Problem3

Method :

1. Get user input N.
2. Factorize N into prime factors p and q.
3. Generate phi = (p-1)(q-1).
4. Choose e such that “gcd(e,phi) = 1” and “1< e < phi”.
5. Find d with “e.d(mod phi) = 1” and 1 < d < phi” using extended euclidean for faster computation.

Encrypt : Plaintext ‘M’ to get Ciphertext ‘C’ by “C = (M)^e (mod N)”.
Decrypt : Ciphertext ‘C’ to get Plaintext ‘P’ by “P = (C)^d (mod N)”.

Run command : python crack.py 69149675305266529.

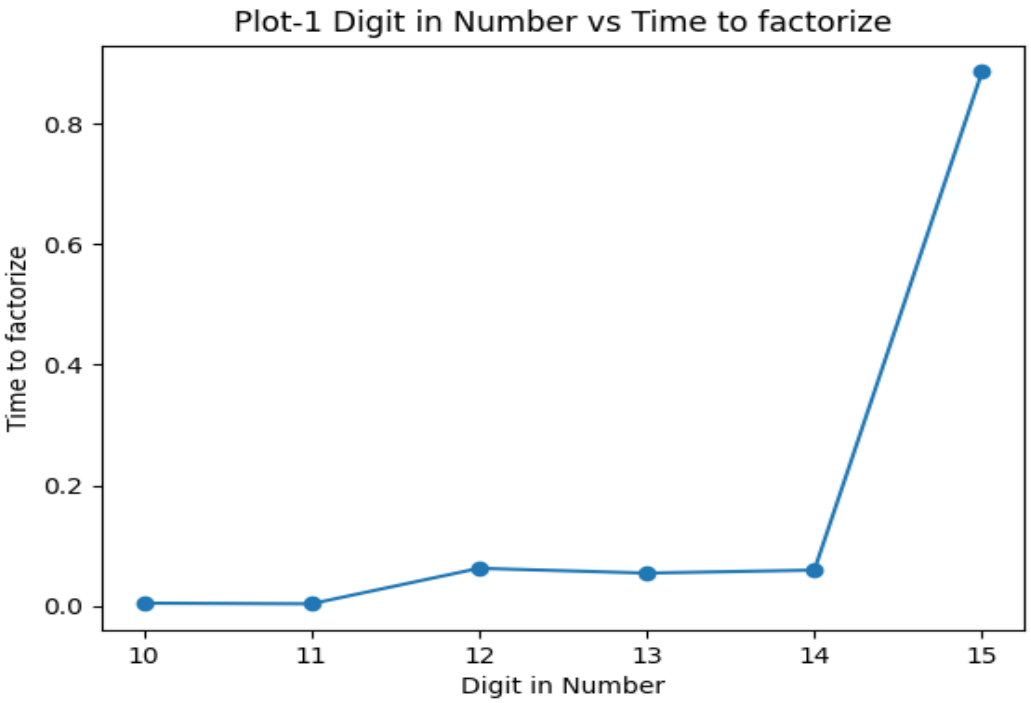
Largest N to factorize within 5 minutes = 996770894558194342950388849 (27 digits)

System Specification :

- Processor :Intel core i-7.
- Ram : 8GB
- Language : Python 3.6

Output Window

```
(venv) C:\SEM2\NSS\problem_3>python crack.py 996770894558194342950388849
factor  1067982407   933321455508016007
Time Taken to factorize N(digit)  27   101.61545372009277
encryption Key= 711342572245523921124408 5 decryption Key= 44295625452137963201078345 number= 996770894558194342950388849
plainText  haha, I can encode stuff that you cannot decode
cipherText  334318788708505980148540951 6337828293821343335741210537 334318788708505980148540951 6337828293821343335741210537 80396209418755643294943077 2 1331
312711023018637835629 64 6648949306439183736896290 22 1331312711023018637835629 64 6478726943228997559726302 69 6337828293821343335741210537 5013459115542102331 7
6955672 1331312711023018637835629 64 7380301208193632411908176 35 5013459115542102331769556 72 6478726943228997559726302 69 1124241560535667719819715 06 2187975 9
780627140284908104 7 7380301208193632411908176 35 1331312711023018637835629 64 1931710432156832771206386 41 6511005100296715650811069 81 2892136965939958166695 97
933 8391882962968364269022539 5 8391882962968364269022539 5 1331312711023018637835629 64 6511005100296715650811069 81 3343187887085059801485409 51 6337828293821 3
4335741210537 6511005100296715650811069 81 1331312711023018637835629 64 7852005733714485057837471 04 1124241560535667719819715 06 2892136965939958166695979 33 13
313127110230186378356296 4 6478726943228997559726302 69 6337828293821343335741210537 5013459115542102331769556 72 5013459115542102331769556 72 1124241560535667 71
981971506 6511005100296715650811069 81 1331312711023018637835629 64 2187975978062714028490810 47 7380301208193632411908176 35 6478726943228997559726302 69 112424
156053566771981971506 2187975978062714028490810 47 738030120819363241190817635
plainText  haha, I can encode stuff that you cannot decode
```


Plot-1 Digit in Number vs Time to factorize
Time to factorize
0.0
0.2
0.4
0.6
0.8
10
11
12
13
14
15
Digit in Number