МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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 дисциплине «Криптография»

Выполнила студент группы М80-307Б-20:
Сафонникова А. Р.

Принял:
Борисов А. В.

Москва 2023

ОПИСАНИЕ

Хеш-функция – это функция, которая преобразует произвольный входной набор данных (например, строку, число, файл) в фиксированный размерный набор данных (обычно строку фиксированной длины) - хеш-значение.

Хеш-функции широко используются в информатике для быстрого и эффективного сравнения и проверки целостности данных. Они используются в хеш-таблицах, блокчейнах, криптографии и других областях, где важна быстрая проверка на соответствие.

Хеш-функция должна быть быстрой и эффективной, то есть она должна работать достаточно быстро, даже для больших объемов данных. Кроме того, хеш-функция должна иметь свойство равномерного распределения, что означает, что любые два разных входных значения должны иметь различные хеш-значения.

Хеш-функции могут быть использованы для хранения пар ключ-значение в хеш-таблицах. Ключ может быть произвольным набором данных, а хеш-функция будет использоваться для быстрого поиска соответствующего значения.

Хеш-функции также используются в криптографии для создания электронной подписи и цифровой подписи. В этом случае хеш-функция используется для генерации уникальной строки фиксированной длины для произвольно больших данных, а затем эта строка подписывается с помощью частного ключа, что позволяет убедиться в подлинности и целостности данных.

Хеш-функции также используются в блокчейнах, где они используются для проверки целостности блоков данных, что позволяет убедиться в том, что данные в блоке не были изменены.

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.

0) 2340571395943468779396457226549795691709967953275152127654153743783

1) 4082641366950946910743038307134981492747773137554505769911052316953

2) 283552415928171651728352951056879916758399987615495692874015865707 3

3) 414923936557600411205328819151637300900312193331664562767218415446 7

4) 309086911254871141538991434992575166692891121664241483573664946812 1

5) 344472733220193753482991356021373584263865069378661059224918094608 3

6) 452080536798612443541374626356752384132476144619627175414634520412 1

7) 389539373867071679527493873849952198395021832651681317692757939072 9

8) 319292372535904692898766202121775436558028352826141020467762142201 3

9) 262247518252116111855438149385320156477186858645932802589265890025 7

A) 330216294007277803545057376069785154304379139118551271814254241072 7

B) 433298625785813054674894855780045876185304466989497103171005491156 9

C) 391729859208429947459826298479418910626394384849150774108621298619 9

D) 488573951867471261413126340909385075222197284517362195224562609627 7

E) 328748827357297780960877983999630524087649300281236656755659637398 9

F) 214146932815131542247106735731841544290441183229121082130332505058 7

РЕШЕНИЕ

Для того, чтобы определить вариант задания, я использовала стандартную библиотеку *hashlib* языка программирования python. Таким образом был

```
import hashlib
```

получаем хеш в шестандцетиричном виде

```
def calculate_hash(FIO):
    hash_object = hashlib.sha256(FIO.encode())
    hex_dig = hash_object.hexdigest()
    return hex_dig
```

```
hash_value = calculate_hash("Сафонникова Анна Романовна")
print("Хэш-код полученного значения:", hash_value)
```

```
Хэш-код полученного значения: 43f165284f9dc615fc4c366230f78ec6f9ce0e960f15264df7da4b9a9491426c
```

берём младший разряд

```
def get_last_digit(hash_value):
    last_digit = int(hash_value[-1], 16)
    return last_digit
```

```
last_digit = get_last_digit(hash_value)
print("Вариант лабораторной работы:", last_digit)
```

```
Вариант лабораторной работы: 12
```

определён вариант под цифрой 12.

Далее раскладываем число на нетривиальные сомножители.

Для этого воспользуемся таким дополнительным ресурсом, как www.alpertron.com.ar, где удалось быстро получить ответ с помощью метода *SIQS* для задачи факторизации целых чисел.

После разложения мы получаем:

3 917298 592084 299474 598262 984794 189106 263943 848491 507741 086212 986199 =

1746 052391 086920 741342 287877 605699

2243 517211 786396 674815 244250 769501

ВЫВОД

В ходе выполнения лабораторной работы был использован метод разложения числа на нетривиальные сомножители. Для выбора варианта было использовано хеширование ФИО с помощью стандартной хеш-функции, а затем приведение результата в шестнадцатеричную систему счисления и выбор младшего разряда как номера варианта.

Лабораторной работа позволила познакомиться с основами хеширования.