

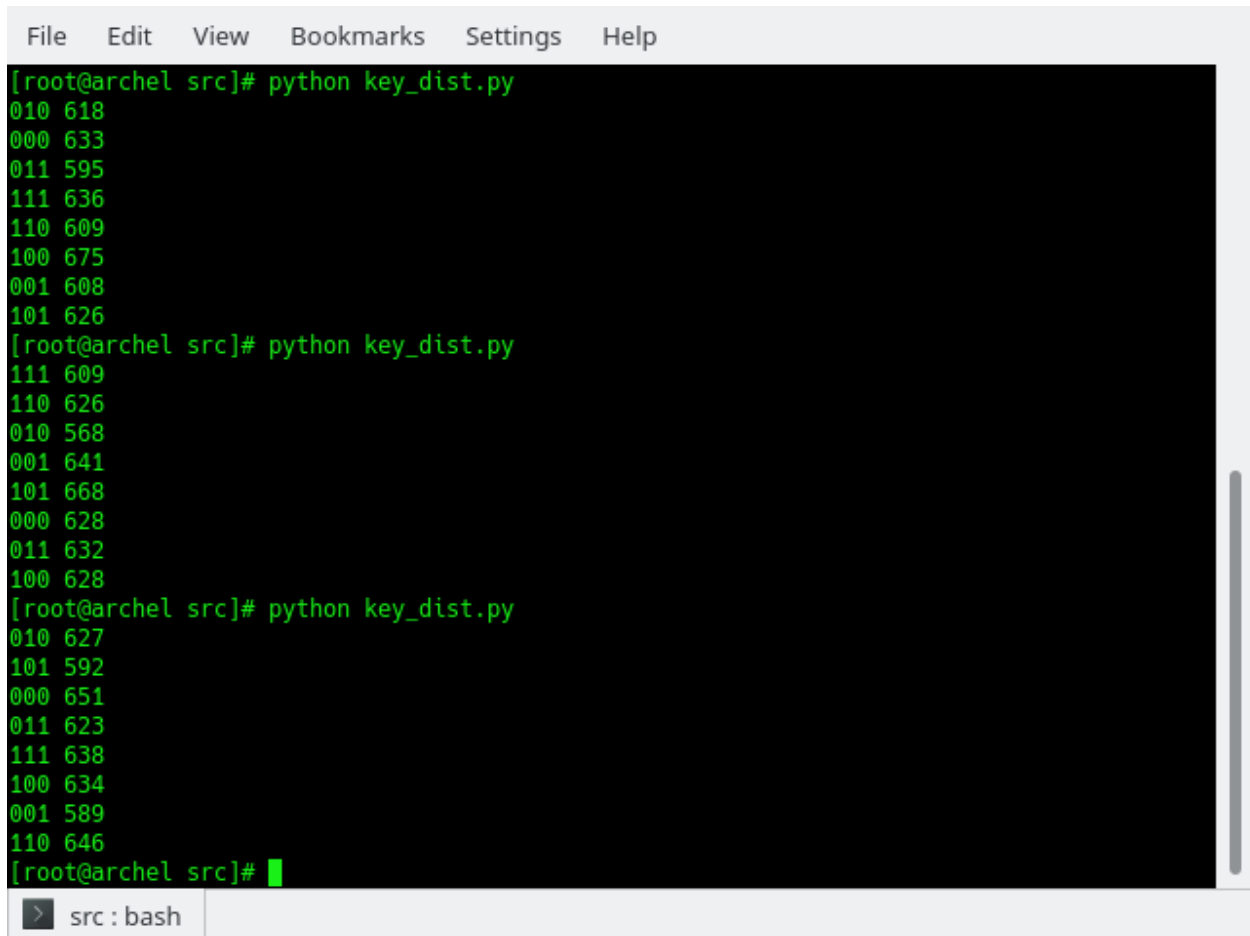
Data Security & Privacy Project 1

Due date: 2/6/2018

Raghu Pusapati

pusaparv@mail.uc.edu

5000 keys are generated randomly and their frequency distributions are calculated. The following is the output of 3 runs

