**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Московский Авиационный Институт»**

**(Национальный Исследовательский Университет)**

**Институт: №8 «Информационные технологии   
и прикладная математика»   
Кафедра: 806 «Вычислительная математика   
и программирование»**

Лабораторная работа № 2   
по курсу «Криптография»

Группа: М8О-306Б-21

Студент: В.Р. Орусский

Преподаватель: А. В. Борисов

Оценка:

Дата: 14.05.2024

Москва, 2024

**ОГЛАВЛЕНИЕ**

[1 Тема 3](#_Toc158983147)

[2 Задание 3](#_Toc158983148)

[3 Теория 4](#_Toc158983149)

[4 Ход лабораторной работы 5](#_Toc158983150)

[5 Выводы 6](#_Toc158983151)

# **Тема**

Факторизация больших чисел – разложение на нетривиальные сомножители

# **Задание**

Даны числа , требуется разложить их на нетривиальные сомножители.

Вариант 14:

# **Теория**

Факторизация натурального числа – его разложение в виде простых множителей. Основная теорема арифметики утверждает, что любое натуральное число может быть факторизовано. Факторизация числа считается вычислительно сложной задачей. Данное предположение (не было доказано обратного) лежит в основе разных криптографических алгоритмов с открытым ключом, среди которых RSA.

Для решения этой вычислительной задачи используются разные алгоритмы, среди которых:

* Перебор возможных делителей
* Метод факторизации Ферма
* Алгоритм Полларда
* Метод Лемана
* Метод квадратичного решета

RSA - аббревиатура от фамилий Rivest, Shamir и Adleman, так называется криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших полупростых чисел (произведение двух простых). Данный алгоритм используется в большом количестве криптографических приложений, среди которых PGP, SSL и т.д. Для реализации данного алгоритма необходимо взаимодействовать с перемножением простых чисел, что приводит нас к процессу факторизации. Поскольку от надёжности RSA алгоритма зависит безопасность огромного количества информации, существует одноимённая задача на факторизацию определённых больших чисел.

RSA Factoring Challenge – задача, поставленная RSA Laboratories 18 марта 1991 года с целью вычисления факторизации больших целых чисел и взломом ключей RSA, используемых в криптографии. Они опубликовали список полупростых чисел (чисел с ровно двумя простыми множителями), известных как числа RZA, с денежным призом за успешную факторизацию некоторых из них. Самое маленькое из них, 100-значное число после запятой, называемое RSA-100, было вычислено к 1 апреля 1991 года. Многие из больших чисел до сих пор не были разложены и такая ситуация ожидается ещё долгое время. На данный момент RSA-250 – максимальные числа, которые удалось факторизовать.

# **Ход лабораторной работы**

Для факторизации данных чисел, я использовал готовое решение – сайт [alpertron.com.ar](https://www.alpertron.com.ar/ECM.HTM), на котором реализован алгоритм факторизации Ленстры с помощью элептических кривых (ECM), занимает 3-е место по скорости факторизации среди всех алгоритмов. Является одним из лучших для нахождения делителей длины 20-25 знаков.

Числоудалось факторизовать за 4 минуты, получив два множителя:

1. 573 733447 260765 268493 955136 095177 485171
2. 652 667025 596202 591708 982935 779112 779639

Результат работы представлен на рисунке 1:

