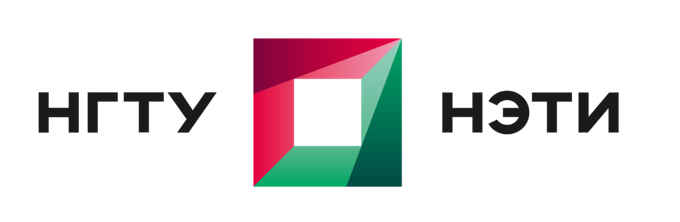
# Министерство науки и Высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное   
учреждение высшего образования

«Новосибирский государственный технический университет»



Кафедра теоретической и прикладной информатики

Лабораторная работа № 5  
по дисциплине «Программные средства защиты информации»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Факультет: | ПМИ |  |  | |
| Группа: | ПМИМ-21 |  |  | |
| Бригада: | 3 | | |  | |
| Студенты: | Бортников. Н, Ефименко А., Кутузова И. | | |  | |
|  |  |  |  | |
| Преподаватель: | Авдеенко Т.В. |  |  | |

Новосибирск

2023

1. **Формулировка задания**

I. Реализовать приложение, позволяющее выполнять следующие действия:

1. Генерировать большие простые числа:

1) программа по заданным (количество проверок в тесте Рабина-Миллера) и (количество бит) должна генерировать простое n-битное число, отображая при этом, сколько итераций алгоритма генерации простого числа потребовалось выполнить для его генерации и сколько времени было затрачено на это;

2) программа по заданным границам диапазона должна выводить все простые числа из этого диапазона, отображая время, затраченное на генерацию всех чисел.

2. Определять для заданного числа первые 100 первообразных корней, отображая при этом суммарное время, затраченное программой на их поиск.

3. Моделировать обмен ключами между абонентами по схеме Диффи-Хеллмана. Программа должна получать большие простые числа , и случайным образом с помощью алгоритма генерации простого числа, а также предоставлять пользователю возможность задавать их.

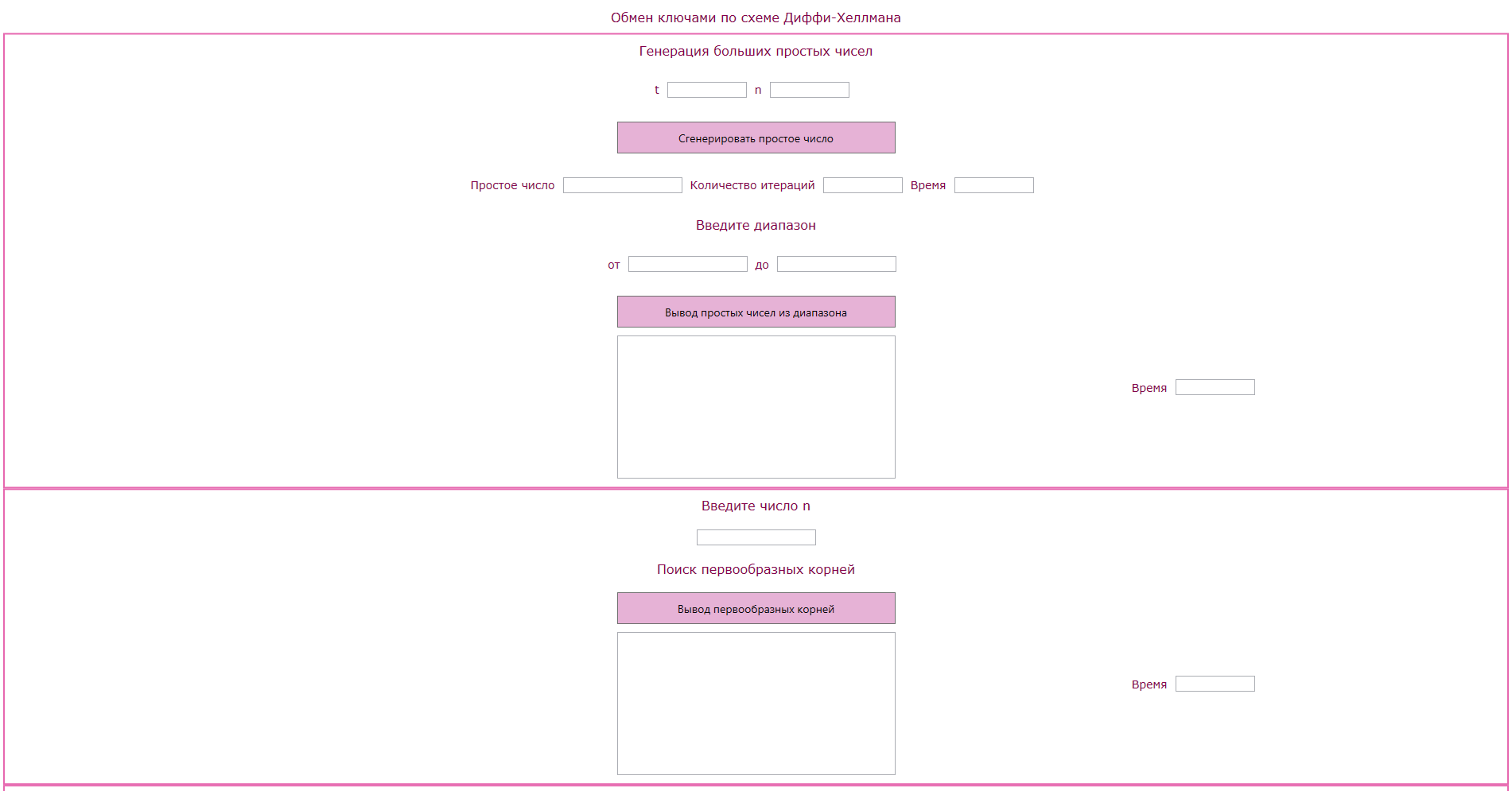
II. С помощью реализованного приложения выполнить следующие задания:

