1 Cracking RSA

To run the script do: (Note here python2 has been used)

`cd problem-3`, `python2 crack.py n`

RSA Algorithm is an asymmetric cryptography algorithm. The algorithm makes use of Public Key and Private Key. Messages encrypted through public key can only be correctly decrypted through private key. As the name describes the public key is given to everyone and the private key is kept private.

Idea of RSA Algorithm:

RSA algorithm is based on the fact that it is very difficult to factorize large integers. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

RSA Algorithm:

- Factorize n

  if $n \leq 10^{20}$ then use Pollard-Rho to factorize n otherwise use ECM to factorize n

- Key Setup

  Obtain the prime factors p, q such that $n = p \cdot q$

  Compute $\phi = (p-1) \cdot (q-1)$

  Choose an integer e such that $\gcd(e, phi) = 1$

  Choose an integer d such that $(d \cdot e) \bmod \phi = 1$

  Publish the public key $\{e, n\}$

  Keep the private key $\{d, n\}$

- Encryption

  Convert the characters of the plain text to numbers.

  Use the public key K and compute the cipher text as $C = M^e \bmod n$

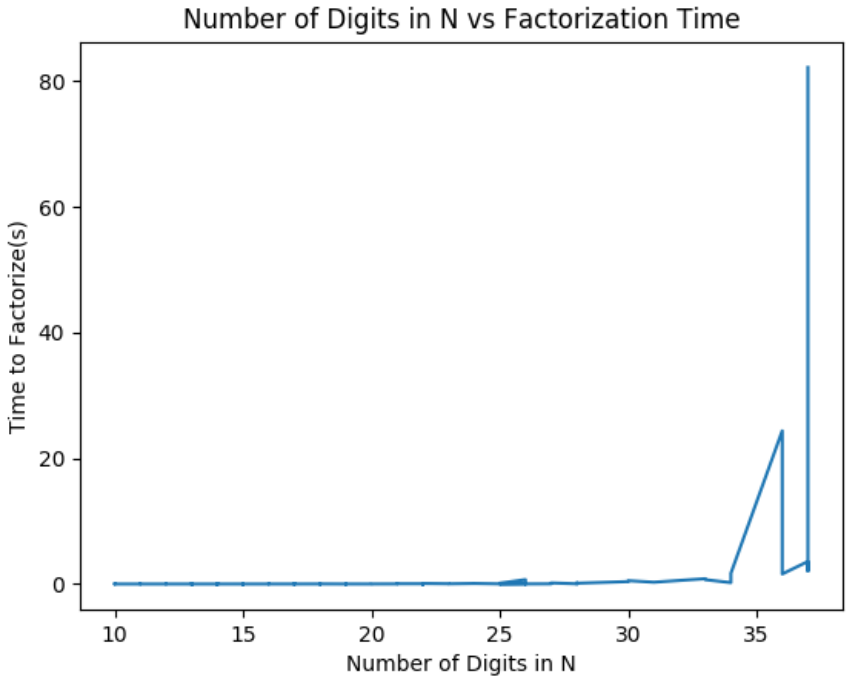
  Convert the numbers of cipher text to characters.

- Decryption

  Convert the characters of the cipher text to numbers.

  Use the private key K and compute the plain text as $M = C^d \bmod n$

2 Time to factorize vs number of digits in n



Observations: In the given file 'nlist.txt' there are several numbers which are square of a prime numbers. But for RSA algorithm to decrypt the cipher text correctly both p and q should be distinct. The following are such numbers in the given file:
2605796209, 3678058609, 3694086841, 4303234442515849, 961801438520428081, 116517380705369133516848889, 840859136266769099141989302482624329, 131687290707360806646882657121529428 9

Configuration of laptop used: Intel i5

Largest n cracked within 5 minutes: All the numbers in the file are cracked within 5 minutes. Largest number of digits in the file is 37.

Conclusion: The time required to factorize is very low but increases slowly when the number of digits in n increases.