Криптографические средства

Лабораторная работа №2

Вариант 2.7

Выполнили студенты группы 22307

Никаноров Роман и Харичев Евгений

ПетрГУ 2022

Формулировка задания

Напишите программу генерации совместного ключа методом Диффи-Хеллмана. Рекомендуется использовать библиотеку для работы с длинными числами. В случае применения этой библиотеки разрешается использовать функции сложения, вычитания, умножения, целочисленного деления, вычисления остатка от деления. Функции возведения числа в степень, нахождения наибольшего общего делителя, обратного элемента в мультипликативной группе вычетов, генерации простого числа реализовать самостоятельно. Использовать подгруппы меньшего размера. Выполняемые функции программы:

1. генерация чисел ;
2. имитация обмена данными между пользователями;
3. получение общего ключа.

Описание метода решения

Существует два абонента и . Обоим абонентам известны 3 числа: – примитивный элемент порождающий группу (мультипликативная группа вычетов), – большое простое число, – большое простое число (делитель , используется для ускорения вычислений).

Если абоненты хотят создать общий секретный ключ , то они должны выполнить шаги:

1. Абонент выбирает случайное целое число и посылает абоненту значение .
2. Абонент выбирает случайное целое число и посылает абоненту значение .
3. Абонент вычисляет .
4. Абонент вычисляет .

Если все сделано правильно, то

Алгоритм генерации и :

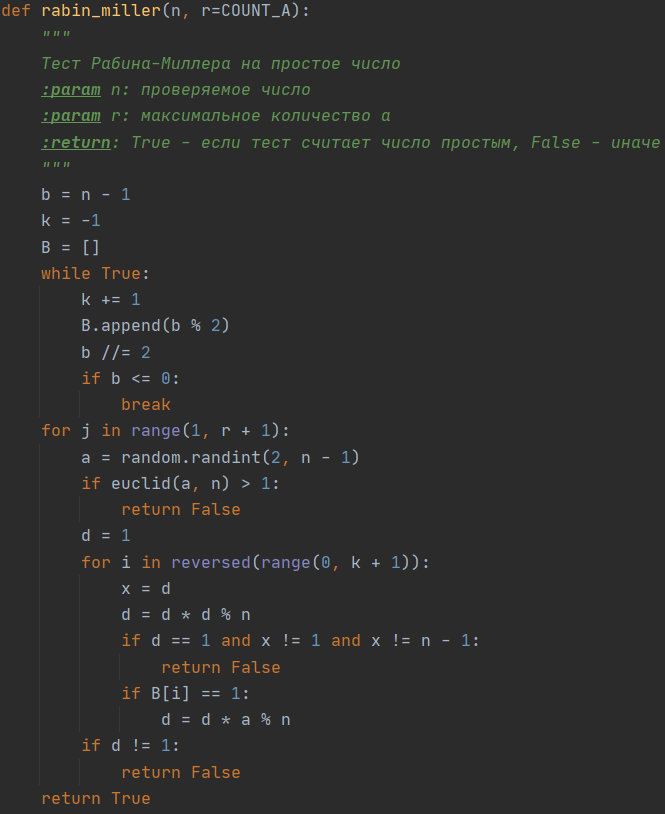
1. Генерируем простое число размером 256 бит (такой размер считается безопасным)
2. Генерируем число , где n – случайное целое число, пока не станет простым.
3. Генерируем число , где – случайное целое число из промежутка , до тех пор пока выполняется условие .

Алгоритм ускоренного возведения в степень по модулю:

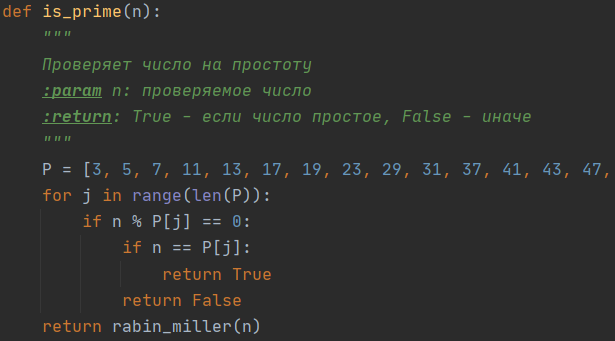
1. Вычисляем – остаток от деления степени на число.
2. Вызываем ранее реализованную функцию возведения в степень по модулю с параметрами и .