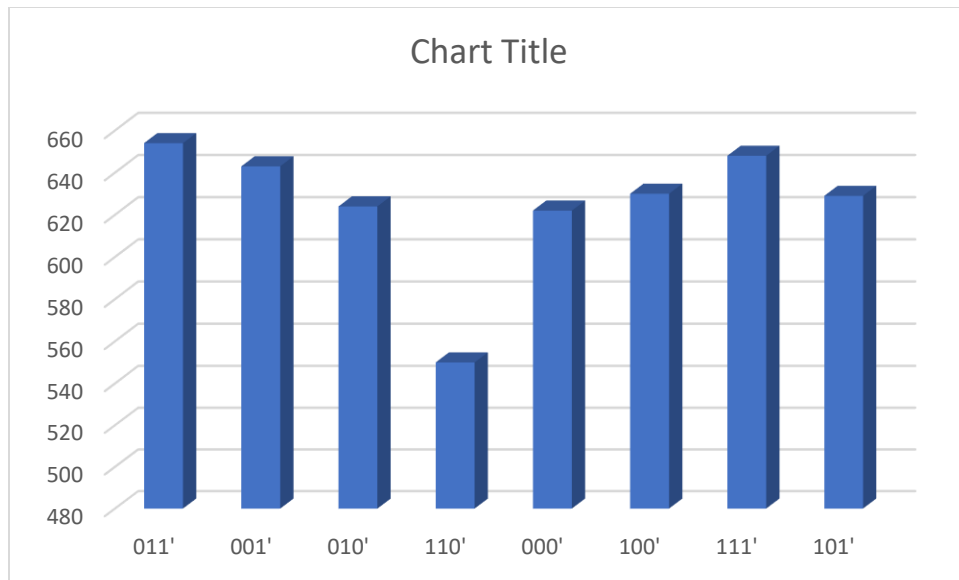


```
File Edit View Bookmarks Settings Help
[root@archel src]# python key_dist.py
010 618
000 633
011 595
111 636
110 609
100 675
001 608
101 626
[root@archel src]# python key_dist.py
111 609
110 626
010 568
001 641
101 668
000 628
011 632
100 628
[root@archel src]# python key_dist.py
010 627
101 592
000 651
011 623
111 638
100 634
001 589
110 646
[root@archel src]#
```

> src : bash

We can see clearly that the distribution is almost uniform for every key.

The following is a bar chart of frequency distribution drawn from output of one of the runs



'timeit' built-in library is used to measure execution time of 128 bit encryption. The following image shows run times of a few executions

```

[root@archel src]# python otp_timer.py enc /root/Documents/otp_12499347/data/key128.txt
/root/Documents/otp_12499347/data/plaintext128.txt /root/Documents/otp_12499347/data/ciph
ertext128.txt
0011000111001011100001000110111000100110110011111001001101111010001001111101101010000010
011001100010001111001011100100110110110
0.0006769129977328703
[root@archel src]# python otp_timer.py enc /root/Documents/otp_12499347/data/key128.txt
/root/Documents/otp_12499347/data/plaintext128.txt /root/Documents/otp_12499347/data/ciph
ertext128.txt
0011000111001011100001000110111000100110110011111001001101111010001001111101101010000010
011001100010001111001011100100110110110
0.0006305269998847507
[root@archel src]# python otp_timer.py enc /root/Documents/otp_12499347/data/key128.txt
/root/Documents/otp_12499347/data/plaintext128.txt /root/Documents/otp_12499347/data/ciph
ertext128.txt
0011000111001011100001000110111000100110110011111001001101111010001001111101101010000010
011001100010001111001011100100110110110
0.0006695629999740049
[root@archel src]# python otp_timer.py enc /root/Documents/otp_12499347/data/key128.txt /root/Documents/otp_12499347/data/plaintext1
00110001110010111000010001101110001001101100111110010011011110100010011111011010100000100110011000100011110010111001001101110110
0.0006851929938420653
[root@archel src]# python otp_timer.py enc /root/Documents/otp_12499347/data/key128.txt /root/Documents/otp_12499347/data/plaintext1
00110001110010111000010001101110001001101100111110010011011110100010011111011010100000100110011000100011110010111001001101110110
0.0006584939983440563
[root@archel src]# python otp_timer.py enc /root/Documents/otp_12499347/data/key128.txt /root/Documents/otp_12499347/data/plaintext1
00110001110010111000010001101110001001101100111110010011011110100010011111011010100000100110011000100011110010111001001101110110
0.000664368002617266
[root@archel src]# python otp_timer.py enc /root/Documents/otp_12499347/data/key128.txt /root/Documents/otp_12499347/data/plaintext1
00110001110010111000010001101110001001101100111110010011011110100010011111011010100000100110011000100011110010111001001101110110
0.0006930649979040027
[root@archel src]# python otp_timer.py enc /root/Documents/otp_12499347/data/key128.txt /root/Documents/otp_12499347/data/plaintext1
00110001110010111000010001101110001001101100111110010011011110100010011111011010100000100110011000100011110010111001001101110110
0.0047114219996728934
[root@archel src]# python otp_timer.py enc /root/Documents/otp_12499347/data/key128.txt /root/Documents/otp_12499347/data/plaintext1
00110001110010111000010001101110001001101100111110010011011110100010011111011010100000100110011000100011110010111001001101110110
0.0006647249974776059
[root@archel src]# █

```

The average execution time is 0.000667 seconds.

Other details about OS and execution are described in the Readme file.