**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-308Б-21

Студент(ка): К.А.Белоносов

Преподаватель: А. В. Борисов

Оценка:

Дата: 21.03.2024

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 чисел

# **Задание**

Разложить каждое из чисел n1 и n2 на нетривиальные сомножители (Вариант 3):

n1=344845228130159226488163571070417679235025139015802019152516926202711846660141,

n2=1626570592384034401231059859408455254810050911431145580773817320385445678597776695068312796145258618012655448521816316108022278762520239267979899184627816793656580906379077745825130933420781919802013703405155696033529555793998359389173755887366857329131343206148632506258546398761725587714083008828347727071434771944964364829767905778186912771898431501076025378480110831840332479020783206206190405100394982218769269156393531604603604142841091039265485070414672259

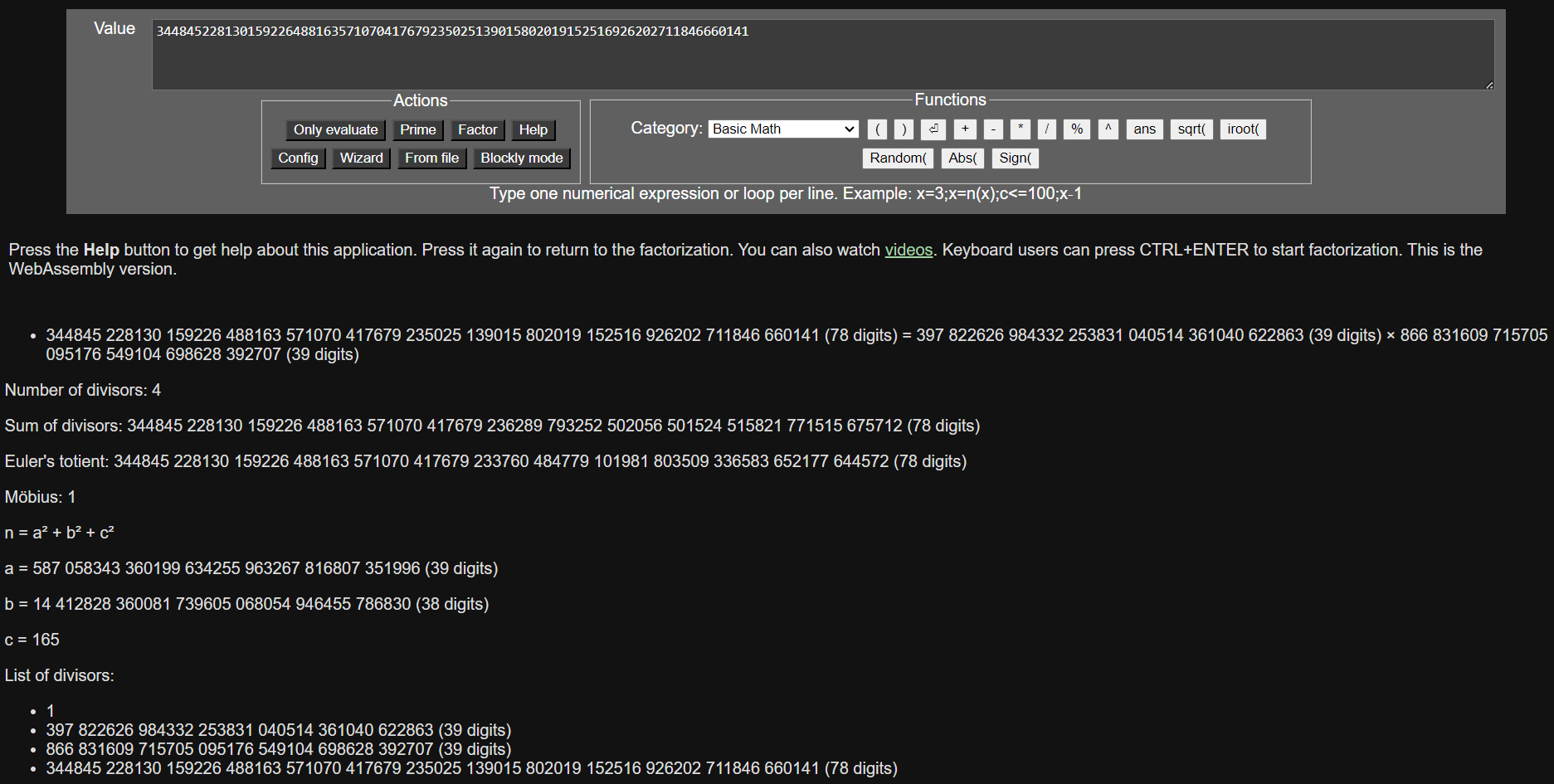
# **Теория**

**Факторизация чисел** — это процесс разложения числа на множители, то есть на более мелкие числа, которые при перемножении дают исходное число. Для простых чисел единственные множители — это 1 и само число, потому что простые числа нельзя разложить на более мелкие делители. В контексте криптографии, интерес представляют большие числа, особенно произведения двух больших простых чисел. На текущий момент не существует эффективного алгоритма, который мог бы быстро факторизовать такие числа, что делает их отличной основой для создания криптографических систем. Одна из основных причин, почему факторизация чисел так важна в криптографии, заключается в том, что она позволяет создавать однонаправленные функции. Это такие функции, которые легко вычислить в одну сторону, но чрезвычайно трудно — в обратную без специального ключа. В случае с факторизацией легко умножить два больших простых числа, но очень сложно разложить их произведение обратно на эти простые числа без знания каких-либо дополнительных данных.