1. Протестировать правильность работы разработанного приложения.

2. Сделать выводы о проделанной работе.

1. **Описание разработанного программного средства**

Решение задачи реализовано в виде программы, написанной на языке C#. Интерфейс, через который осуществляется работа с ней, имеет следующий вид:



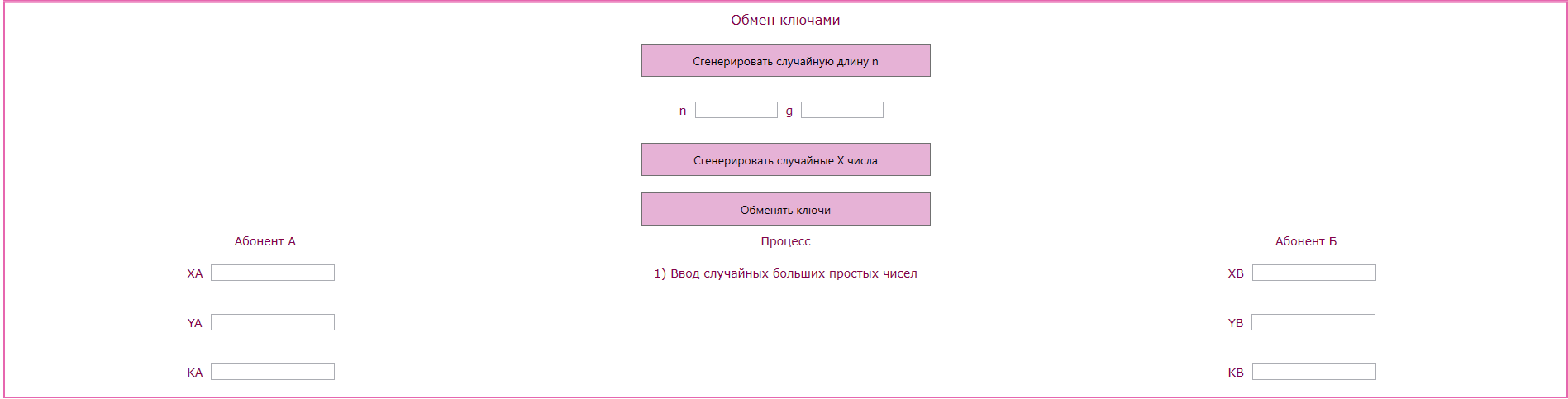
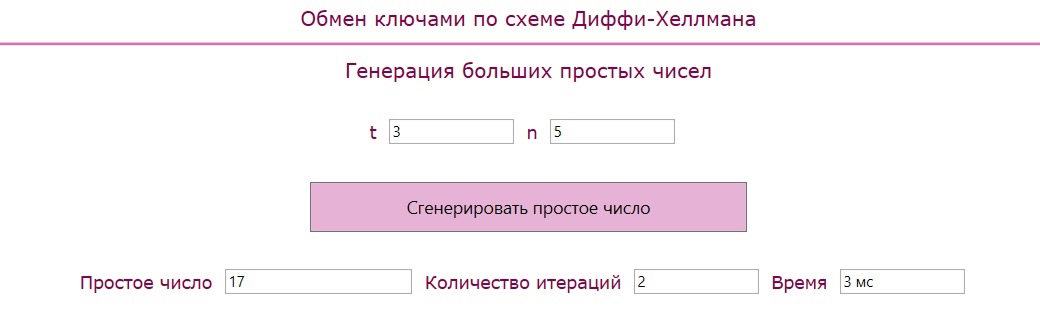
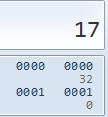


