Московский Авиационный Институт
(Национальный Исследовательский Университет)

Факультет: «Информационных технологий и прикладной математики»
Кафедра: 806 «Вычислительная математика и программирование»
Дисциплина: «Криптография»

Лабораторная работа №2

Студент:	Чекменев В.А
Группа:	М8О-307Б-20
Преподаватель:	Борисов А. В.
Дата:	
Оценка:	

Москва 2023

Задание

Разложить число на нетривиальные сомножители. Ниже представлены 16 вариантов. Вариант выбрать следующим образом: свое ФИО подать на вход в хеш-функцию, являющуюся стандартом, выход хеш-функции представить в шестнадцатеричном виде и рассматривать младший разряд как номер варианта. В отчете привести подробности процесса вычисления номера варианта.

Выполнение

В начале выполнения работы выберем свой вариант следующим образом - по своему ФИО: Чекменев Вячеслав Алексеевич. Далее воспользуемся вспомогательным ресурсом, который определит младший разряд ФИО как номер варианта. На выходе я получил число 9, следовательно, у меня вариант 9.

https://www.convertstring.com/Hash/SHA512

Вариант 9:

26224751825211611185543814938532015647718685864593280258926589002 57

Далее раскладываем число на нетривиальные сомножители, воспользуемся дополнительным ресурсом для этой задачи:

https://www.cryptool.org/en/cto/msieve

После разложения мы получаем:

Входное число состоит из 221 бит

Найдены факторы:2

Факторизованное число:

26224751825211611185543814938532015647718685864593280258926589002 57

1). *157284844227269891201769474334549 3*

2). *166734131022299665239736598398274 9*

Вывод

Данная лабораторная работа по криптографии посвящена разложению числа на нетривиальные сомножители. Разложение числа на нетривиальные сомножители является сложной задачей и требует применения специальных алгоритмов. В результате выполнения лабораторной работы был получен опыт применения алгоритма факторизации числа на простые множители Эта задача является актуальной в современной криптографии, поскольку многие криптографические алгоритмы используют большие простые числа.