PRIME NUMBER FACTORIZATION

Title -

Implementation of prime number factorization for very large numbers with User Interface

Description-

What is Prime Factorization?

Prime factorization is a way of expressing a number as a product of its prime factors. A prime number is a number that has exactly two factors, 1 and the number itself.
For example - 330 = 2 x 3 x 5 x 11
2,3,5,11 are prime factors of number 330.

In this way we can express every number as a product of its prime factors.Prime factorization is similar to factoring a number and considering only the prime numbers (2, 3, 5, 7, 11, 13, 17, 19, and so on) among all the factors.

Methods to find Prime Factorization

There are various methods to find the prime factorization of a number. The most common methods used to find the prime factorization are:

- Prime factorization using factor tree method
- Division method of prime factorization

And there is another method called **Pollard's rho algorithm**.Pollard's rho algorithm is an algorithm for integer factorization. It was invented by John Pollard in 1975. It uses only a small amount of space, and its expected

running time is proportional to the square root of the size of the smallest prime factor of the composite number being factorized. Its time complexity is very less compared to other methods.

Prime Factorization using Factor Tree Method

In the factor tree method, the factors of a number are found and then those numbers are further factorized until we reach the prime numbers. We have to consider the number as the root of the tree that is at the top of the factor tree. Then write down the corresponding pair of factors as the branches of the tree.Factorize the composite factors that are found in step 2, and write down the pair of factors as the next branches of the tree.We have to do it until we get the prime factors of all the composite factors.

Division Method of Prime Factorization

The division method can also be used to find the prime factors of a large number by dividing the number by prime numbers.In this method we divide the number by smallest prime number such that the smallest prime number should divide the number completely.We have to do divisions for all the numbers less than square root of given number until quotient becomes 1.

Pollard's rho algorithm

Given an integer n which we assume has a small factor we choose some x_0

(often $x_0 = 2$), and we choose $f(x) = x^2 + 1$ (this is typical). We generate $x_1 = f(x_0)$ reduced mod n,

$x_2 = f(x_1)$ reduced mod n, and so on. At each even subscript x_2x we calculate gcd $(x_2s - xs, n)$ and

immediately upon obtaining a number greater than 1 we are done.

By using this method we can compute whether a number is prime or not easily by using less time complexity. This method uses a miller rabin test to ny using random function to generate random integers.

Applications of Prime Factorization

There is a wide range of properties of prime factorization. The two most important applications of the prime factorization are :

- Cryptography and Prime Factorization
- HCF and LCM Using Prime Factorization

Cryptography and Prime Factorization

Cryptography is a method of protecting information and communicating cryptography through the use of codes. Prime factorization plays an important role for the coders who want to create a unique code using numbers that is not too heavy for computers to store or process quickly.

Source code of the project -

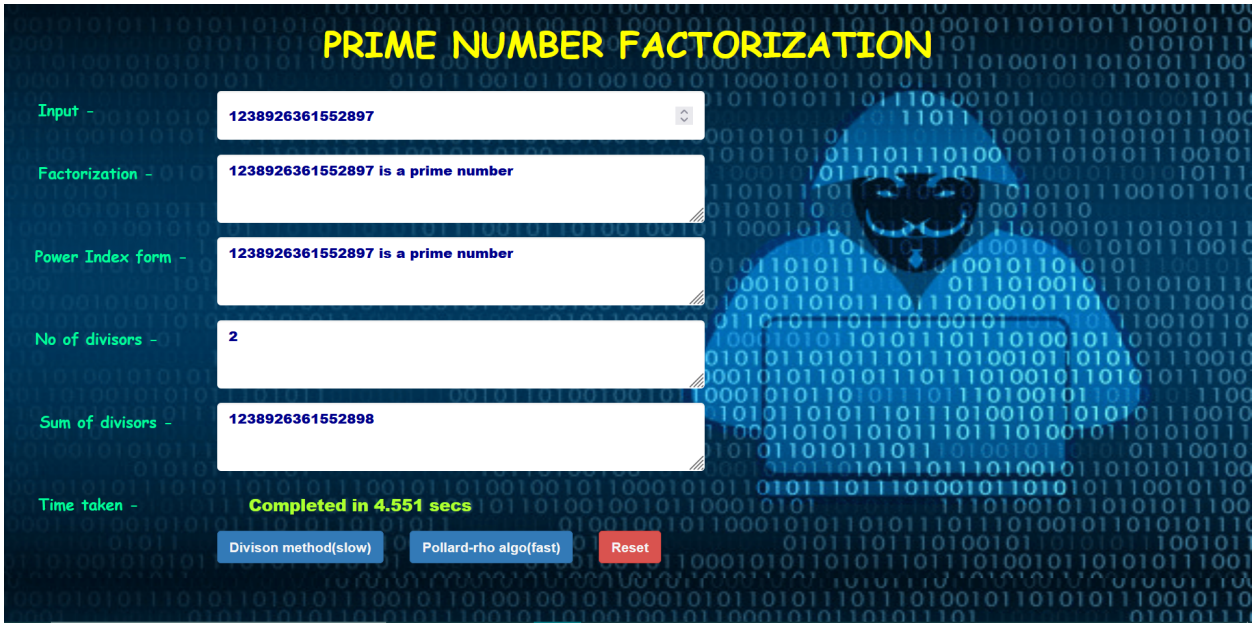
Pushed our codes into the github repository and attached the link.