Рис. 1 – Интерфейс реализованного приложения

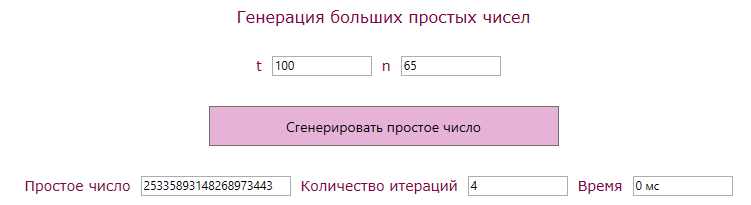
1. **Тестирование**

Тест 1. Генерация случайного простого числа

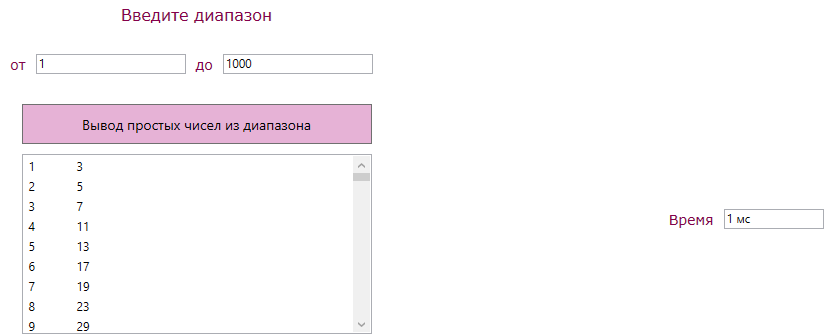




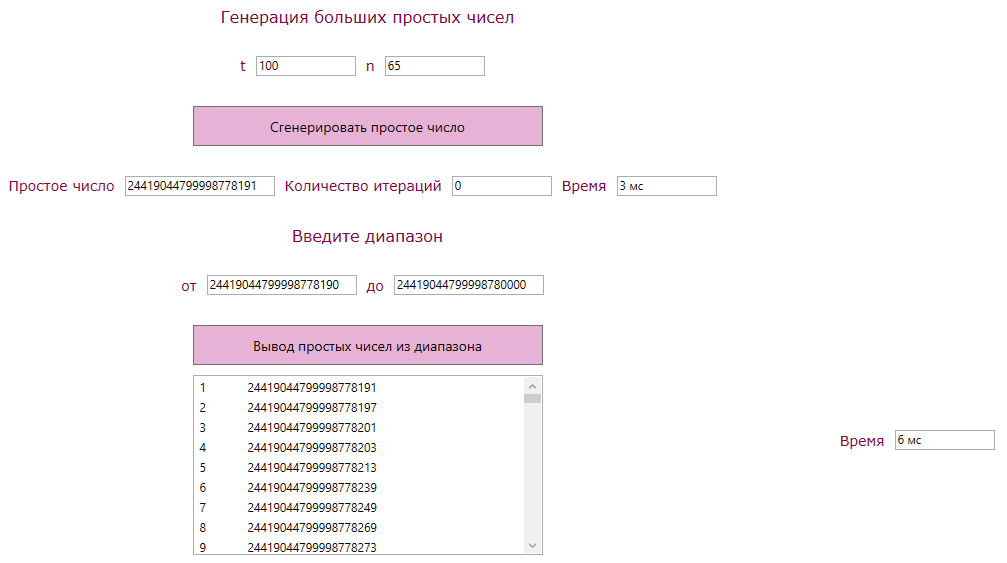
Тест 2. Генерация случайного большого простого числа



