with key as **6** is fetched as **Toners raiCntisippoh**.

```
import math, pyperclip
def main():
    myMessage= 'Toners raiCntisippoh'
    myKey = 6
    plaintext = decryptMessage(myKey, myMessage)

    print("The plain text is")
    print('Transposition Cipher')

def decryptMessage(key, message):
    num0fColumns = math.ceil(len(message) / key)
    num0fRows = key
    num0fShadedBoxes = (num0fColumns * num0fRows) - len(message)
    plaintext = float('') * num0fColumns
    col = 0
    row = 0

    for symbol in message:
        plaintext[col] += symbol
        col += 1
        if (col == num0fColumns) or (col == num0fColumns - 1 and row >= num0fRows):
            col = 0
            row += 1

    return plaintext
```

```

        col = 0 row += 1 return ''.join(plaintext)
if __name__ == '__main__':
    main()

```

Explanation

The cipher text and the mentioned key are the two values taken as input parameters for decoding or decrypting the cipher text in reverse technique by placing characters in a column format and reading them in a horizontal manner.

You can place letters in a column format and later combined or concatenate them together using the following piece of code –

```

for symbol in message:
    plaintext[col] += symbol
    col += 1

    if (col == numColumns) or (col == numColumns - 1 and row >= numRows):
        col = 0
        row += 1
return ''.join(plaintext)

```

Output

The program code for decrypting transposition cipher gives the following output –

```
E:\Cryptography- Python>python transpositionDecrypt.py
The plain text is
Transposition Cipher
E:\Cryptography- Python>
```

Encryption of files

In Python, it is possible to encrypt and decrypt files before transmitting to a communication channel. For this, you will have to use the plugin **PyCrypto**. You can installation this plugin using the command given below.

```
pip install pycrypto
```

```
E:\Cryptography- Python>pip install pycrypto
Requirement already satisfied: pycrypto in c:\python27\lib\site-packages\pycrypto-2.6.1-py2.7-win32.egg (2.6.1)
```

```
E:\Cryptography- Python>
```

Code

The program code for encrypting the file with password protector is mentioned below –

```
# ======Other Configuration=====
# Usages :
usage = "usage: %prog [options] "
# Version
Version="%prog 0.0.1"
# =====
# Import Modules
import optparse, sys,os
from toolkit import processor as ps
def main():
    parser = optparse.OptionParser(usage = usage,version = Version)
    parser.add_option(
        '-i','--input',type = 'string',dest = 'inputfile',
        help = "File Input Path For Encryption", default = None)

    parser.add_option(
        '-o','--output',type = "string",dest = 'outputfile',
        help = "File Output Path For Saving Encryter Cipher",default = ".") 

    parser.add_option(
        '-p','--password',type = "string",dest = 'password',
        help = "Provide Password For Encrypting File",default = None)

    parser.add_option(
        '-p','--password',type = "string",dest = 'password',
        help = "Provide Password For Encrypting File",default = None)

(options, args)= parser.parse_args()

# Input Conditions Checkings
if not options.inputfile or not os.path.isfile(options.inputfile):
    print " [Error] Please Specify Input File Path"
    exit(0)
if not options.outputfile or not os.path.isdir(options.outputfile):
    print " [Error] Please Specify Output Path"
    exit(0)
if not options.password:
    print " [Error] No Password Input"
    exit(0)
inputfile = options.inputfile
```

```

        outfile = os.path.join(
            options.outputfile,os.path.basename(options.inputfile).split('.')[0])
        password = options.password
        base = os.path.basename(inputfile).split('.')[1]
        work = "E"

    ps.FileCipher(inputfile,outfile,password,work)
    return

if __name__ == '__main__':
    main()

```

You can use the following command to execute the encryption process along with password –

```
python pyfilecipher-encrypt.py -i file_path_for_encryption -o output_pat
```

Output

You can observe the following output when you execute the code given above –

```

Git CMD
E:\Cryptography- Python\py-filecipher\pyfilecipher>python pyfilecipher-encrypt.py -i test.txt -p p@ssw0rd
[+] Please Wait... Calculating MD5 SUM
[+] Input File MD5 Sum : 5e7c683623bdabaeae97f8157e80f85c
[+] Please Wait.. Encrypting File..
[+] Encryption Done!
[+] Thanks For Using My Program.

E:\Cryptography- Python\py-filecipher\pyfilecipher>

```

Explanation

The passwords are generated using MD5 hash algorithm and the values are stored in simply safe backup files in Windows system, which includes the values as displayed below –

```

hackRSA.py  test.ssb  rsa-decryption.py
1 5e7c683623bdabaeae97f8157e80f85c
2 dGVzdC50eHQ=
3 SjjizjD0oVdb17acpDMp5a5FX6raQYqXg2EJ2VBIzenUHwXJkj7f3Dl7YX0fs1cI

```

Decryption of files

In this chapter, let us discuss decryption of files in cryptography using Python. Note that for decryption process, we will follow the same procedure, but instead of specifying the output path, we will focus on input path or the necessary file which is encrypted.

Code

The following is a sample code for decrypting files in cryptography using Python –

```
#!/usr/bin/python
# ----- READ ME -----
# This Script is Created Only For Practise And Educational Purpose Only
# This Script Is Created For http://bitforestinfo.blogspot.in
# This Script is Written By
#
#
#####
##### Please Don't Remove Author Name #####
##### Thanks #####
#####
#
#
# =====Other Configuration=====
# Usages :
usage = "usage: %prog [options] "
# Version
Version="%prog 0.0.1"
# =====
# Import Modules
import optparse, sys,os
from toolkit import processor as ps
def main():
    parser = optparse.OptionParser(usage = usage,version = Version)
    parser.add_option(
        '-i','--input',type = 'string',dest = 'inputfile',
        help = "File Input Path For Encryption", default = None)

    parser.add_option(
        '-o','--output',type = "string",dest = 'outputfile',
        help = "File Output Path For Saving Encrypter Cipher",default = ".") 

    parser.add_option(
        '-p','--password',type = "string",dest = 'password',
        help = "Provide Password For Encrypting File",default = None)
    (options, args) = parser.parse_args()
    # Input Conditions Checkings
    if not options.inputfile or not os.path.isfile(options.inputfile):
        print "[Error] Please Specify Input File Path"
        exit(0)
    if not options.outputfile or not os.path.isdir(options.outputfile):
        print "[Error] Please Specify Output Path"
```

```
exit(0)
if not options.password:
    print "[Error] No password"
    exit(0)
inputfile = options.inputfile
outputfile = options.outputfile
password = options.password
work = "D"
ps.FileCipher(inputfile,outputfile,password,work)
return

if __name__ == '__main__':
    main()
```

You can use the following command for executing the above code –

```
python pyfilecipher-decrypt.py -i encrypted_file_path -p password
```

Output

You can observe the following code when you execute the command shown above –

```
E:\Cryptography- Python\py-filecipher\pyfilecipher>python pyfilecipher-decrypt.py -i test.ssb -p p@sswOrd
[+] Please Wait... Reading File.
[+] Please Wait... Decrypting File.
[+] Decryption Complete.
[+] Please Wait..
[+] Check File MD5SUM
[+] Before Encryption : [5e7c683623bdabaeae97f8157e80f85c]
[+] After Decryption : [5e7c683623bdabaeae97f8157e80f85c]

[+] File is Verified.
[+] Thanks For Using My Program.

E:\Cryptography- Python\py-filecipher\pyfilecipher>
```

Note – The output specifies the hash values before encryption and after decryption, which keeps a note that the same file is encrypted and the process was successful.

Base64 Encoding and Decoding

Base64 encoding converts the binary data into text format, which is passed through communication channel where a user can handle text safely. Base64 is also called as **Privacy enhanced Electronic mail (PEM)** and is primarily used in email encryption process.

Python includes a module called **BASE64** which includes two primary functions as given below –

- **base64.decode(input, output)** – It decodes the input value parameter specified and stores the decoded output as an object.

- **Base64.encode(input, output)** – It encodes the input value parameter specified and stores the decoded output as an object.

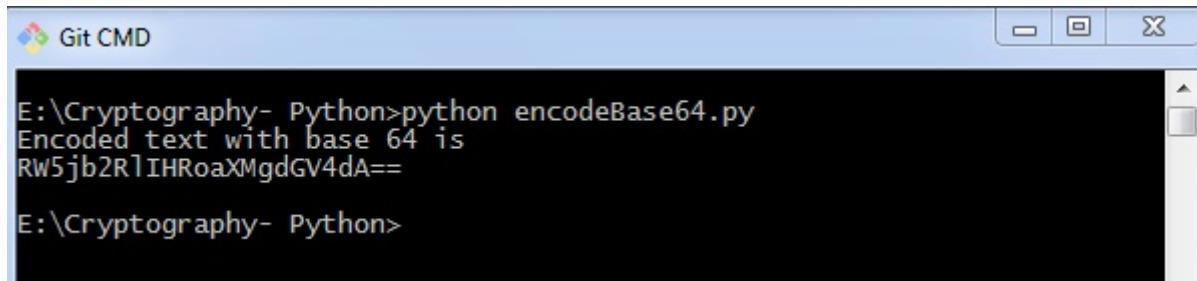
Program for Encoding

You can use the following piece of code to perform base64 encoding –

```
import base64  
encoded_data = base64.b64encode("Encode this text")  
  
print("Encoded text with base 64 is")  
print(encoded_data)
```

Output

The code for base64 encoding gives you the following output –



A screenshot of a Windows Command Prompt window titled "Git CMD". The window shows the command "python encodeBase64.py" being run, followed by the encoded output "Rw5jb2RlIHRoaXMgdGV4dA==". The prompt then changes to "E:\Cryptography- Python>".

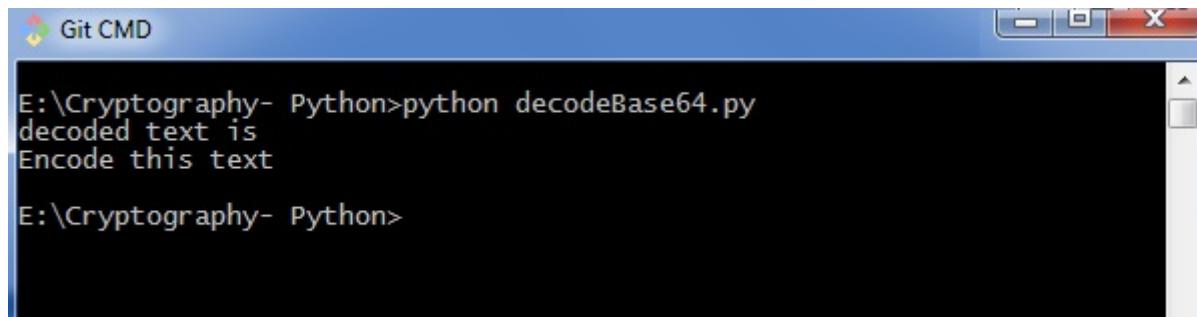
Program for Decoding

You can use the following piece of code to perform base64 decoding –

```
import base64  
decoded_data = base64.b64decode("Rw5jb2RlIHRoaXMgdGV4dA==")  
  
print("decoded text is ")  
print(decoded_data)
```

Output

The code for base64 decoding gives you the following output –



A screenshot of a Windows Command Prompt window titled "Git CMD". The window shows the command "python decodeBase64.py" being run, followed by the decoded output "Encode this text". The prompt then changes to "E:\Cryptography- Python>".

