Московский Авиационный Институт

(Национальный Исследовательский Университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

**Лабораторная работа №2 по курсу**

**«Криптография»**

Студент: Почечура Артемий Андреевич

Группа: М80-306Б-20

Преподаватель: Борисов Август Валерьевич

Дата: 06.04.2023

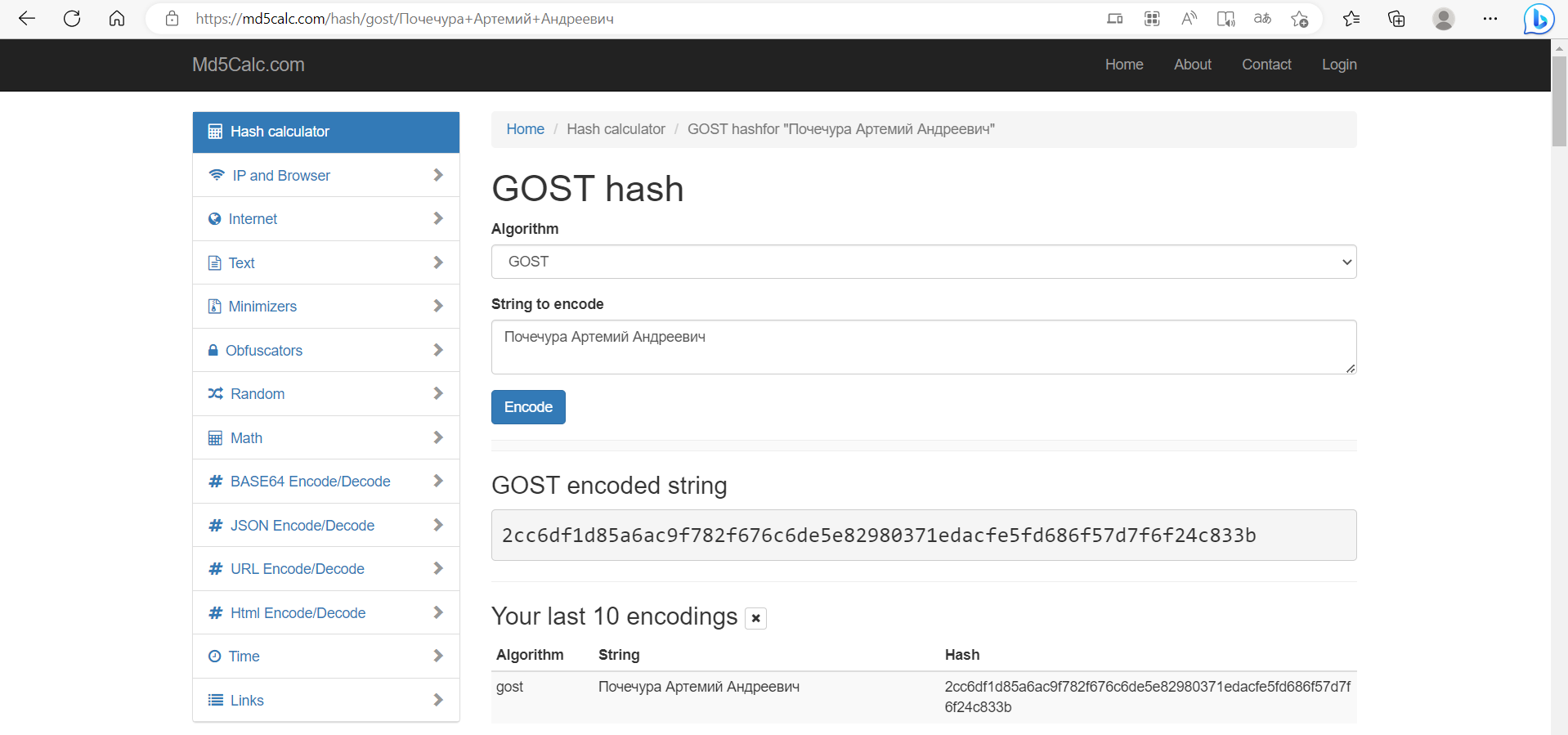
Оценка:

Подпись: \_\_\_\_\_\_\_\_\_\_\_

Москва, 2023

**1. Генерация варианта**

Получение варианта осуществлялось при помощи сайта 'https://md5calc.com/hash/gost'. На нём была выбрана хэш-функция, соответствующая ГОСТу, и поданы на вход мои ФИО. Из полученной строки, представленной в шестнадцатеричном виде, нужно выбрать младший разряд. Он будет являться моим вариантом.