**RSA (Rivest–Shamir–Adleman)** — это один из первых публичных криптографических алгоритмов с открытым ключом, широко используемых для безопасного обмена данными. Основа его безопасности заключается именно в сложности задачи факторизации больших чисел.

# **Ход лабораторной работы**

Для факторизации первого числа я воспользовался сайтом: <https://www.alpertron.com.ar/ECM.HTM>

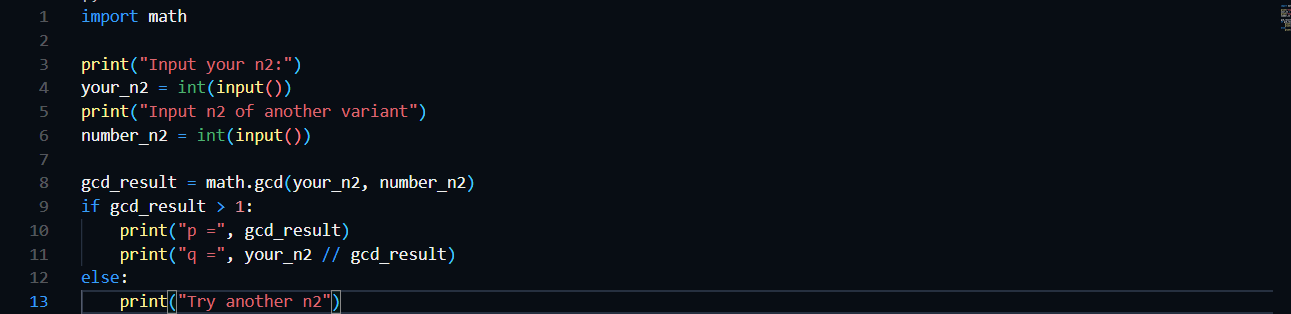


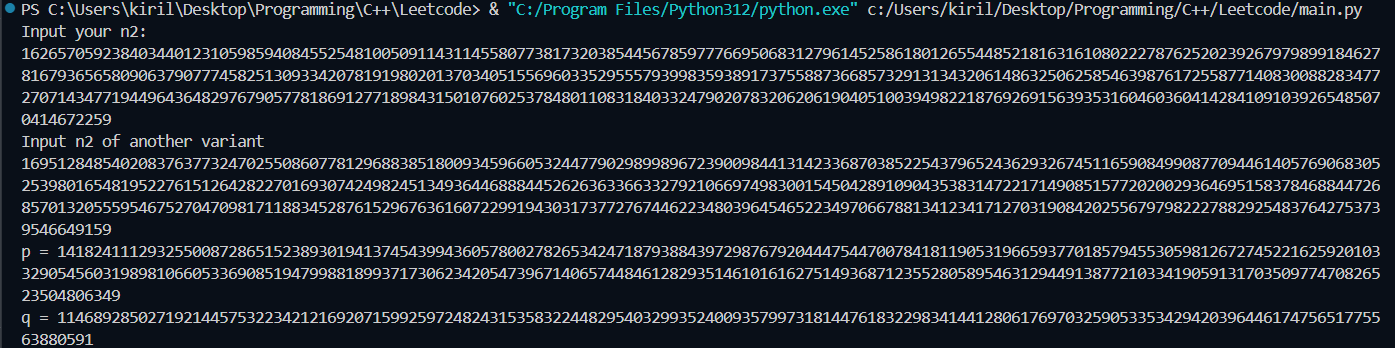
Как можно заметить, число имеет 4 делителя: единицу, само себя и 2 простых числа.

p = 397822626984332253831040514361040622863

q = 866831609715705095176549104698628392707

Так как следующее число слишком большое для разложения с помощью онлайн калькулятора. Тогда чтобы получить делители я написал скрипт на языке Python, чтобы находить GCD (Наибольший общий делитель) между моим числом n2 и числами других вариантов. Мне подошло число из первого варианта. Чтобы найти второй делитель, я поделил своё число n2 на найденное GCD



