Государственное учреждение образования

“БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ”

Кафедра: Интеллектуальных информационных технологий

Дисциплина: Средства и методы защиты информации в интеллектуальных системах

**Отчет по лабораторной работе №4**

**“Открытое распространение ключей”**

Вариант 21

Выполнил:

студент гр.221701

Телица И.Д.

Проверил:

Захаров В.В.

Минск 2024

#### **Цель**:

Получить навыки генерации общего ключа для протокола Диффи-Хеллмана.

#### **Задача:**

Для заданного простого P (4877) найти g – примитивный элемент конечного поля GF(P) и выполнить генерацию общего секрета.

## **Ход работы:**

1. Алиса и Боб договариваются о наборе больших простых чисел P и g, таких, что g является наименьшим первообразным корнем P.

2. Алиса генерирует случайное секретное число a и вычисляет .

3. Боб генерирует случайное секретное число b и вычисляет .

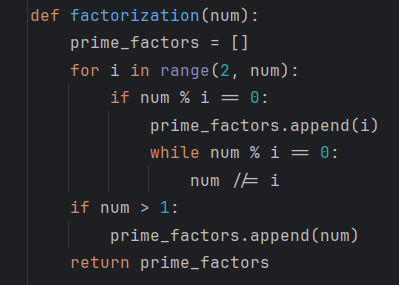
4. Алиса отправляет Бобу .

5. Боб отправляет Алисе .

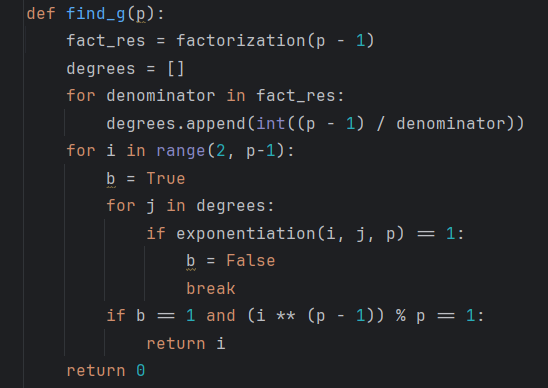
6. Алиса вычисляет общий секрет .

7. Боб вычисляет общий секрет .

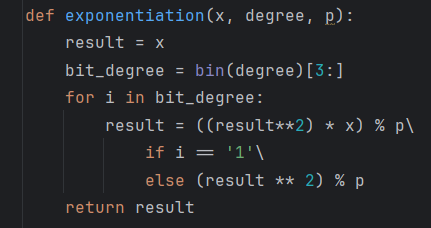
Функция **factorization(num)** ищет все простые делители числа, передаваемого в качестве аргумента num и возвращает список этих делителей.



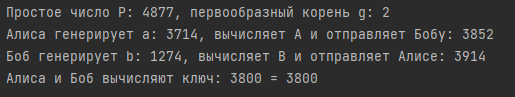
Функция **find\_g(p)** производит нахождение наименьшего первообразного корня простого числа p. Первообразным корнем будет то число g, которое принадлежит промежутку , при этом Но для всех степеней должно выполняться Для этого достаточно проверить те , где – элемент множества простых делителей числа .



Функция **exponentiation(x, degree, p)** производит возведение в степень методом последовательного возведения в квадрат и умножения, операция взятия по модулю производится на каждом шаге.



#### **Результат работы:**



#### **Вывод**:

В результате выполнения лабораторной работы была написана программа для генерации общего секрета по протоколу Диффи-Хеллмана. Этот протокол основан на идее, что произведение двух больших простых чисел очень сложно разложить на факторы даже при использовании современных вычислительных технологий.

Если злоумышленник будет использовать метод подбора, то быстро подберет нужный ключ, поэтому нужно подбирать достаточно большие числа p и g. Злоумышленник может использовать метод “человек посередине”: он может генерировать свои значения для Алисы и Боба и вести переписку с ними двумя. Для предотвращения необходимо использовать дополнительные протоколы аутентификации.