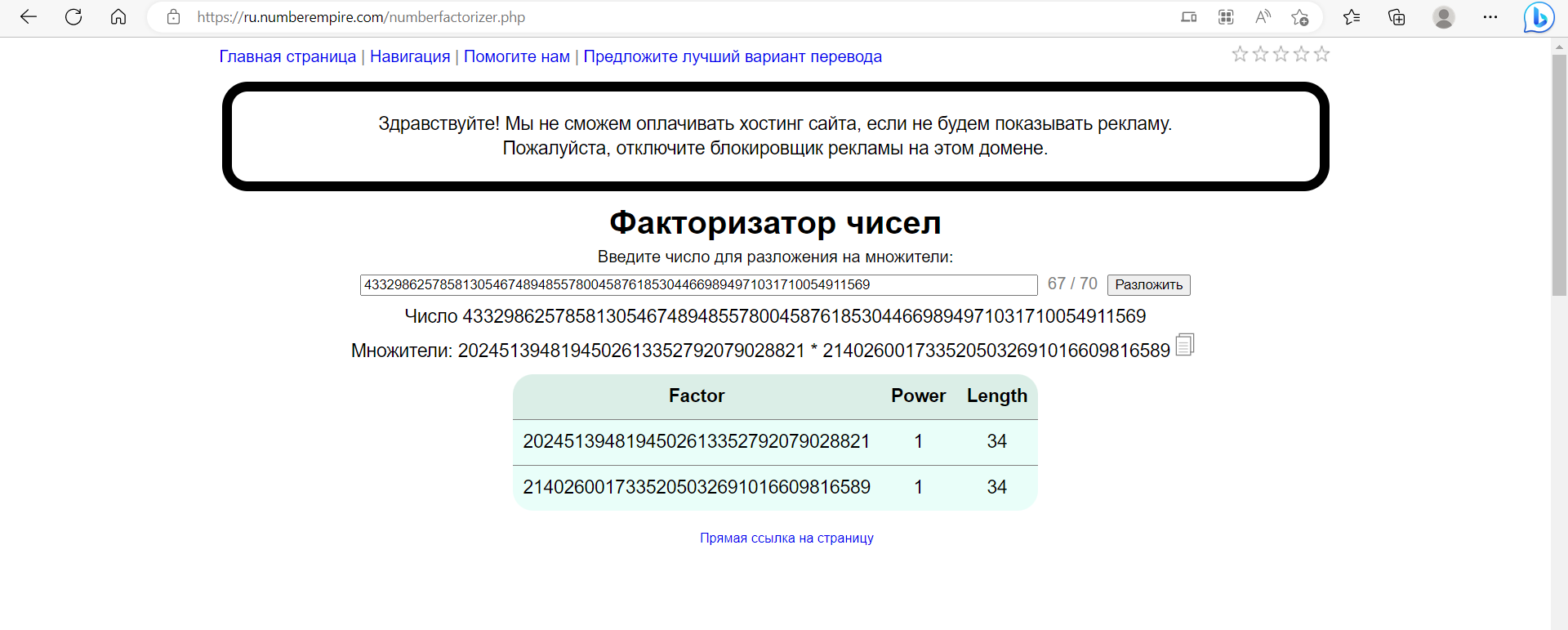


Как видно на скриншоте, мой вариант соответствует следующему числу:

B) 4332986257858130546748948557800458761853044669894971031710054911569

**2. Разложение числа на нетривиальные сомножители**

В этой части задания требуется число, соответствующее моему варианту, разложить на простые сомножители, не являющиеся исходным числом и единицей. Разложение будет производиться с помощью сайта 'https://ru.numberempire.com/numberfactorizer.php'.



Как видно на скриншоте, полученные числа:

2024513948194502613352792079028821 и 2140260017335205032691016609816589

**4. Вывод**

В процессе работы над данной лабораторной работой, я впервые встретился с разложением числа на простые сомножители, количество разрядов которого сильно превышает десять (67 разрядов). В результате было получено, что у данного числа имеется два нетривиальных сомножителя, количество разрядов которых также немало (34 разряда у каждого числа). Исходное число неплохо подойдёт для создания ключей шифрования, ведь его простые сомножители не являются сильно большими или сильно маленькими, а значит, простым перебором получить их будет весьма проблематично.