Difference between ASCII and base64

You can observe the following differences when you work on ASCII and base64 for encoding data –

- When you encode text in ASCII, you start with a text string and convert it to a sequence of bytes.
- When you encode data in Base64, you start with a sequence of bytes and convert it to a text string.

Drawback

Base64 algorithm is usually used to store passwords in database. The major drawback is that each decoded word can be encoded easily through any online tool and intruders can easily get the information.

Cryptography with Python - XOR Process

In this chapter, let us understand the XOR process along with its coding in Python.

Algorithm

XOR algorithm of encryption and decryption converts the plain text in the format ASCII bytes and uses XOR procedure to convert it to a specified byte. It offers the following advantages to its users –

- Fast computation
- No difference marked in left and right side
- Easy to understand and analyze

Code

You can use the following piece of code to perform XOR process –

```
def xor_crypt_string(data, key = 'awesom password', encode = False, decode = False):
    from itertools import izip, cycle
    import base64

    if decode:
        data = base64.decodestring(data)
        xored = ''.join(chr(ord(x) ^ ord(y)) for (x,y) in izip(data, cycle(key)))
    else:
        xored = ''.join(chr(ord(x) ^ ord(y)) for (x,y) in izip(data, cycle(key)))
        xored = base64.encodestring(xored).strip()

    return xored

secret_data = "XOR procedure"
```

```

print("The cipher text is")
print xor_crypt_string(secret_data, encode = True)
print("The plain text fetched")
print xor_crypt_string(xor_crypt_string(secret_data, encode = True), decode = True)

```

Output

The code for XOR process gives you the following output –

```

Git CMD
E:\Cryptography- Python>python xor.py
The cipher text is
OTg3UX8fChMEFwYFCg==
The plain text fetched
XOR procedure
E:\Cryptography- Python>

```

Explanation

- The function `xor_crypt_string()` includes a parameter to specify mode of encode and decode and also the string value.
- The basic functions are taken with `base64` modules which follows the XOR procedure/ operation to encrypt or decrypt the plain text/ cipher text.

Note – XOR encryption is used to encrypt data and is hard to crack by brute-force method, that is by generating random encrypting keys to match with the correct cipher text.

Multiplicative Cipher

While using Caesar cipher technique, encrypting and decrypting symbols involves converting the values into numbers with a simple basic procedure of addition or subtraction.

If multiplication is used to convert to cipher text, it is called a **wrap-around** situation. Consider the letters and the associated numbers to be used as shown below –

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

The numbers will be used for multiplication procedure and the associated key is 7. The basic formula to be used in such a scenario to generate a multiplicative cipher is as follows –

$$(\text{Alphabet Number} * \text{key}) \bmod (\text{total number of alphabets})$$

The number fetched through output is mapped in the table mentioned above and the corresponding letter is taken as the encrypted letter.

| Plaintext Symbol | Number | Encryption with Key 7 | Ciphertext Symbol |
|---------------------|--------|--------------------------|----------------------|
| A | 0 | (0 * 7) % 26 = 0 | A |
| B | 1 | (1 * 7) % 26 = 7 | H |
| C | 2 | (2 * 7) % 26 = 14 | O |
| D | 3 | (3 * 7) % 26 = 21 | V |
| E | 4 | (4 * 7) % 26 = 2 | C |
| F | 5 | (5 * 7) % 26 = 9 | J |
| G | 6 | (6 * 7) % 26 = 16 | Q |
| H | 7 | (7 * 7) % 26 = 23 | X |
| I | 8 | (8 * 7) % 26 = 4 | E |
| J | 9 | (9 * 7) % 26 = 11 | L |
| K | 10 | (10 * 7) % 26 = 18 | S |
| L | 11 | (11 * 7) % 26 = 25 | Z |
| M | 12 | (12 * 7) % 26 = 6 | G |
| N | 13 | (13 * 7) % 26 = 13 | N |
| O | 14 | (14 * 7) % 26 = 20 | U |
| P | 15 | (15 * 7) % 26 = 1 | B |
| Q | 16 | (16 * 7) % 26 = 8 | I |
| R | 17 | (17 * 7) % 26 = 15 | P |
| S | 18 | (18 * 7) % 26 = 22 | W |
| T | 19 | (19 * 7) % 26 = 3 | D |
| U | 20 | (20 * 7) % 26 = 10 | K |
| V | 21 | (21 * 7) % 26 = 17 | R |
| W | 22 | (22 * 7) % 26 = 24 | Y |
| X | 23 | (23 * 7) % 26 = 5 | F |
| Y | 24 | (24 * 7) % 26 = 12 | M |
| Z | 25 | (25 * 7) % 26 = 19 | T |

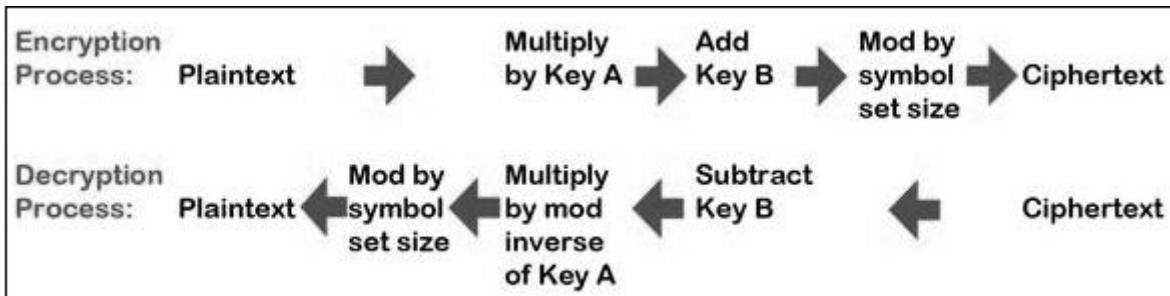
The basic modulation function of a multiplicative cipher in Python is as follows –

```
def unshift(key, ch):
    offset = ord(ch) - ASC_A
    return chr(((key[0] * (offset + key[1]))) % WIDTH) + ASC_A)
```

Note – The advantage with a multiplicative cipher is that it can work with very large keys like 8,953,851. It would take quite a long time for a computer to brute-force through a majority of nine million keys.

Cryptography with Python - Affine Cipher

Affine Cipher is the combination of Multiplicative Cipher and Caesar Cipher algorithm. The basic implementation of affine cipher is as shown in the image below –



In this chapter, we will implement affine cipher by creating its corresponding class that

includes two basic functions for encryption and decryption.

Code

You can use the following code to implement an affine cipher –

```
class Affine(object):
    DIE = 128
    KEY = (7, 3, 55)
    def __init__(self):
        pass
    def encryptChar(self, char):
        K1, K2, KI = self.KEY
        return chr((K1 * ord(char) + K2) % self.DIE)

    def encrypt(self, string):
        return "".join(map(self.encryptChar, string))

    def decryptChar(self, char):
        K1, K2, KI = self.KEY
        return chr(KI * (ord(char) - K2) % self.DIE)

    def decrypt(self, string):
        return "".join(map(self.decryptChar, string))
        affine = Affine()
print affine.encrypt('Affine Cipher')
print affine.decrypt('*18?FMT')
```

Output

You can observe the following output when you implement an affine cipher –

The screenshot shows a Windows Command Prompt window titled "Git CMD". The command "python affineCipher.py" is run, resulting in the output:

```
E:\Cryptography- Python>python affineCipher.py
JMMbFcXb!![F!
abcdefg
E:\Cryptography- Python>
```

The output displays the encrypted message for the plain text message **Affine Cipher** and decrypted message for the message sent as input **abcdefg**.

Hacking Monoalphabetic Cipher

In this chapter, you will learn about monoalphabetic cipher and its hacking using Python.

Monoalphabetic Cipher

A Monoalphabetic cipher uses a fixed substitution for encrypting the entire message. A monoalphabetic cipher using a Python dictionary with JSON objects is shown here –

```
monoalpha_cipher = {  
    'a': 'm',  
    'b': 'n',  
    'c': 'b',  
    'd': 'v',  
    'e': 'c',  
    'f': 'x',  
    'g': 'z',  
    'h': 'a',  
    'i': 's',  
    'j': 'd',  
    'k': 'f',  
    'l': 'g',  
    'm': 'h',  
    'n': 'j',  
    'o': 'k',  
    'p': 'l',  
    'q': 'p',  
    'r': 'o',  
    's': 'i',  
    't': 'u',  
    'u': 'y',  
    'v': 't',  
    'w': 'r',  
    'x': 'e',  
    'y': 'w',  
    'z': 'q',  
    ' ': ' ',  
}
```

With help of this dictionary, we can encrypt the letters with the associated letters as values in JSON object. The following program creates a monoalphabetic program as a class representation which includes all the functions of encryption and decryption.

```
from string import letters, digits  
from random import shuffle  
  
def random_monaalpha_cipher(pool = None):  
    if pool is None:  
        pool = letters + digits  
    original_pool = list(pool)
```

```

shuffled_pool = list(pool)
shuffle(shuffled_pool)
return dict(zip(original_pool, shuffled_pool))

def inverse_monoalpha_cipher(monoalpha_cipher):
    inverse_monoalpha = {}
    for key, value in monoalpha_cipher.iteritems():
        inverse_monoalpha[value] = key
    return inverse_monoalpha

def encrypt_with_monoalpha(message, monoalpha_cipher):
    encrypted_message = []
    for letter in message:
        encrypted_message.append(monoalpha_cipher.get(letter, letter))
    return ''.join(encrypted_message)

def decrypt_with_monoalpha(encrypted_message, monoalpha_cipher):
    return encrypt_with_monoalpha(
        encrypted_message,
        inverse_monoalpha_cipher(monoalpha_cipher)
    )

```

This file is called later to implement the encryption and decryption process of Monoalphabetic cipher which is mentioned as below –

```

import monoalphabeticCipher as mc

cipher = mc.random_monoalpha_cipher()
print(cipher)
encrypted = mc.encrypt_with_monoalpha('Hello all you hackers out there!', 
decrypted = mc.decrypt_with_monoalpha('sXGGt SGG Nt0 HSrLXFC t0U UHxFX!', 

print(encrypted)
print(decrypted)

```

Output

You can observe the following output when you implement the code given above –

```

E:\Cryptography- Python>python monoalphabetic_cipher.py
{'1': 'w', '0': 'd', '3': 'x', '2': '4', '5': 'G', '4': 'P', '7': 'g', '6':
9': '7', '8': 'K', 'A': '5', 'C': 'F', 'B': 'U', 'E': 'r', 'D': 'M', 'G':
F': 'S', 'I': '3', 'H': 'Q', 'K': 'V', 'J': '2', 'M': 'j', 'L': 'D', 'O':
N': 'Z', 'Q': '1', 'P': '8', 'S': 's', 'R': 'z', 'U': 'I', 'T': 'B', 'W':
V': 'N', 'Y': 'W', 'X': 'C', 'Z': 'v', 'a': 'Y', 'c': '9', 'b': 'x', 'e':
'd': '0', 'g': 'A', 'f': 'c', 'i': 'i', 'h': 'o', 'k': 'b', 'j': 'a', 'm':
'l': '6', 'o': 'y', 'n': 'H', 'q': 'L', 'p': 'n', 's': 'h', 'r': 'T', 'u':
't': 't', 'w': 'l', 'v': 'k', 'y': 'R', 'x': 'u', 'z': 'q'}
qf66y Y66 RyJ oY9bfTh yJt tofIf!
S355t E55 Vtd nEEa3CX fdb Rn3C3l

```



```
E:\Cryptography- Python>
```

Thus, you can hack a monoalphabetic cipher with specified key value pair which cracks the cipher text to actual plain text.

