Лабораторная работа по криптографии №2

Криптосхема Диффи-Хеллмана

Автор: Гашков С.П., гр.22305

23.02.2024

1. 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 p, g, x, y;

2) имитация обмена данными между пользователями;

3) получение общего ключа.

1. Описание метода решения

***Генерация параметров:***  
1. p – большое простое случайное число

2. g – примитивный элемент, порождающий группу (g является первообразным корнем для p, т.е. )

3. Числа p и g открыты, передаются по открытым каналам связи и должны быть у каждого абонента

***Создание секретного ключа k:***

1. Пользователь A выбирает случайное целое число и посылает пользователю B значение

2. Пользователь B выбирает случайное целое число и посылает пользователю A значение

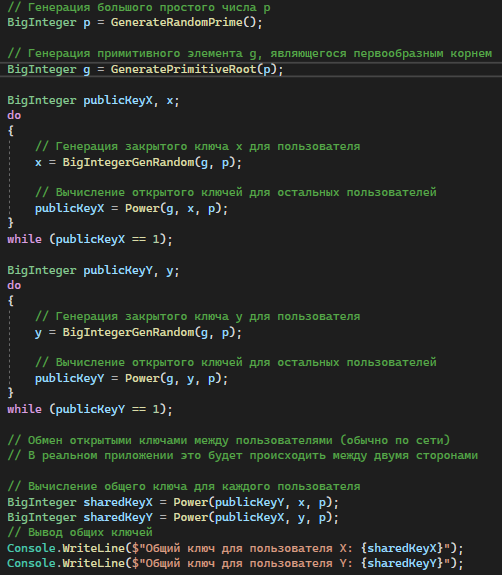
3. Пользователь A вычисляет значение

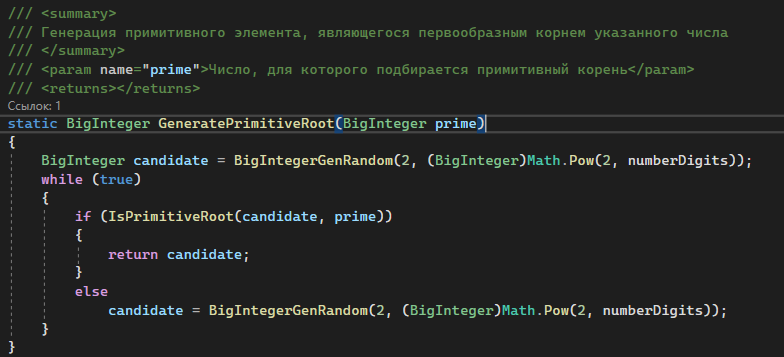
4. Пользователь A вычисляет значение

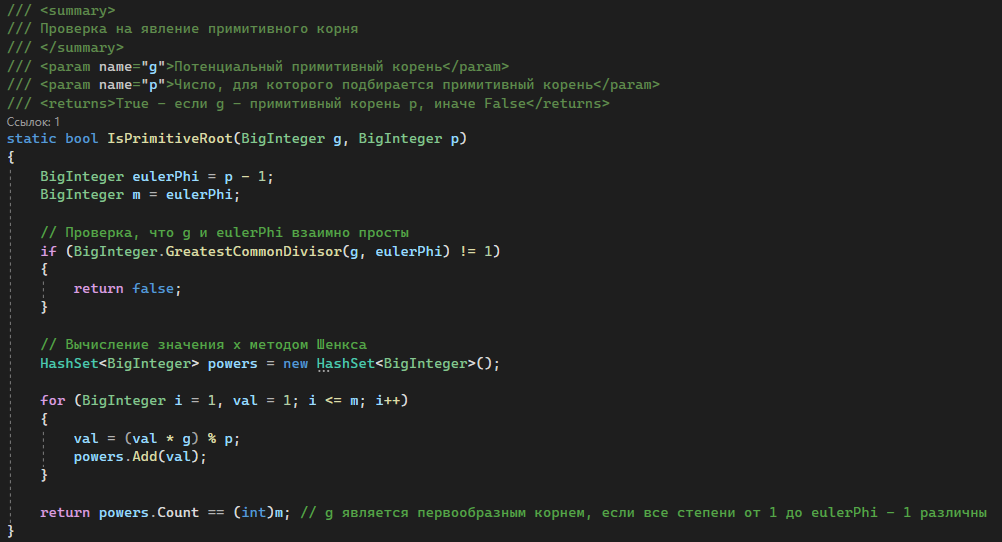
Если всё сделано правильно, то

1. Примеры кода

Примечание: ввиду высокой сложности операции поиска первообразных корней, тестирование при разработке проходило на числах, разрядностью не более 16 бит. Изменив настройки класса, можно увеличить/уменьшить количество бит на число, тем самым изменив время расчётов и надёжность шифрования.







1. Тестовые данные
   1. Получение одинакового совместного ключа у обоих имитируемых пользователей – позитивный тест
2. Ссылка на репозиторий

<https://github.com/Nemo121007/cryptography.git>