Link to repository

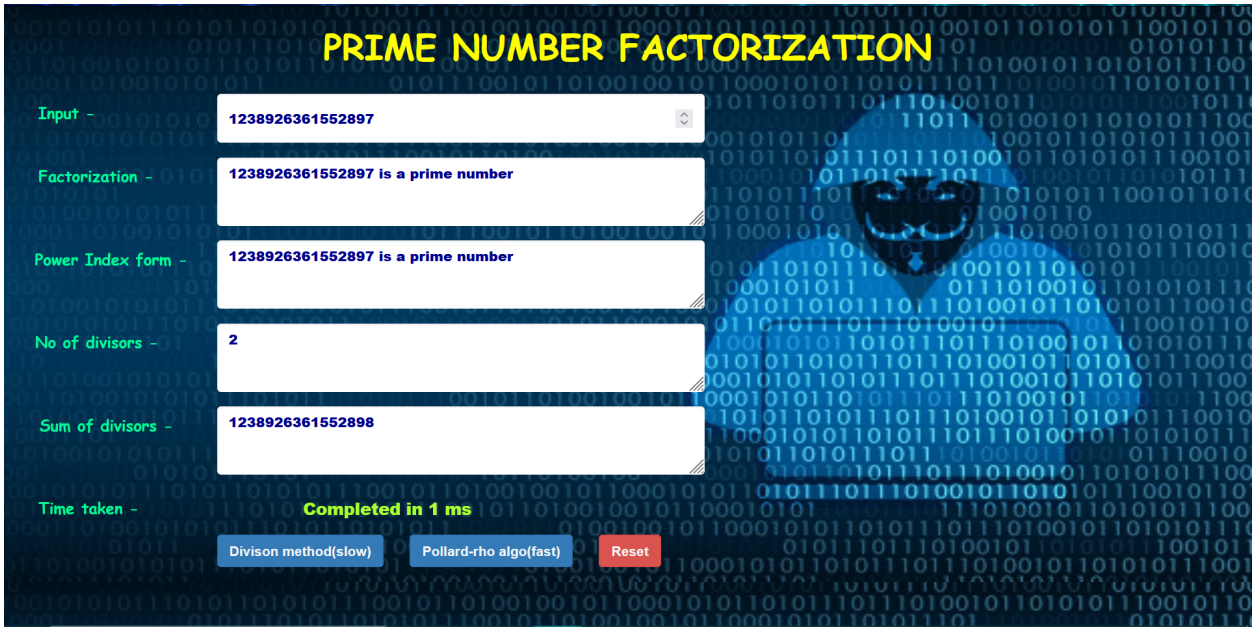
Screenshots of the outputs -

For prime number -

Division method - took 5 secs



Pollard rho method - Took 1 ms



For larger number which is product of 2 large primes

Division method - Took ~ 1minute

Pollard rho method - Took 6 secs