Simple Substitution Cipher

Simple substitution cipher is the most commonly used cipher and includes an algorithm of substituting every plain text character for every cipher text character. In this process, alphabets are jumbled in comparison with Caesar cipher algorithm.

Example

Keys for a simple substitution cipher usually consists of 26 letters. An example key is –

```
plain alphabet : abcdefghijklmnopqrstuvwxyz  
cipher alphabet: phqgiumeaylnofdxjkrcvstzwb
```

An example encryption using the above key is–

```
plaintext : defend the east wall of the castle  
ciphertext: giuifg cei iprc tpnn du cei qprcni
```

The following code shows a program to implement simple substitution cipher –

```
import random, sys

LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
def main():
    message = ''
    if len(sys.argv) > 1:
        with open(sys.argv[1], 'r') as f:
            message = f.read()
    else:
        message = raw_input("Enter your message: ")
    mode = raw_input("E for Encrypt, D for Decrypt: ")
    key = ''

    while checkKey(key) is False:
        key = raw_input("Enter 26 ALPHA key (leave blank for random key): ")
        if key == '':
            key = getRandomKey()
        if checkKey(key) is False:
            print('There is an error in the key or symbol set.')

    encryptDecryptMessage(message, key, mode)
```

```
translated = translateMessage(message, key, mode)
print('Using key: %s' % (key))

if len(sys.argv) > 1:
    fileOut = 'enc.' + sys.argv[1]
    with open(fileOut, 'w') as f:
        f.write(translated)
    print('Success! File written to: %s' % (fileOut))
else: print('Result: ' + translated)

# Store the key into list, sort it, convert back, compare to alphabet.
def checkKey(key):
    keyString = ''.join(sorted(list(key)))
    return keyString == LETTERS

def translateMessage(message, key, mode):
    translated = ''
    charsA = LETTERS
    charsB = key

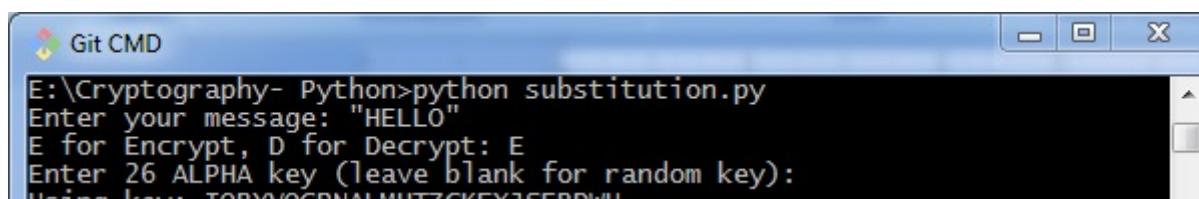
    # If decrypt mode is detected, swap A and B
    if mode == 'D':
        charsA, charsB = charsB, charsA
    for symbol in message:
        if symbol.upper() in charsA:
            symIndex = charsA.find(symbol.upper())
            if symbol.isupper():
                translated += charsB[symIndex].upper()
            else:
                translated += charsB[symIndex].lower()
        else:
            translated += symbol
    return translated

def getRandomKey():
    randomList = list(LETTERS)
    random.shuffle(randomList)
    return ''.join(randomList)

if __name__ == '__main__':
    main()
```

Output

You can observe the following output when you implement the code given above –



```
Key: RTWGOUIKZBYDNJYXSCPQAMFEHL
Result: "PVMMZ"
E:\Cryptography- Python>
```

Testing of Simple Substitution Cipher

In this chapter, we will focus on testing substitution cipher using various methods, which helps to generate random strings as given below –

```
import random, string, substitution
def main():
    for i in range(1000):
        key = substitution.getRandomKey()
        message = random_string()
        print('Test %s: String: "%s.."' % (i + 1, message[:50]))
        print("Key: " + key)
        encrypted = substitution.translateMessage(message, key, 'E')
        decrypted = substitution.translateMessage(encrypted, key, 'D')

        if decrypted != message:
            print('ERROR: Decrypted: "%s" Key: %s' % (decrypted, key))
            sys.exit()
        print('Substitution test passed!')

def random_string(size = 5000, chars = string.ascii_letters + string.digits):
    return ''.join(random.choice(chars) for _ in range(size))
if __name__ == '__main__':
    main()
```

Output

You can observe the output as randomly generated strings which helps in generating random plain text messages, as shown below –

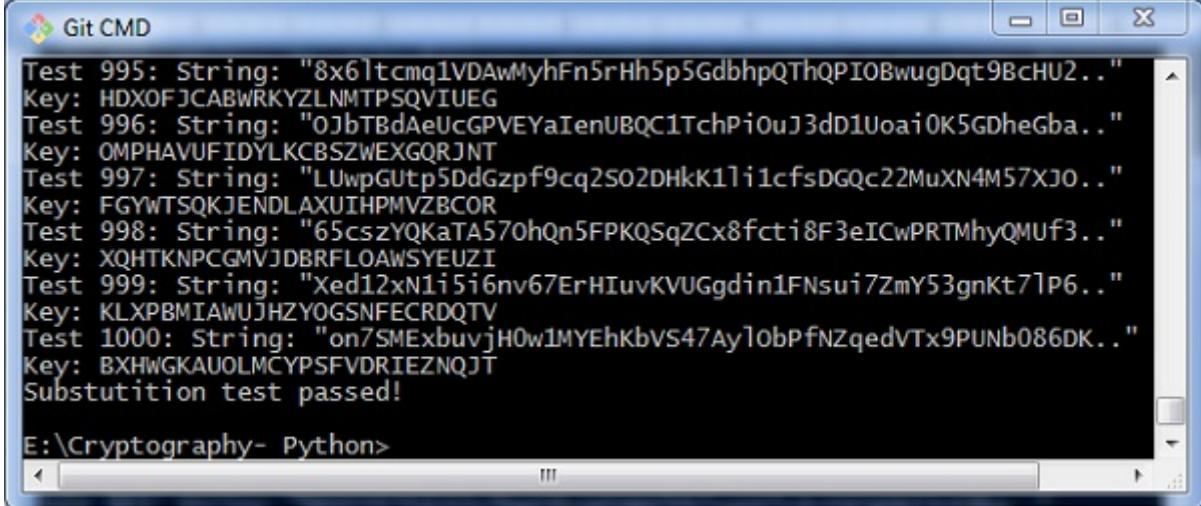
```
Key: RTWGOUIKZBYDNJYXSCPQAMFEHL
Test 853: String: "CANiR6kd1kNWtKC5LLtvM8rRZ9KhtBZQeg8kJn5WqIZGuSPQcC.."
Key: VKJNDHLPBCWOISTUARXFMYQZEG
Test 854: String: "Fan0n1Jz3zFArwAwcoPWLEjMNngCYj1xFQG9M44CcFwECCU9jIX.."
Key: XTFBYWQIDPUANCSKZMRLVGHJOE
Test 855: String: "yhG37cnkpodgm0gxdlkZQ3P7tZxpM4z0H14f1jgRRz1qbvSyG5L.."
Key: MLEROFGWAHYVQJNZTSKCIDPBUX
Test 856: String: "0dm6GZrMhNfJtc2CWsBRa09NH3VhhjYKrGkc5nv3GS6akKQ2qd.."
Key: QBZWLYUCGDTNMRVASOPIFEJHKX
Test 857: String: "hecudiviLYQzDD9VFysL7NFWT5BHH2jd693UQj7KysdVHXQpu3M.."
Key: JSFKWRGZYUNAPMHVLXEDBCQOT
Test 858: String: "8KsedvvWrVvEGQXHF6sf49iTjyOsoDwy1wDjlqcfjJpXq54dARz.."
Key: XFBGCKLSUWOMVDHRZNJITQYPEA
Test 859: String: "yhTwR717pSZLdHRvbHVkdEM9qf2cjmuUtl1gYvDi7F6HkwIqaTv.."
Key: AMLOZNDYSKIPQFUGEWBRHXJCTV
Test 860: String: "MhAj7hkeBMhJbhLPUD45NCPrcc280ufYs2RkaZX6I7Lk18hugwK.."
Key: ZHLIKWPGNBSVUOOQAYJCMRXDET
Test 861: String: "NybzvRU2hzBRpjUT7BkTiuHiSijIDzXyP6vHPfSb1B4Zis8x.."
```

```

Key: WAGTAMPCCQDSDKUCHNNVJFJY26E
Test 862: String: "YMgHNqAwM1LTIOvMJAvzodG4eQqRStvEjyu4ecpRXMwFUYxy3.."
Key: BZKXPNJDHWVFCGROIMYSTLQEUA
Test 863: String: "PEO2357SgytGu1hms1kswZURH7fh1xpUGls4vYXCWUb53cF8hq.."
Key: SWNGTPXYKDRMUOVEBZFACIJQLH
Test 864: String: "UONgJqjywxru25quPGkD572Ywbu0chuqGsdG7PtN8upVyl9fF.."
Key: AYGEPVQNBDTCMFUXSOHJJZWKRL
Test 865: String: "GMoamfZqASZHdnUk5LN46F5gRM87D0z0FQvaJinkiIoWSkQnkY.."
Key: EBASFDFGUTRKOYXMJIWZCVPHLNQ
Test 866: String: "hen1Qxux49rwKKP5wSnknedBgd2NBjGMWNrWbkqneEBMvtU0cn.."
Key: RFHNSQUBGYMOAKXJPZVCIDLEWT
Test 867: String: "2mKjE4T2bdStzjmT5yHEemSBIBf1w0bTCojGqqdazXo7lq0uLD.."
Key: DLUZWYGOQXVJHNBRMIEASFCTKP
Test 868: String: "jycpUC31kewdTK31lV7tmtK7VG55kusbb2U6IJwLqzXvW7okLs.."
Key: OPVECBWMYTHDXFJQARNSGIULKZ
Test 869: String: "8Bhrr4E32s0iGTyJVn7emNf9GIInn8bs1jrYI5ubk2wt dxVcnEg.."

