**Отчет по лабораторной работе №2 по курсу «Криптография»**

Выполнил Лисин Роман Сергеевич, М8О-306Б-20.

***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.

***Ход работы***

Для разложения числа на нетривиальные сомножители я воспользовался готовой онлайн реализацией метода квадратичного решета, потому что мой ноутбук не потянул такие вычисления.

Код на Python (в комментариях пояснения по ходу выполнения работы):

import hashlib  
  
sha = hashlib.sha256()  
sha.update(b"Lisin Roman Sergeevich")  
print(sha.hexdigest())  
# b1bf248f84f3b35537dea29b3174917a56e4adb6c4c687c7192886846ff25963 => 3 вариант  
  
n = 4149239365576004112053288191516373009003121933316645627672184154467  
# online service: https://www.alpertron.com.ar/ECM.HTM  
p = 1801980724165903959833591766451811  
q = 2302599195391833607443261812080897  
print(n == p \* q)  
# True