Assignment 1
SIL765

Gaurav Chauhan
2018CS50406

Question 3.

In this question we had to calculate the value of the prime numbers.

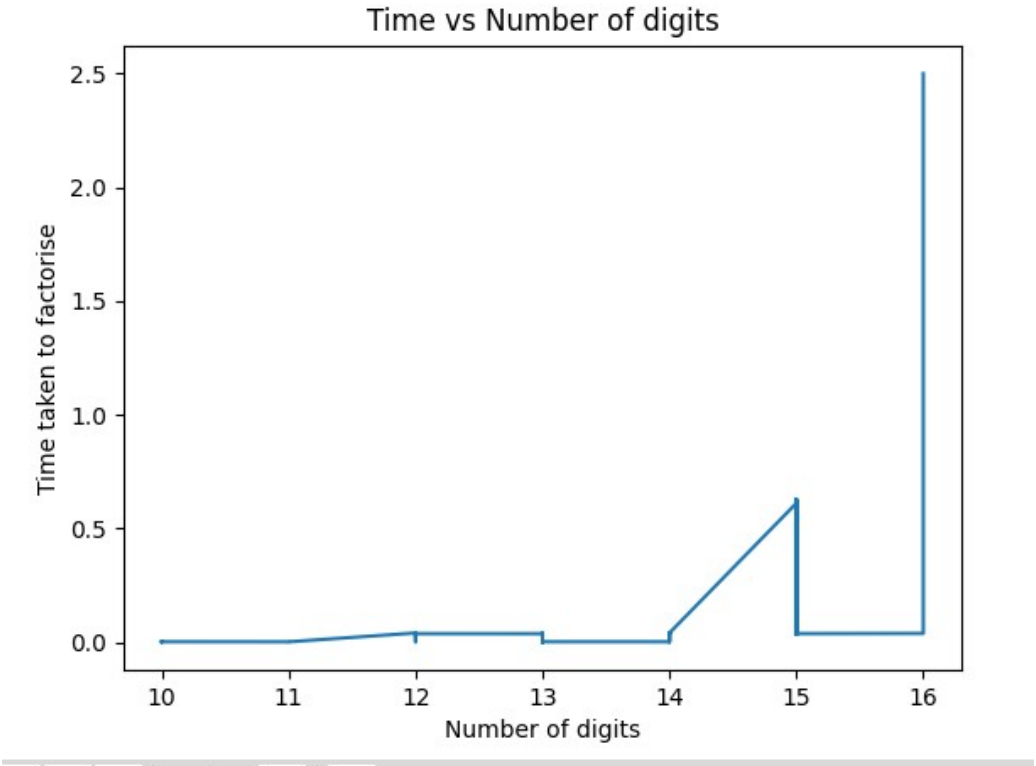
This was done through two approaches:-

1) In this case I used a library to implement the quadratic sieve (https://github.com/skollmann/PyFactorise). In this case I used this and easily factorised all the inputs.

2) The other method was used in which I first checked divisibility of the input value with 2, if it was not divisible then I used 3 and tried factorizing the input uptil sqrt(n) + 1. This method calculated the prime factor for the input number of max 21 digits.

The next step was to calculate the encrypted value and then to decrypt it. For this I made a function know as power which calculated the value of (a^b)%p through the use of the modulus property which is (a*b)%p == ((a%p)*(b%p))%p

The graph of the time vs the number of digits in the input is as follows for the first 50 numbers:-



RUNNING COMMANDS:

python3 crack.py nlist.txt

here the plain.txt message is assumed to be the same.