```

After the test is successfully completed, we can observe the output message **Substitution test passed!**.



```

Git CMD
Test 995: String: "8x6ltcmq1VDAwMyhFn5rHh5p5GdbhpQThQPIOBwugDqt9BcHU2.."
Key: HDXOFJCABWRKYZLNMTPSQVIUEG
Test 996: String: "0jbTBdAeUcGPVEYaIenUBQC1TchPi0uJ3dD1Uoai0K5GDheGba.."
Key: QMPHAVUFIDYLKCBSZWEXGQRJNT
Test 997: String: "LUwpGUtp5DdGzpf9cq2502DHkK1l1i1cf5DGQc22MuXN4M57XJO.."
Key: FGYWTSQKJENDLAXUIHPMVZBCOR
Test 998: String: "65cszYQKaTA570hQn5FPKQSqZCx8fcti8F3eICwPRTMhyQMUF3.."
Key: XQHTKNPCGMVJDBRFLOAWSYEUZI
Test 999: String: "Xed12xN1i5i6nv67ErHIuvKVUGgdin1FNsu17zmY53gnKt7lP6.."
Key: KLXPBMIAWUJHZYOGSNFECRDQTV
Test 1000: String: "on7SMExbuvjH0w1MYEhKbVS47Ay1obPfNZqedVTx9PUNb086DK.."
Key: BXHWGKAUOLMCYPSFVDRIEZQNJT
Substitution test passed!
E:\Cryptography- Python>

```

Thus, you can hack a substitution cipher in the systematic manner.

Decryption of Simple Substitution Cipher

In this chapter, you can learn about simple implementation of substitution cipher which displays the encrypted and decrypted message as per the logic used in simple substitution cipher technique. This can be considered as an alternative approach of coding.

Code

You can use the following code to perform decryption using simple substitution cipher –

```

import random
chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' + \
'abcdefghijklmnopqrstuvwxyz' + \
'0123456789' + \
':.;,!@#$%&()+=-*/_<> []{}`~^"\\"\\'
def generate_key():
    """Generate an key for our cipher"""
    shuffled = sorted(chars, key=lambda k: random.random())

```

```

    return dict(zip(chars, shuffled))

def encrypt(key, plaintext):
    """Encrypt the string and return the ciphertext"""
    return ''.join(key[l] for l in plaintext)

def decrypt(key, ciphertext):
    """Decrypt the string and return the plaintext"""
    flipped = {v: k for k, v in key.items()}
    return ''.join(flipped[l] for l in ciphertext)

def show_result(plaintext):
    """Generate a resulting cipher with elements shown"""
    key = generate_key()
    encrypted = encrypt(key, plaintext)
    decrypted = decrypt(key, encrypted)

    print 'Key: %s' % key
    print 'Plaintext: %s' % plaintext
    print 'Encrypted: %s' % encrypted
    print 'Decrypted: %s' % decrypted
show_result('Hello World. This is demo of substitution cipher')

```

Output

The above code gives you the output as shown here –

```

E:\Cryptography- Python>python substitutionDecrypt.py
Key: {':': '?', '$': '%', '(': 'f', ')': 'o', '0': '0', '4': '!', '8': 'v', '<': 'N', '\\': 'x', '#': 'x', '@': 't', 'D': '^', 'H': 'g', 'L': 'x', 'P': '5', 'T': 'x', 'X': 'N', '\\\\': 'x', 'o': 'M', 'd': 'q', 'h': '8', 'l': ')', 'p': '/', 't': 'x', 'x': 'x', '+': 'u', '@': '/', 'U': '3', 'r': '7', 'b': 'b', 'D': '?', 'G': 'C', '<': 'G', 'Y': 'K', 'O': 'B', 'S': '3', 'W': 'w', 'Q': 'T', 'c': '#', 'g': 'k', 'k': 's', 'o': 'j', 's': '[', 'w': 'w', 'h': 'R', '&': 'K', 'j': 'Z', '2': 'y', '6': 'A', '9': '>', 'B': 'L', 'F': '&': 'J', 'N': '\\', 'R': 'n', 'V': 'E', 'Z': 'c', '^': 'p', 'b': ']', 'F': '2', 'j': '>', 'n': 'p', 'r': 'l', 'v': 'F', 'z': 'e', '~': 'H', '!:': '=', '%': '}', '}:': 'v', '1': 's', '5': '9', 'a': '4', 'A': 'i', 'E': '}', 'I': 'm', 'M': '!', 'Q': 'I', 'U': '*', 'Y': 'c', 'z': 'a', '(': '(', 'e': '~, 'i': '7', 'm': 's', 'q': '+', 'u': 'd', 'y': '6', ')': '}'}
plaintext: Hello World. This is demo of substitution cipher
Encrypted: g~)j?wj1)qz? 87[?7[?q~sj?j2?[d][,7,d,7jp?#7/8~1
Decrypted: Hello World. This is demo of substitution cipher
E:\Cryptography- Python>

```

Python Modules of Cryptography

In this chapter, you will learn in detail about various modules of cryptography in Python.

Cryptography Module

It includes all the recipes and primitives, and provides a high level interface of coding in Python. You can install cryptography module using the following command –

```
pip install cryptography
```

```
E:\Cryptography- Python>pip install cryptography
Requirement already satisfied: cryptography in c:\python27\lib\site-packages (2.2.1)
Requirement already satisfied: six>=1.4.1 in c:\python27\lib\site-packages (from cryptography) (1.11.0)
Requirement already satisfied: cffi>=1.7; platform_python_implementation != "PyPy" in c:\python27\lib\site-packages (from cryptography) (1.11.5)
Requirement already satisfied: enum34; python_version < "3" in c:\python27\lib\site-packages (from cryptography) (1.1.6)
Requirement already satisfied: asn1crypto>=0.21.0 in c:\python27\lib\site-packages (from cryptography) (0.24.0)
Requirement already satisfied: idna>=2.1 in c:\python27\lib\site-packages (from cryptography) (2.6)
Requirement already satisfied: ipaddress; python_version < "3" in c:\python27\lib\site-packages (from cryptography) (1.0.19)
Requirement already satisfied: pycparser in c:\python27\lib\site-packages (from cffi>=1.7; platform_python_implementation != "PyPy"->cryptography) (2.18)
E:\Cryptography- Python>
```

Code

You can use the following code to implement the cryptography module –

```
from cryptography.fernet import Fernet
key = Fernet.generate_key()
cipher_suite = Fernet(key)
cipher_text = cipher_suite.encrypt("This example is used to demonstrate ci
plain_text = cipher_suite.decrypt(cipher_text)
```

Output

The code given above produces the following output –

```
E:\Cryptography- Python>python cryptography-module.py
The cipher text is
gAAAAABa5L1CX4fyS-D1h44w7hQIWfTvUxoxxr05uUgyAzlgBzMzogbKYW-AVX13h5Q1lQ-Vs_oKbDd
bVW0oN4Jt0iWjJ34NSDDrPZzqdq1XZMskDzKcx28_sBFfAE71dKVpfKAJuTTjqoBF3ZMsuGSELa0YasM
FQ==
The plain text is
This example is used to demonstrate cryptography module
E:\Cryptography- Python>
```

The code given here is used to verify the password and creating its hash. It also includes logic for verifying the password for authentication purpose.

```
import uuid
import hashlib

def hash_password(password):
    # uuid is used to generate a random number of the specified password
    salt = uuid.uuid4().hex
    return hashlib.sha256(salt.encode() + password.encode()).hexdigest() + \
        salt

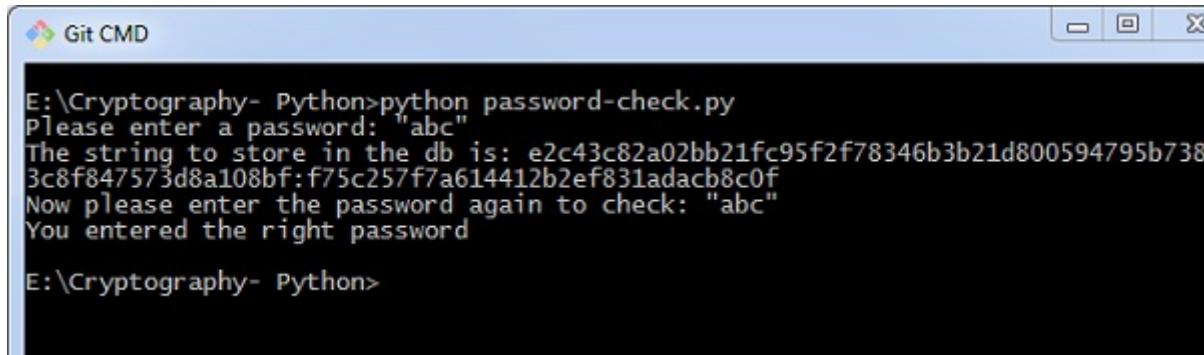
def check_password(hashed_password, user_password):
    password, salt = hashed_password.split(':')
    return password == hashlib.sha256(salt.encode() + user_password.encode()).hexdigest() + salt

new_pass = input('Please enter a password: ')
hashed_password = hash_password(new_pass)
print('The string to store in the db is: ' + hashed_password)
old_pass = input('Now please enter the password again to check: ')

if check_password(hashed_password, old_pass):
    print('You entered the right password')
else:
    print('Passwords do not match')
```

Output

Scenario 1 – If you have entered a correct password, you can find the following output –

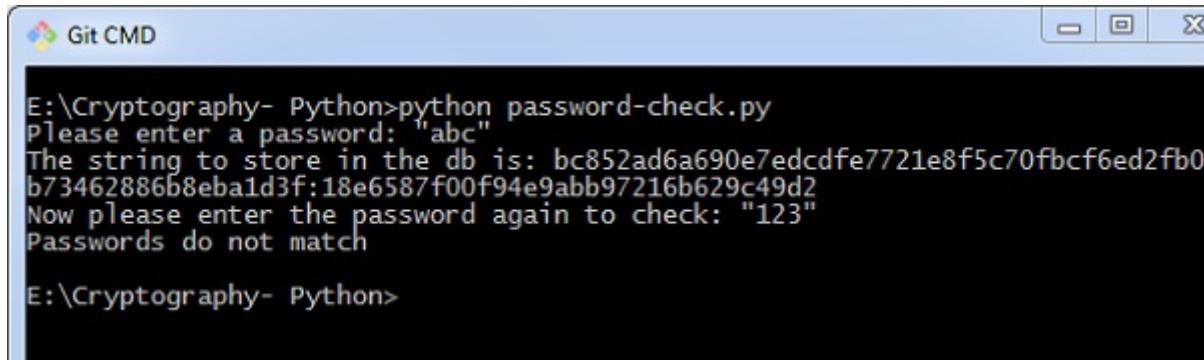


The screenshot shows a Windows Command Prompt window titled "Git CMD". The command `python password-check.py` is run, followed by entering the password "abc". The program outputs the hashed password "e2c43c82a02bb21fc95f2f78346b3b21d800594795b7383c8f847573d8a108bf:f75c257f7a614412b2ef831adacb8c0f" and then asks for the password again. Upon re-entering "abc", it prints "You entered the right password".

```
E:\Cryptography- Python>python password-check.py
Please enter a password: "abc"
The string to store in the db is: e2c43c82a02bb21fc95f2f78346b3b21d800594795b7383c8f847573d8a108bf:f75c257f7a614412b2ef831adacb8c0f
Now please enter the password again to check: "abc"
You entered the right password

E:\Cryptography- Python>
```

Scenario 2 – If we enter wrong password, you can find the following output –



The screenshot shows a Windows Command Prompt window titled "Git CMD". The command `python password-check.py` is run, followed by entering the password "abc". The program outputs the hashed password "bc852ad6a690e7edcdf7721e8f5c70fbef6ed2fb0b73462886b8eba1d3f:18e6587f00f94e9abb97216b629c49d2" and then asks for the password again. Upon re-entering "123", it prints "Passwords do not match".

```
E:\Cryptography- Python>python password-check.py
Please enter a password: "abc"
The string to store in the db is: bc852ad6a690e7edcdf7721e8f5c70fbef6ed2fb0b73462886b8eba1d3f:18e6587f00f94e9abb97216b629c49d2
Now please enter the password again to check: "123"
Passwords do not match

E:\Cryptography- Python>
```

Explanation

Hashlib package is used for storing passwords in a database. In this program, **salt** is used which adds a random sequence to the password string before implementing the hash function.

Understanding Vignere Cipher

Vignere Cipher includes a twist with Caesar Cipher algorithm used for encryption and decryption. Vignere Cipher works similar to Caesar Cipher algorithm with only one major distinction: Caesar Cipher includes algorithm for one-character shift, whereas Vignere Cipher includes key with multiple alphabets shift.

Mathematical Equation

For encryption the mathematical equation is as follows –

$$E_k (M_i) = (M_i + K_i) \mod 26$$

For decryption the mathematical equation is as follows –

$$D_k (C_i) = (C_i - K_i) \mod 26$$

Vignere cipher uses more than one set of substitutions, and hence it is also referred as **polyalphabetic cipher**. Vignere Cipher will use a letter key instead of a numeric key representation: Letter A will be used for key 0, letter B for key 1 and so on. Numbers of the letters before and after encryption process is shown below –

| Plaintext Letter | Subkey Letter | Ciphertext Letter |
|---------------------|------------------|----------------------|
| C (2) | P (15) | → R (17) |
| O (14) | I (8) | → W (22) |
| M (12) | Z (25) | → L (11) |
| M (12) | Z (25) | → L (11) |
| O (14) | A (0) | → O (14) |
| N (13) | P (15) | → C (2) |
| S (18) | I (8) | → A (0) |
| E (4) | Z (25) | → D (3) |
| N (13) | Z (25) | → M (12) |
| S (18) | A (0) | → S (18) |
| E (4) | P (15) | → T (19) |
| I (8) | I (8) | → Q (16) |
| S (18) | Z (25) | → R (17) |
| N (13) | Z (25) | → M (12) |
| O (14) | A (0) | → O (14) |
| T (19) | P (15) | → I (8) |
| S (18) | I (8) | → A (0) |
| O (14) | Z (25) | → N (13) |

| | | |
|--------|--------|----------|
| C (2) | Z (25) | → B (1) |
| O (14) | A (0) | → O (14) |
| M (12) | P (15) | → B (1) |
| M (12) | I (8) | → U (20) |
| O (14) | Z (25) | → N (13) |
| N (13) | Z (25) | → M (12) |

The possible combination of number of possible keys based on Vignere key length is given as follows, which gives the result of how secure is Vignere Cipher Algorithm –

| Key Length | Equation | Possible Keys |
|------------|---------------------------------------|------------------------------|
| 1 | 26 | = 26 |
| 2 | 26×26 | = 676 |
| 3 | 676×26 | = 17,576 |
| 4 | $17,576 \times 26$ | = 456,976 |
| 5 | $456,976 \times 26$ | = 11,881,376 |
| 6 | $11,881,376 \times 26$ | = 308,915,776 |
| 7 | $308,915,776 \times 26$ | = 8,031,810,176 |
| 8 | $8,031,810,176 \times 26$ | = 208,827,064,576 |
| 9 | $208,827,064,576 \times 26$ | = 5,429,503,678,976 |
| 10 | $5,429,503,678,976 \times 26$ | = 141,167,095,653,376 |
| 11 | $141,167,095,653,376 \times 26$ | = 3,670,344,486,987,776 |
| 12 | $3,670,344,486,987,776 \times 26$ | = 95,428,956,661,682,176 |
| 13 | $95,428,956,661,682,176 \times 26$ | = 2,481,152,873,203,736,576 |
| 14 | $2,481,152,873,203,736,576 \times 26$ | = 64,509,974,703,297,150,976 |

Vignere Tableau

The tableau used for Vignere cipher is as shown below –

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 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 |
| A | 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 |
| B | 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 | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | 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 |

Implementing Vignere Cipher

In this chapter, let us understand how to implement Vignere cipher. Consider the text **This is basic implementation of Vignere Cipher** is to be encoded and the key used is **PIZZA**.

Code

You can use the following code to implement a Vignere cipher in Python –

```
import pyperclip

LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
def main():
    myMessage = "This is basic implementation of Vignere Cipher"
    myKey = 'PIZZA'
    myMode = 'encrypt'

    if myMode == 'encrypt':
        translated = encryptMessage(myKey, myMessage)
    elif myMode == 'decrypt':
        translated = decryptMessage(myKey, myMessage)

    print('%sed message: ' % (myMode.title()))
    print(translated)
    print()

def encryptMessage(key, message):
    return translateMessage(key, message, 'encrypt')
def decryptMessage(key, message):
    return translateMessage(key, message, 'decrypt')
def translateMessage(key, message, mode):
    translated = [] # stores the encrypted/decrypted message string
    keyIndex = 0
    key = key.upper()

    for symbol in message:
        num = LETTERS.find(symbol.upper())
        if num != -1:
            if mode == 'encrypt':
                num += LETTERS.find(key[keyIndex])
                    elif mode == 'decrypt':
                num -= LETTERS.find(key[keyIndex])
            num %= len(LETTERS)

            if symbol.isupper():
                translated.append(LETTERS[num])
            else:
```

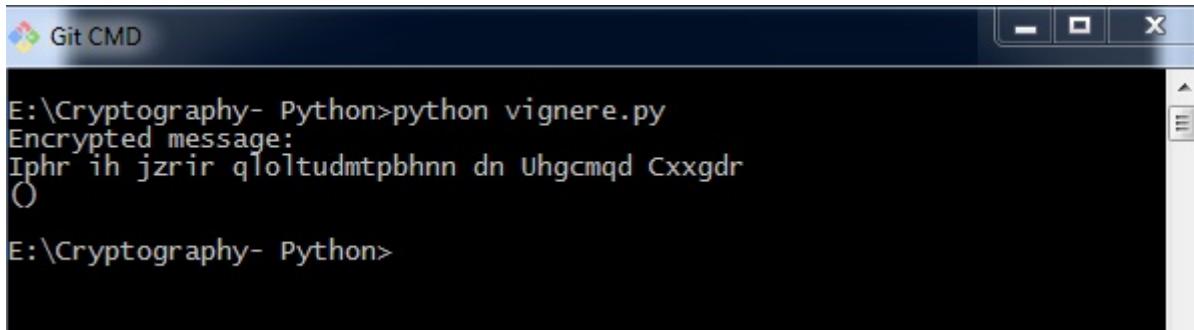
```
    elif symbol.islower():
        translated.append(LETTERS[num].lower())
        keyIndex += 1

    if keyIndex == len(key):
        keyIndex = 0
    else:
        translated.append(symbol)
return ''.join(translated)

if __name__ == '__main__':
    main()
```

Output

You can observe the following output when you implement the code given above –



The screenshot shows a Windows Command Prompt window titled "Git CMD". The command "E:\Cryptography- Python>python vignere.py" is entered, followed by the output "Encrypted message:" and the ciphertext "Iphr ih jzrir qoltudmtpbhnn dn Uhgcjqd Cxxgdr O". The prompt "E:\Cryptography- Python>" is visible at the bottom.

The possible combinations of hacking the Vignere cipher is next to impossible. Hence, it is considered as a secure encryption mode.

One Time Pad Cipher

One-time pad cipher is a type of Vignere cipher which includes the following features –

- It is an unbreakable cipher.
- The key is exactly same as the length of message which is encrypted.
- The key is made up of random symbols.
- As the name suggests, key is used one time only and never used again for any other message to be encrypted.

Due to this, encrypted message will be vulnerable to attack for a cryptanalyst. The key used for a one-time pad cipher is called **pad**, as it is printed on pads of paper.

Why is it Unbreakable?

The key is unbreakable owing to the following features –

- The key is as long as the given message.

- The key is truly random and specially auto-generated.
- Key and plain text calculated as modulo 10/26/2.
- Each key should be used once and destroyed by both sender and receiver.
- There should be two copies of key: one with the sender and other with the receiver.

Encryption

To encrypt a letter, a user needs to write a key underneath the plaintext. The plaintext letter is placed on the top and the key letter on the left. The cross section achieved between two letters is the plain text. It is described in the example below –

| |
|----------------------------|
| Plain text: THIS IS SECRET |
| OTP-Key : XVHE UW NOPGDZ |
| ----- |
| Ciphertext: QCPW CO FSRXHS |
| In groups : QCPWC OFSRX HS |

Decryption

To decrypt a letter, user takes the key letter on the left and finds cipher text letter in that row. The plain text letter is placed at the top of the column where the user can find the cipher text letter.

Implementation of One Time Pad Cipher

Python includes a hacky implementation module for **one-time-pad** cipher implementation. The package name is called One-Time-Pad which includes a command line encryption tool that uses encryption mechanism similar to the one-time pad cipher algorithm.