Примеры кода программы

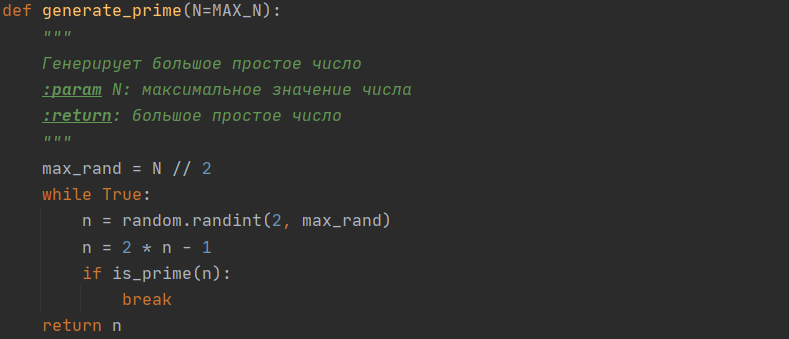
Тест Рабина-Миллера на простое число:



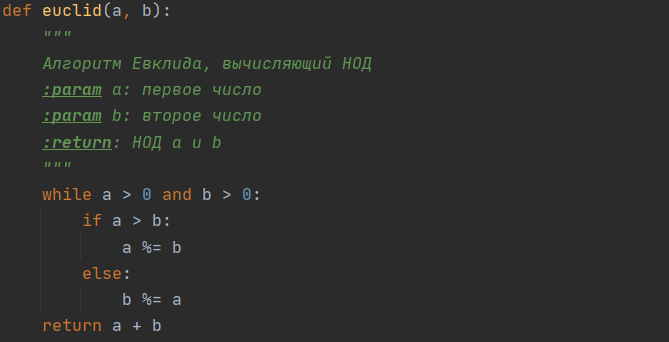
Проверка на простое число:



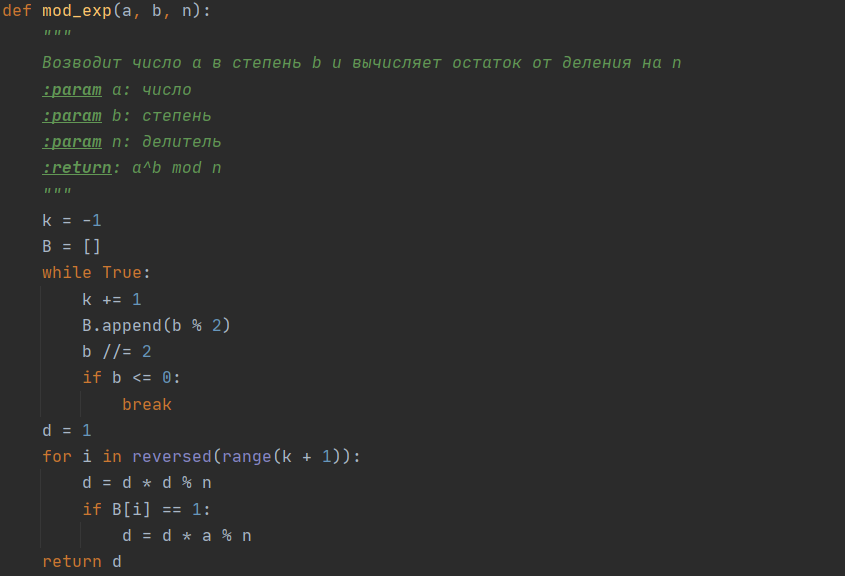
Генерация большого простого числа:



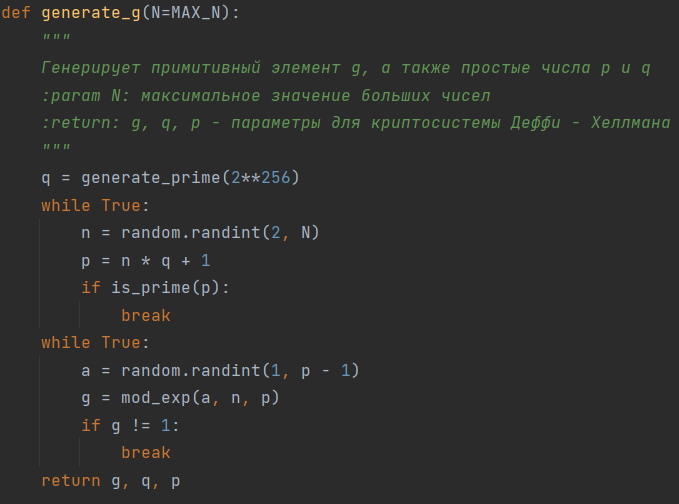
Алгоритм Евклида, вычисляющий НОД:



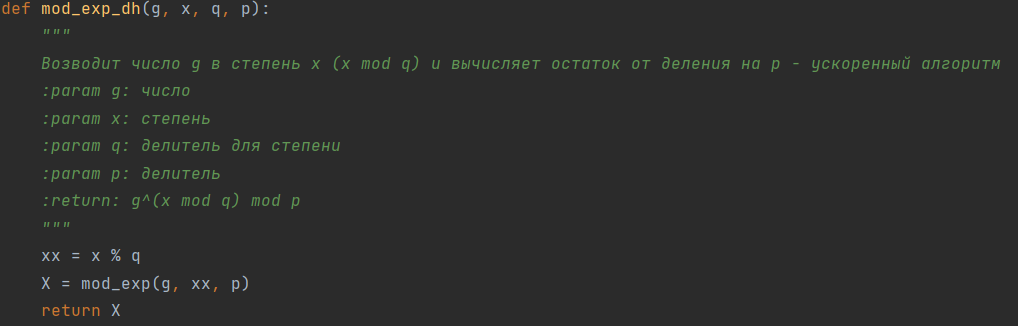
Метод возведения в степень по модулю:



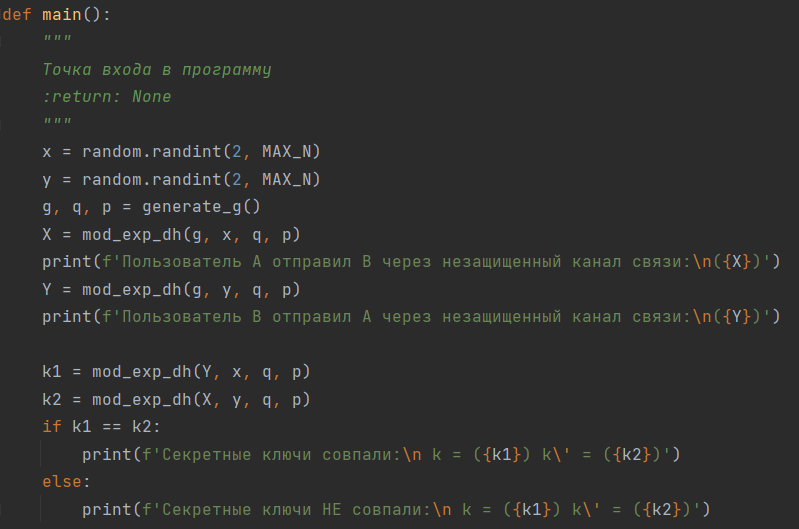
Метод для генерации , и :



Метод ускоренного возведения в степень по модулю для криптосистемы Диффи - Хеллмана:



Получение общего секретного ключа:



Тестовые данные

Примеры работы программы для сообщения M = 123456789, максимальной длине чисел в 25 символов и количестве проверок в тесте Рабина-Миллера равном 100:

