LAB

3

Cryptography with Python

By the end of this section, you should be able to:

- Know basic Python in programming.
- Developed basic tool to brute force a ceaser cipher.

3.1 Introduction

3.1.1 Python 101

Python is a powerful multi-purpose programming language created by Guido van Rossum with python's simple easy-to-use syntax, making it the perfect language for someone trying to learn computer programming for the first time. Support with wide range of applications such as Web development (like: Django and Bottle), scientific and mathematical computing (Orange, SymPy, NumPy) to desktop graphical user Interfaces (Pygame, Panda3D).

The syntax of the language is clean and length of the code is relatively short. It's fun to work in Python because it allows programmer to think about the problem rather than focusing on the syntax.

3.1.2 Basic Syntax

A **string** can be declared as

`str` =' HEY YOU'

Where `str` is the variable name and 'HEY YOU' is the string assigned to `str`

A **list** of data can be declared as compound of data types, separated by commas and enclosed by '['and ']'

`listofvalue`= [123, 'abc' , 456, 'xyz']

Where `listofvalue` is the name of the list and compound in the square bracket is the list of data types. A number can straight written as it is but a character or string need to written within a compound of **' '** .

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

`atupple` = (123, 'abc')

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

`adictionary` = { 'name' : 'Emran' , 'stdID' : 'B013190007' , 'Age' : 16 }

To start a python that support a cryptography package, a user need to install the cryptography package. To install the package, use the following command

```
pip install cryptography
```

3.2 Caesar Cipher

Named after Julius Caesar, who used it to communicate with his generals. It is also known as the shift cipher, Caesar's code or Caesar shift. It is one of the simplest and most widely known encryption techniques. Letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For an example, consider the key for the cipher is 3, the alphabet is shift to become

Plaintext	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
CipherText	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**

Plaintext	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
CipherText	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**

Plain text is ="WELCOME"

Cipher text is ="ZHOFRPH

Caesar ciphers are vulnerable to exhaustive key search attack where the ciphertext can be known if the code breaker work through all the 26 keys. Furthermore the key can be determined from knowledge of a single pair of corresponding plaintext and ciphertext characters

Task 1

Caesar cipher using python.

1. Open a text editor in your Kali linux
2. Write the python code below :-

```
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)
```

3. Save the code as caesordemo.py in /root/Desktop
4. To run the code go to a terminal and type

```
root@kali-linux:~ python caesordemo.py
```

- **This activity need a python to be install in the computer. For kali linux it have been preinstall in the kali**

Task 2

Brute Force Caesar Cipher using Python

Write a python program to decrypt the following Caesar ciphertext

```
MVGRZUDPULVJKZDVRWKVIKZDVZMVUFEVDPJVEKVETVSLK
TFDDZKKVUEFTIZDVREUSRUDZJKRBVJZMVDRUVRWVNZMV
YRUDPJYRIVFWJREUBZTBVUZEDPWRTVSLKZMVTFDVKYIFL
XYNVRIVKYVTYRDGZFEJDPWIZVEUJREUNVCCBVVGFEWZXY
KZEXKZCKYVVEUNVRIVKYVTYRDGZFEJNVRIVKYVTYRDGZF
EJEFKZDVWFICFJVIJTRLJVNVRIVKYVTYRDGZFEJFWKYVNFI
CUZMVKRBVEDPSFNJREUDPTLIKRZETRCCJPFLSIFLXYKDVW
RDVREUWFIKLEVREUVMVIPKYZEXKYRKXFVJNZKYZKZKYRE
BPFLRCCSLKZKJSVVEEFSVUFWIFJVJEFGCVRJLIVTILZJVZTF
EJZUVIZKRTYRCCVEXVSVWFIVKYVNYFCVYLDREIRTVREUZR
ZEKXFEERCFJVNVRIVKYVTYRDGZFEJDPWIZVEUJREUNVCC
```