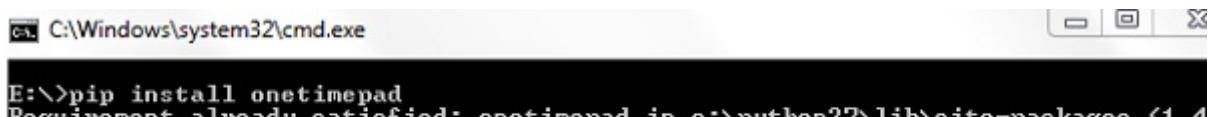
Installation

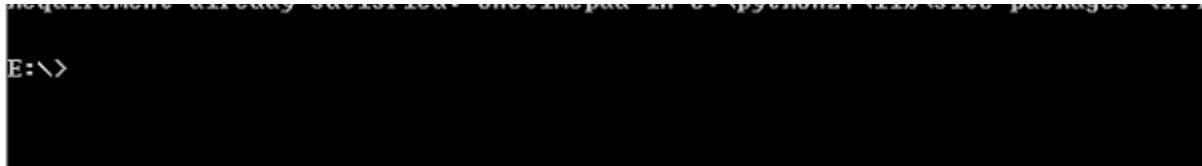
You can use the following command to install this module –

```
pip install onetimepad
```

If you wish to use it from the command-line, run the following command –

```
onetimepad
```





Code

The following code helps to generate a one-time pad cipher –

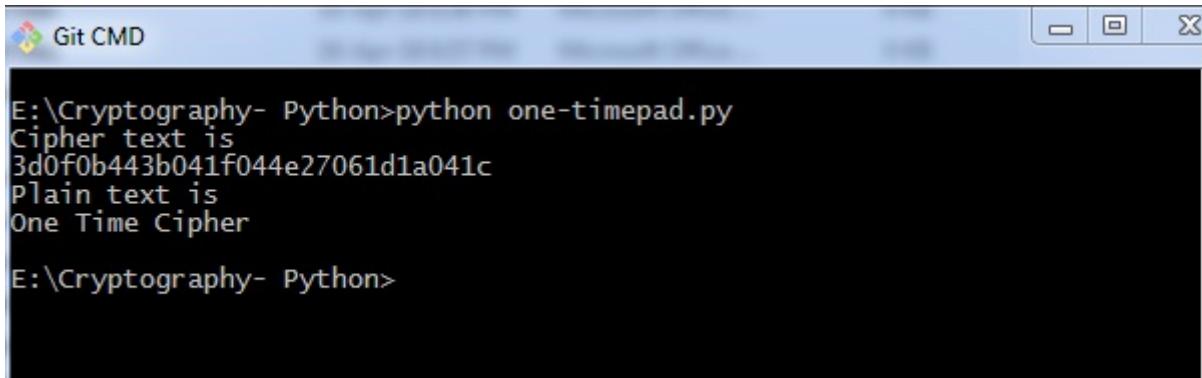
```
import onetimepad

cipher = onetimepad.encrypt('One Time Cipher', 'random')
print("Cipher text is ")
print(cipher)
print("Plain text is ")
msg = onetimepad.decrypt(cipher, 'random')

print(msg)
```

Output

You can observe the following output when you run the code given above –



Note – The encrypted message is very easy to crack if the length of the key is less than the length of message (plain text).

In any case, the key is not necessarily random, which makes one-time pad cipher as a worth tool.

Symmetric and Asymmetric Cryptography

In this chapter, let us discuss in detail about symmetric and asymmetric cryptography.

Symmetric Cryptography

In this type, the encryption and decryption process uses the same key. It is also called as **secret key cryptography**. The main features of symmetric cryptography are as follows –

- It is simpler and faster.
- The two parties exchange the key in a secure way.

Drawback

The major drawback of symmetric cryptography is that if the key is leaked to the intruder, the message can be easily changed and this is considered as a risk factor.

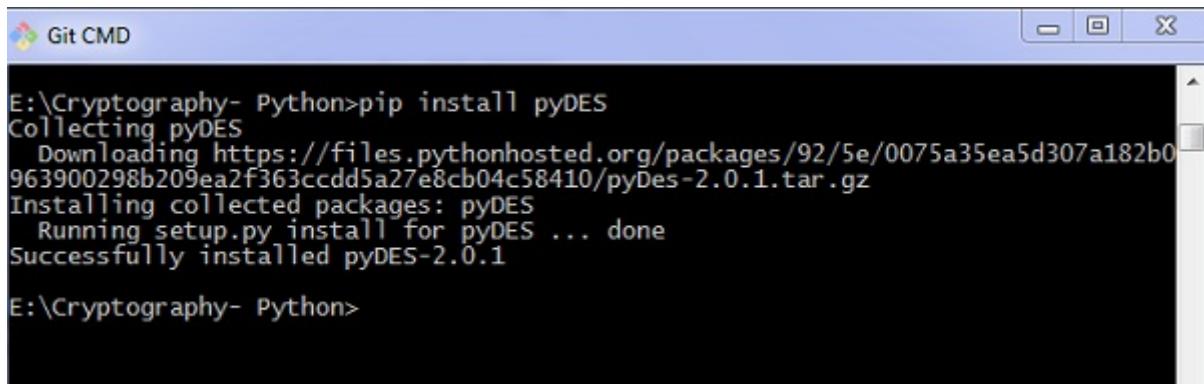
Data Encryption Standard (DES)

The most popular symmetric key algorithm is Data Encryption Standard (DES) and Python includes a package which includes the logic behind DES algorithm.

Installation

The command for installation of DES package **pyDES** in Python is –

```
pip install pyDES
```



A screenshot of a Windows Command Prompt window titled "Git CMD". The command "E:\Cryptography- Python>pip install pyDES" is entered, followed by the output of the pip install command. The output shows the package being downloaded from Python's file host, the files being extracted, and the setup process running successfully. The final message is "Successfully installed pyDES-2.0.1".

```
E:\Cryptography- Python>pip install pyDES
Collecting pyDES
  Downloading https://files.pythonhosted.org/packages/92/5e/0075a35ea5d307a182b0963900298b209ea2f363ccdd5a27e8cb04c58410/pyDes-2.0.1.tar.gz
Installing collected packages: pyDES
  Running setup.py install for pyDES ... done
Successfully installed pyDES-2.0.1
E:\Cryptography- Python>
```

Simple program implementation of DES algorithm is as follows –

```
import pyDes

data = "DES Algorithm Implementation"
k = pyDes.des("DESCRYPT", pyDes.CBC, "\0\0\0\0\0\0\0\0", pad=None, padmode=pyDes.PAD_PKCS5)
d = k.encrypt(data)

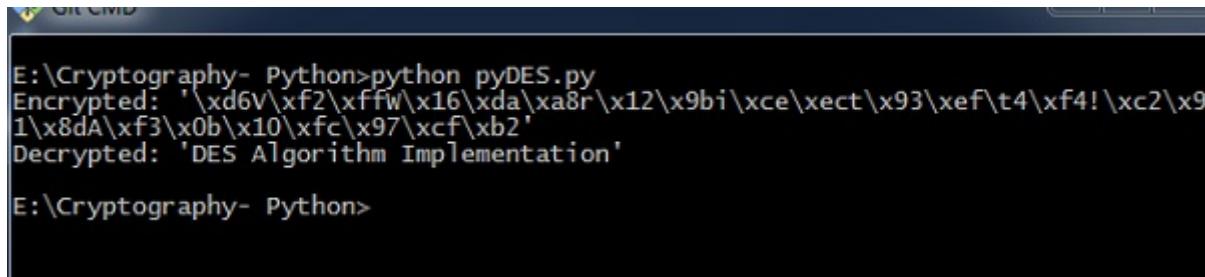
print "Encrypted: %r" % d
print "Decrypted: %r" % k.decrypt(d)
assert k.decrypt(d) == data
```

It calls for the variable **padmode** which fetches all the packages as per DES algorithm implementation and follows encryption and decryption in a specified manner.

Output

You can see the following output as a result of the code given above –





```
E:\Cryptography- Python>python pyDES.py
Encrypted: '\xd6\xf2\xfw\x16\xda\x8r\x12\x9bi\xce\xect\x93\xef\t4\xf4!\xc2\x91\x8dA\xf3\x0b\x10\xfc\x97\xcf\xb2'
Decrypted: 'DES Algorithm Implementation'

E:\Cryptography- Python>
```

Asymmetric Cryptography

It is also called as **public key cryptography**. It works in the reverse way of symmetric cryptography. This implies that it requires two keys: one for encryption and other for decryption. The public key is used for encrypting and the private key is used for decrypting.

Drawback

- Due to its key length, it contributes lower encryption speed.
- Key management is crucial.

The following program code in Python illustrates the working of asymmetric cryptography using RSA algorithm and its implementation –

```
from Crypto import Random
from Crypto.PublicKey import RSA
import base64

def generate_keys():
    # key length must be a multiple of 256 and >= 1024
    modulus_length = 256*4
    privatekey = RSA.generate(modulus_length, Random.new().read)
    publickey = privatekey.publickey()
    return privatekey, publickey

def encrypt_message(a_message , publickey):
    encrypted_msg = publickey.encrypt(a_message, 32)[0]
    encoded_encrypted_msg = base64.b64encode(encrypted_msg)
    return encoded_encrypted_msg

def decrypt_message(encoded_encrypted_msg, privatekey):
    decoded_encrypted_msg = base64.b64decode(encoded_encrypted_msg)
    decoded_decrypted_msg = privatekey.decrypt(decoded_encrypted_msg)
    return decoded_decrypted_msg

a_message = "This is the illustration of RSA algorithm of asymmetric crypt
privatekey , publickey = generate_keys()
encrypted_msg = encrypt_message(a_message , publickey)
decrypted_msg = decrypt_message(encrypted_msg, privatekey)
```

```

print "%s - (%d)" % (privatekey.exportKey() , len(privatekey.exportKey()))
print "%s - (%d)" % (publickey.exportKey() , len(publickey.exportKey()))
print " Original content: %s - (%d)" % (a_message, len(a_message))
print "Encrypted message: %s - (%d)" % (encrypted_msg, len(encrypted_msg))
print "Decrypted message: %s - (%d)" % (decrypted_msg, len(decrypted_msg))

```

Output

You can find the following output when you execute the code given above –

```

Git CMD
E:\Cryptography- Python>python RSAexample.py
-----BEGIN RSA PRIVATE KEY-----
MIICXAIKAKBgQDTtpzRwM2V9EnEzcJ/tcSm59dH+xJ/TtS5WqUjjynHMB1ReC7sympQrA0KEUXjxf68ercilEOKgdVLUh1rlfFi4nwaloqKVkwzUiCotLZGqKuDJ+a7TQae+N3pqTZBU3IyKzGqsSG+X608PKR0aEb2763Cwi+W1671JCH2RV06QIDAQAB
AoGAK5q+7cyiczkHRwuB9h/AQwgZJPAnPSVFVu++d3ZzC110jGU0dSK9QjNbrdk
B5JcdxttnQK38wzg+cAb3nC2Y03+xu86Qld23f9L3ZJqxZffp5AQa1gFF1D8NYDNA
ABmbY3jh0ZBdh7yJshlp8YpVoKo10jgs8akayMjhvV3cAAECQQDjYchk57+EJFVi
S7NeTQtRvIyh4Sn0Ay59cIyLFMn/bX7k9p8Vl7q7wtYZusHKzeFY3R1NXymLdT0a
T03hk1ABAKEA71v9C1b0SDXv08cRm7osvY9h5pMCGBneXBvq5/jWgyx5H/4d1LCI
OoUWyRtuYrYKTfgC3En/NY9ygj0ThMGk6QJAaGXa5klpKzirY0gygjeLH0oe/6wr
z4SycbGdnBzD0FzrqCB7hiR1/gNE3edbVswULQLIk1+f6YHUQYMryPggAQJBAKSP
ga4YhGJuSntNjoyTBlyA5zhG+kUlZuz0oUMx+vdo9t7t1C7JCeRCNiQh+h3QTGDz
/xwTSMzzkjzt2sTm5DECQB9ts4ExaQo0lVK+6t08WzKo1oLBdkAcPH1owTsTzpkxp
1pQJBBaS8X3v9AZIynbne0kDtNJ/0d2T9Gp8wFIUW6U=
-----END RSA PRIVATE KEY----- - (886)
-----BEGIN RSA PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDTtpzRwM2V9EnEzcJ/tcSm59dH
+xJ/TtS5WqUjjynHMB1ReC7sympQrA0KEUXjxf68ercilEOKgdVLUh1rlfFi4nwaloqKVkwzUiCotLZGqKuDJ+a7TQae+N3pqTZBU3IyKzGqsSG+X608PKR0aEb2763Cwi+W1671JCH2RV06QIDAQAB
-----END PUBLIC KEY----- - (271)
Original content: This is the illustration of RSA algorithm of asymmetric cryptography - (68)
Encrypted message: W+O+5u8uAACmuHD5GnEiObfuqr1Du92k6+qtw/b/9aurkE8DQQfMfGhMwk5DR
J1bMbxx73yKFGUGPv+T7TgAOAJBvY1FTmJn8THUbznX7t7QYwtA0euyEssHc4J8v6NMK0S/3dsExxF4II
7JfZzVp1P8Rs0o50Ix0/n91kn+1qgc= - (172)
Decrypted message: This is the illustration of RSA algorithm of asymmetric cryptography - (68)
E:\Cryptography- Python>

```

Understanding RSA Algorithm

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name **RSA** algorithm.

Algorithm

The RSA algorithm holds the following features –

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.

- There are two sets of keys in this algorithm: private key and public key.

You will have to go through the following steps to work on RSA algorithm –

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown –

$$N=p \cdot q$$

Here, let N be the specified large number.

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than $(p-1)$ and $(q-1)$. The primary condition will be that there should be no common factor of $(p-1)$ and $(q-1)$ except 1

Step 3: Public key

The specified pair of numbers **n** and **e** forms the RSA public key and it is made public.

Step 4: Private Key

Private Key **d** is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows –

$$ed = 1 \pmod{(p-1)(q-1)}$$

The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is **(n,e)**. To encrypt the plain text message in the given scenario, use the following syntax –

$$C = Pe \pmod{n}$$

Decryption Formula

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver **C** has the private key **d**, the result modulus will be calculated as –

```
Plaintext = Cd mod n
```

Creating RSA Keys

In this chapter, we will focus on step wise implementation of RSA algorithm using Python.

Generating RSA keys

The following steps are involved in generating RSA keys –

- Create two large prime numbers namely **p** and **q**. The product of these numbers will be called **n**, where **n=p*q**
- Generate a random number which is relatively prime with **(p-1)** and **(q-1)**. Let the number be called as **e**.
- Calculate the modular inverse of e. The calculated inverse will be called as **d**.

Algorithms for generating RSA keys

We need two primary algorithms for generating RSA keys using Python – **Cryptomath module** and **Rabin Miller module**.

Cryptomath Module

The source code of cryptomath module which follows all the basic implementation of RSA algorithm is as follows –

```
def gcd(a, b):  
    while a != 0:  
        a, b = b % a, a  
    return b  
  
def findModInverse(a, m):  
    if gcd(a, m) != 1:  
        return None  
    u1, u2, u3 = 1, 0, a  
    v1, v2, v3 = 0, 1, m  
  
    while v3 != 0:  
        q = u3 // v3  
        v1, v2, v3, u1, u2, u3 = (u1 - q * v1), (u2 - q * v2), (u3 - q *  
    return u1 % m
```

RabinMiller Module

The source code of RabinMiller module which follows all the basic implementation of RSA algorithm is as follows –

```
import random
def rabinMiller(num):
    s = num - 1
    t = 0

    while s % 2 == 0:
        s = s // 2
        t += 1
    for trials in range(5):
        a = random.randrange(2, num - 1)
        v = pow(a, s, num)
        if v != 1:
            i = 0
            while v != (num - 1):
                if i == t - 1:
                    return False
                else:
                    i = i + 1
                    v = (v ** 2) % num
    return True

def isPrime(num):
    if (num < 2):
        return False
    lowPrimes = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,
    67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139,
    157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 251,
    257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337,
    353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 449,
    457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557,
    563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653,
    667, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 767,
    773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 897,
    911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997]

    if num in lowPrimes:
        return True
    for prime in lowPrimes:
        if (num % prime == 0):
            return False
    return rabinMiller(num)

def generateLargePrime(keysize = 1024):
    while True:
        num = random.randrange(2**(keysize-1), 2**keysize)
        if isPrime(num):
```

```
    return num
```

The complete code for generating RSA keys is as follows –

```
import random, sys, os, rabinMiller, cryptomath

def main():
    makeKeyFiles('RSA_demo', 1024)

def generateKey(keySize):
    # Step 1: Create two prime numbers, p and q. Calculate n = p * q.
    print('Generating p prime...')
    p = rabinMiller.generateLargePrime(keySize)
    print('Generating q prime...')
    q = rabinMiller.generateLargePrime(keySize)
    n = p * q

    # Step 2: Create a number e that is relatively prime to (p-1)*(q-1).
    print('Generating e that is relatively prime to (p-1)*(q-1)...')
    while True:
        e = random.randrange(2 ** (keySize - 1), 2 ** (keySize))
        if cryptomath.gcd(e, (p - 1) * (q - 1)) == 1:
            break

    # Step 3: Calculate d, the mod inverse of e.
    print('Calculating d that is mod inverse of e...')
    d = cryptomath.findModInverse(e, (p - 1) * (q - 1))
    publicKey = (n, e)
    privateKey = (n, d)
    print('Public key:', publicKey)
    print('Private key:', privateKey)
    return (publicKey, privateKey)

def makeKeyFiles(name, keySize):
    # Creates two files 'x_pubkey.txt' and 'x_privkey.txt'
    # (where x is the value in name) with the the n,e and d,e integers written
    # delimited by a comma.
    if os.path.exists('%s_pubkey.txt' % (name)) or os.path.exists('%s_privkey.txt' % (name)):
        sys.exit('WARNING: The file %s_pubkey.txt or %s_privkey.txt already exists' % (name))
    publicKey, privateKey = generateKey(keySize)
    print()
    print('The public key is a %s and a %s digit number.' % (len(str(publicKey[0])), len(str(publicKey[1]))))
    print('Writing public key to file %s_pubkey.txt...' % (name))

    fo = open('%s_pubkey.txt' % (name), 'w')
        fo.write('%s,%s,%s' % (keySize, publicKey[0], publicKey[1]))
    fo.close()
```

```

print()
print('The private key is a %s and a %s digit number.' % (len(str(privateKey[0])), len(str(privateKey[1]))))
print('Writing private key to file %s_privkey.txt...' % (name))

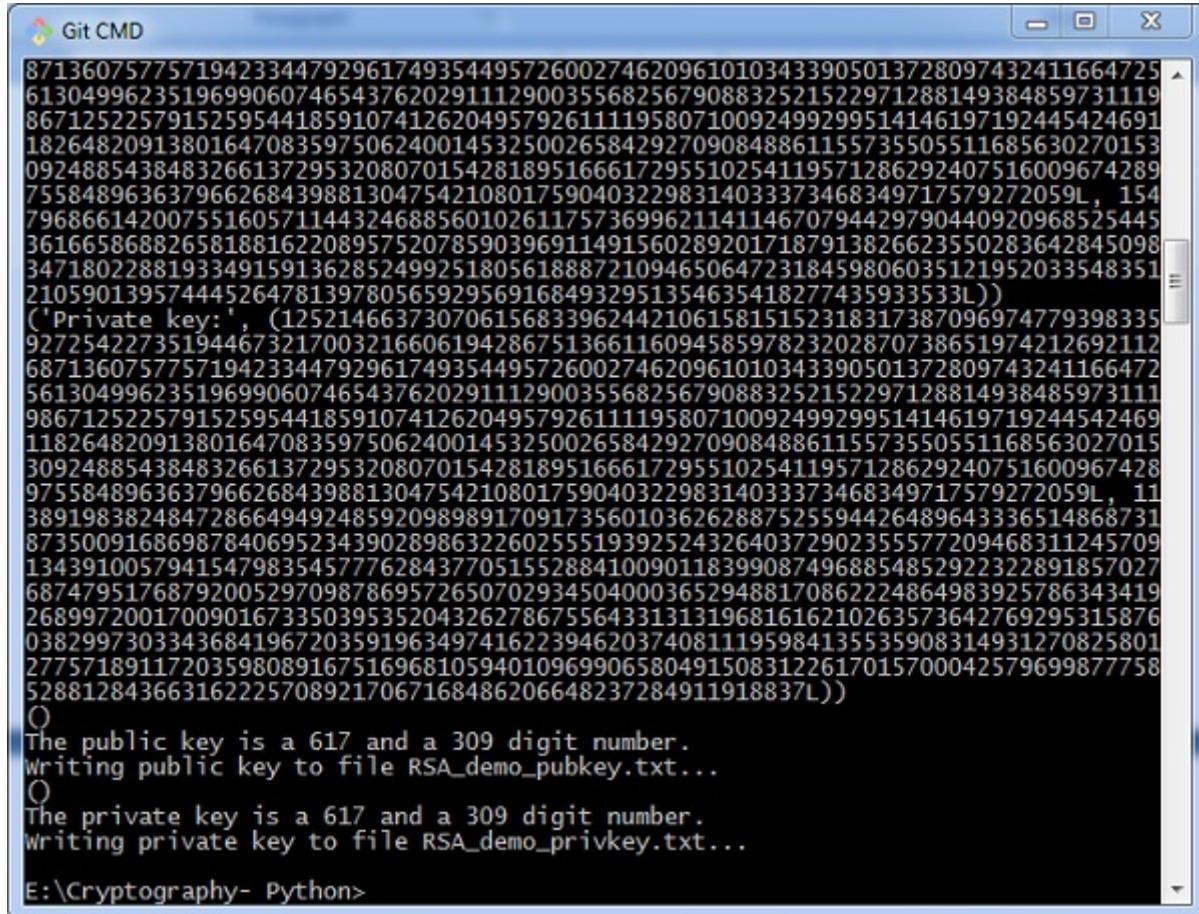
fo = open('%s_privkey.txt' % (name), 'w')
fo.write('%s,%s,%s' % (keySize, privateKey[0], privateKey[1]))
fo.close()

# If makeRsaKeys.py is run (instead of imported as a module) call
# the main() function.
if __name__ == '__main__':
    main()