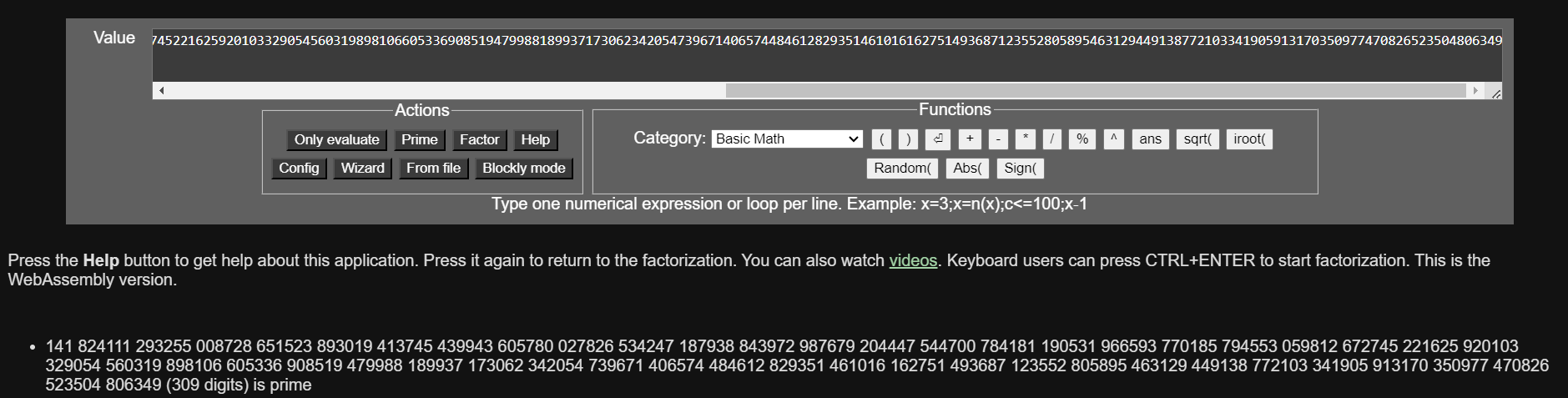


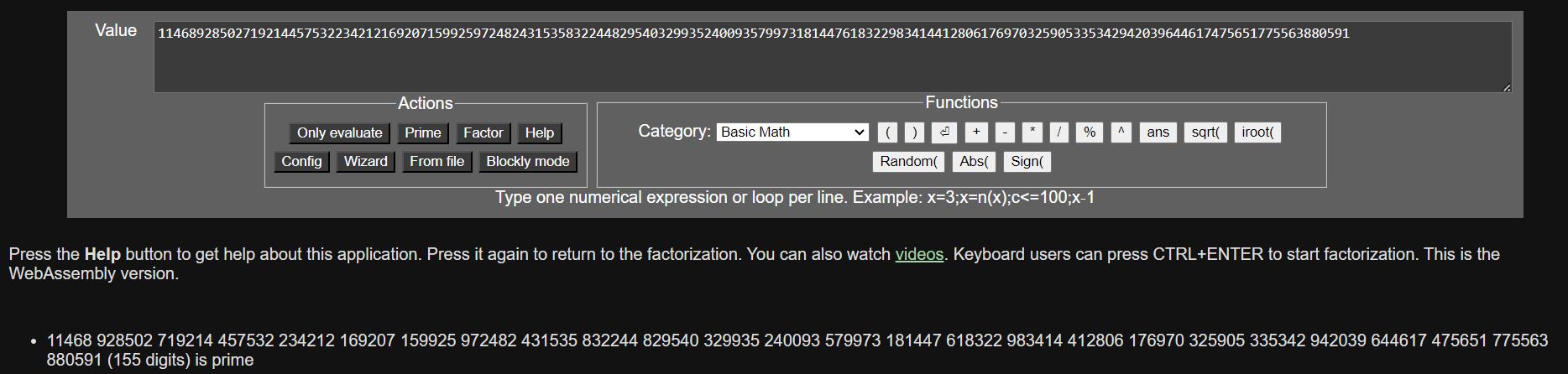
В результате были получены числа:

p = 141824111293255008728651523893019413745439943605780027826534247187938843972987679204447544700784181190531966593770185794553059812672745221625920103329054560319898106605336908519479988189937173062342054739671406574484612829351461016162751493687123552805895463129449138772103341905913170350977470826523504806349

q = 11468928502719214457532234212169207159925972482431535832244829540329935240093579973181447618322983414412806176970325905335342942039644617475651775563880591

Чтобы убедиться, что я сделал все правильно, я с помощью того же калькулятора я проверил числа на простоту





# **Выводы**

В результате данной лабораторной работы были факторизованы 2 больших числа. Данное действие относит к использованию факторизации в криптографических алгоритмах, таких как RSA. Использование перемножения двух больших простых чисел является основой построения таких алгоритмов

# **Список используемой литературы**

<https://www.alpertron.com.ar/ECM.HTM>

<https://habr.com/ru/sandbox/163811/>

<https://en.wikipedia.org/wiki/Integer_factorization>

<https://www.geeksforgeeks.org/gcd-in-python/>

<https://en.wikipedia.org/wiki/RSA_(cryptosystem)>