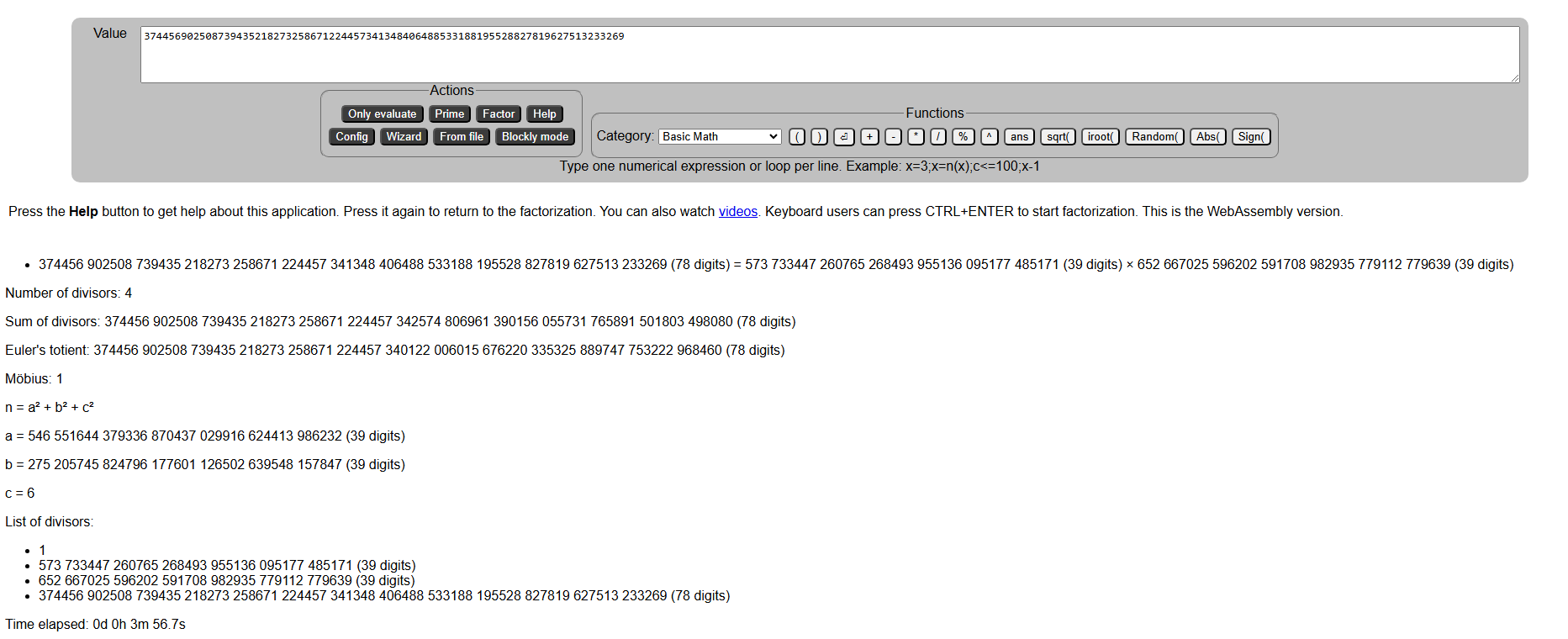


Рис. №1

Числоимеет длину 462 символа, а как мы знаем из теории, на данный момент наибольшее факторизованное число имело 250 символов, поэтому, данное число факторизовать за разумное время не получилось.

# **Выводы**

В процессе выполнения данной работы, я познакомился с понятием факторизации больших целых чисел, с различными алгоритмами для этого. Узнал о том, как факторизация связана с ключами RSA, что их безопасность напрямую зависит от разложения больших чисел на 2 множителя. Так же ознакомился с реализациями некоторых алгоритмов факторизации, что было очень интересно и полезно.

# **Список используемой литературы**

1. RSA Factoring Challenge - [https://en.wikipedia.org/wiki/](https://en.wikipedia.org/wiki/RSA_Factoring_Challenge)
2. RSA - <https://ru.wikipedia.org/wiki/RSA>
3. Факторизация целых чисел - [https://ru.wikipedia.org/wiki/](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%86%D0%B5%D0%BB%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB)
4. Факторизация с помощью эллиптических кривых - <https://ru.wikipedia.org/wiki/\>
5. Инструмент для факторизации - [https://www.alpertron.com.ar/](https://www.alpertron.com.ar/ECM.HTM)