```

Output

The public key and private keys are generated and saved in the respective files as shown in the following output.



```

87136075775719423344792961749354495726002746209610103433905013728097432411664725
61304996235196990607465437620291112900355682567908832521522971288149384859731119
86712522579152595441859107412620495792611119580710092499299514146197192445424691
18264820913801647083597506240014532500265842927090848861155735505511685630270153
09248854384832661372953208070154281895166617295510254119571286292407516009674289
75584896363796626843988130475421080175904032298314033373468349717579272059L, 154
79686614200755160571144324688560102611757369962114114670794429790440920968525445
36166586882658188162208957520785903969114915602892017187913826623550283642845098
34718022881933491591362852499251805618887210946506472318459806035121952033548351
210590139574445264781397805659295691684932951354635418277435933533L))
('Private key:', (12521466373070615683396244210615815152318317387096974779398335
92725422735194467321700321660619428675136611609458597823202870738651974212692112
68713607577571942334479296174935449572600274620961010343390501372809743241166472
56130499623519699060746543762029111290035568256790883252152297128814938485973111
98671252257915259544185910741262049579261111958071009249929951414619719244542469
11826482091380164708359750624001453250026584292709084886115573550551168563027015
30924885438483266137295320807015428189516661729551025411957128629240751600967428
975584896363796626843988130475421080175904032298314033373468349717579272059L, 11
38919838248472866494924859209898917091735601036262887525594426489643336514868731
87350091686987840695234390289863226025551939252432640372902355577209468311245709
13439100579415479835457776284377051552884100901183990874968854852922322891857027
68747951768792005297098786957265070293450400036529488170862224864983925786343419
26899720017009016733503953520432627867556433131319681616210263573642769295315876
03829973033436841967203591963497416223946203740811195984135535908314931270825801
27757189117203598089167516968105940109699065804915083122617015700042579699877758
5288128436631622257089217067168486206648237284911918837L))
O
The public key is a 617 and a 309 digit number.
Writing public key to file RSA_demo_pubkey.txt...
O
The private key is a 617 and a 309 digit number.
Writing private key to file RSA_demo_privkey.txt...
E:\Cryptography- Python>

```

RSA Cipher Encryption

In this chapter, we will focus on different implementation of RSA cipher encryption and the functions involved for the same. You can refer or include this python file for implementing RSA cipher algorithm implementation.

The modules included for the encryption algorithm are as follows –

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
from Crypto.Signature import PKCS1_v1_5
from Crypto.Hash import SHA512, SHA384, SHA256, SHA, MD5
from Crypto import Random
from base64 import b64encode, b64decode
hash = "SHA-256"
```

We have initialized the hash value as SHA-256 for better security purpose. We will use a function to generate new keys or a pair of public and private key using the following code.

```
def newkeys(keysize):
    random_generator = Random.new().read
    key = RSA.generate(keysize, random_generator)
    private, public = key, key.publickey()
    return public, private
def importKey(externKey):
    return RSA.importKey(externKey)
```

For encryption, the following function is used which follows the RSA algorithm –

```
def encrypt(message, pub_key):
    cipher = PKCS1_OAEP.new(pub_key)
    return cipher.encrypt(message)
```

Two parameters are mandatory: **message** and **pub_key** which refers to Public key. A public key is used for encryption and private key is used for decryption.

The complete program for encryption procedure is mentioned below –

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
from Crypto.Signature import PKCS1_v1_5
from Crypto.Hash import SHA512, SHA384, SHA256, SHA, MD5
from Crypto import Random
from base64 import b64encode, b64decode
hash = "SHA-256"

def newkeys(keysize):
    random_generator = Random.new().read
    key = RSA.generate(keysize, random_generator)
    private, public = key, key.publickey()
    return public, private

def importKey(externKey):
    return RSA.importKey(externKey)
```

```
def getpublickey(priv_key):
    return priv_key.publickey()

def encrypt(message, pub_key):
    cipher = PKCS1_OAEP.new(pub_key)
    return cipher.encrypt(message)
```

RSA Cipher Decryption

This chapter is a continuation of the previous chapter where we followed step wise implementation of encryption using RSA algorithm and discusses in detail about it.

The function used to decrypt cipher text is as follows –

```
def decrypt(ciphertext, priv_key):
    cipher = PKCS1_OAEP.new(priv_key)
    return cipher.decrypt(ciphertext)
```

For public key cryptography or asymmetric key cryptography, it is important to maintain two important features namely **Authentication** and **Authorization**.

Authorization

Authorization is the process to confirm that the sender is the only one who have transmitted the message. The following code explains this –

```
def sign(message, priv_key, hashAlg="SHA-256"):
    global hash
    hash = hashAlg
    signer = PKCS1_v1_5.new(priv_key)

    if (hash == "SHA-512"):
        digest = SHA512.new()
    elif (hash == "SHA-384"):
        digest = SHA384.new()
    elif (hash == "SHA-256"):
        digest = SHA256.new()
    elif (hash == "SHA-1"):
        digest = SHA.new()
    else:
        digest = MD5.new()
    digest.update(message)
    return signer.sign(digest)
```

Authentication

Authentication is possible by verification method which is explained as below –

```
def verify(message, signature, pub_key):
    signer = PKCS1_v1_5.new(pub_key)
    if (hash == "SHA-512"):
        digest = SHA512.new()
    elif (hash == "SHA-384"):
        digest = SHA384.new()
    elif (hash == "SHA-256"):
        digest = SHA256.new()
    elif (hash == "SHA-1"):
        digest = SHA.new()
    else:
        digest = MD5.new()
    digest.update(message)
    return signer.verify(digest, signature)
```

The digital signature is verified along with the details of sender and recipient. This adds more weight age for security purposes.

RSA Cipher Decryption

You can use the following code for RSA cipher decryption –

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
from Crypto.Signature import PKCS1_v1_5
from Crypto.Hash import SHA512, SHA384, SHA256, SHA, MD5
from Crypto import Random
from base64 import b64encode, b64decode
hash = "SHA-256"

def newkeys(keysize):
    random_generator = Random.new().read
    key = RSA.generate(keysize, random_generator)
    private, public = key, key.publickey()
    return public, private

def importKey(externKey):
    return RSA.importKey(externKey)

def getpublickey(priv_key):
    return priv_key.publickey()
```

```
def encrypt(message, pub_key):
    cipher = PKCS1_OAEP.new(pub_key)
    return cipher.encrypt(message)

def decrypt(ciphertext, priv_key):
    cipher = PKCS1_OAEP.new(priv_key)
    return cipher.decrypt(ciphertext)

def sign(message, priv_key, hashAlg = "SHA-256"):
    global hash
    hash = hashAlg
    signer = PKCS1_v1_5.new(priv_key)

    if (hash == "SHA-512"):
        digest = SHA512.new()
    elif (hash == "SHA-384"):
        digest = SHA384.new()
    elif (hash == "SHA-256"):
        digest = SHA256.new()
    elif (hash == "SHA-1"):
        digest = SHA.new()
    else:
        digest = MD5.new()
    digest.update(message)
    return signer.sign(digest)

def verify(message, signature, pub_key):
    signer = PKCS1_v1_5.new(pub_key)
    if (hash == "SHA-512"):
        digest = SHA512.new()
    elif (hash == "SHA-384"):
        digest = SHA384.new()
    elif (hash == "SHA-256"):
        digest = SHA256.new()
    elif (hash == "SHA-1"):
        digest = SHA.new()
    else:
        digest = MD5.new()
    digest.update(message)
    return signer.verify(digest, signature)
```

Hacking RSA Cipher

Hacking RSA cipher is possible with small prime numbers, but it is considered impossible if it

is used with large numbers. The reasons which specify why it is difficult to hack RSA cipher are as follows –

- Brute force attack would not work as there are too many possible keys to work through. Also, this consumes a lot of time.
- Dictionary attack will not work in RSA algorithm as the keys are numeric and does not include any characters in it.
- Frequency analysis of the characters is very difficult to follow as a single encrypted block represents various characters.
- There are no specific mathematical tricks to hack RSA cipher.

The RSA decryption equation is –

$$M = C^d \bmod n$$

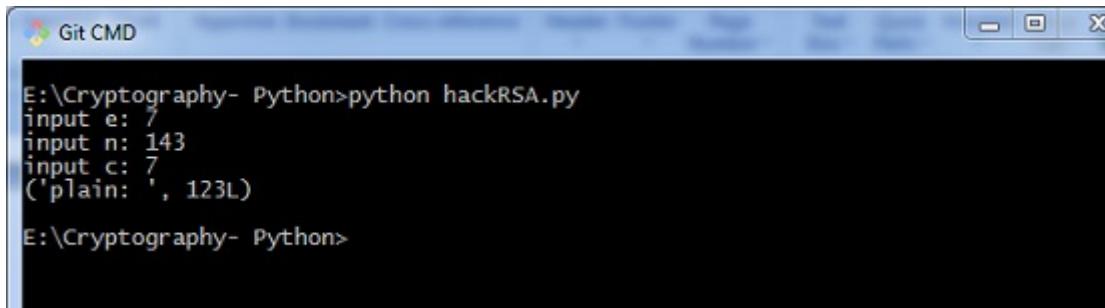
With the help of small prime numbers, we can try hacking RSA cipher and the sample code for the same is mentioned below –

```
def p_and_q(n):  
    data = []  
    for i in range(2, n):  
        if n % i == 0:  
            data.append(i)  
    return tuple(data)  
  
def euler(p, q):  
    return (p - 1) * (q - 1)  
  
def private_index(e, euler_v):  
    for i in range(2, euler_v):  
        if i * e % euler_v == 1:  
            return i  
  
def decipher(d, n, c):  
    return c ** d % n  
    def main():  
        e = int(input("input e: "))  
        n = int(input("input n: "))  
        c = int(input("input c: "))  
  
        # t = 123  
        # private key = (103, 143)  
        p_and_q_v = p_and_q(n)  
        # print("[p_and_q]: ", p_and_q_v)  
        euler_v = euler(p_and_q_v[0], p_and_q_v[1])
```

```
# print("[euler]: ", euler_v)
d = private_index(e, euler_v)
plain = decipher(d, n, c)
print("plain: ", plain)
if __name__ == "__main__":
    main()
```

Output

The above code produces the following output –



```
Git CMD
E:\Cryptography- Python>python hackRSA.py
input e: 7
input n: 143
input c: 7
('plain: ', 123L)
E:\Cryptography- Python>
```

Useful Video Courses



Conversation On Cryptography: W/ Mike Meyers

10 Lectures 2 hours

Total Seminars

[More Detail](#)



Ethical Hacking: Cryptography For Hackers

10 Lectures 2 hours

Stone River ELearning

More Detail