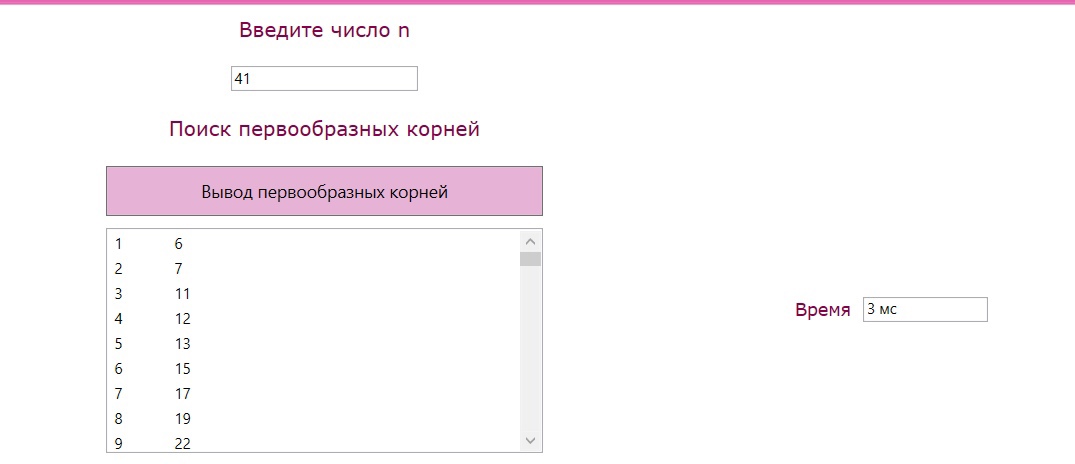
Тест 3. Генерация простых чисел в диапазоне от 1 до 1000

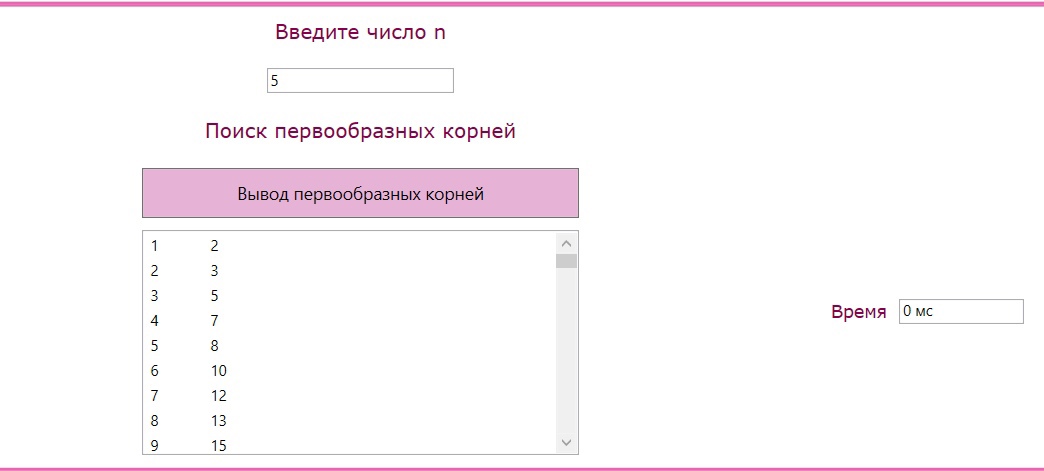


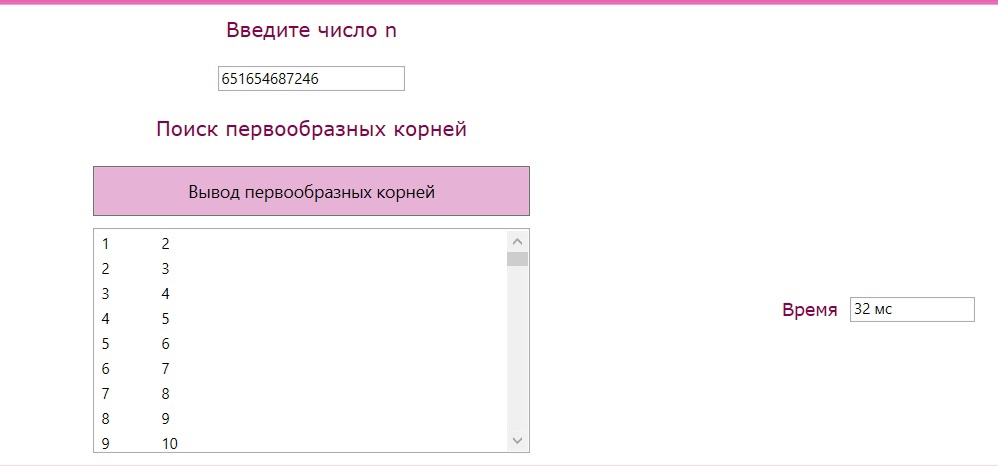
Тест 4. Генерация простых больших чисел в диапазоне



Тест 5. Генерация первообразных корней

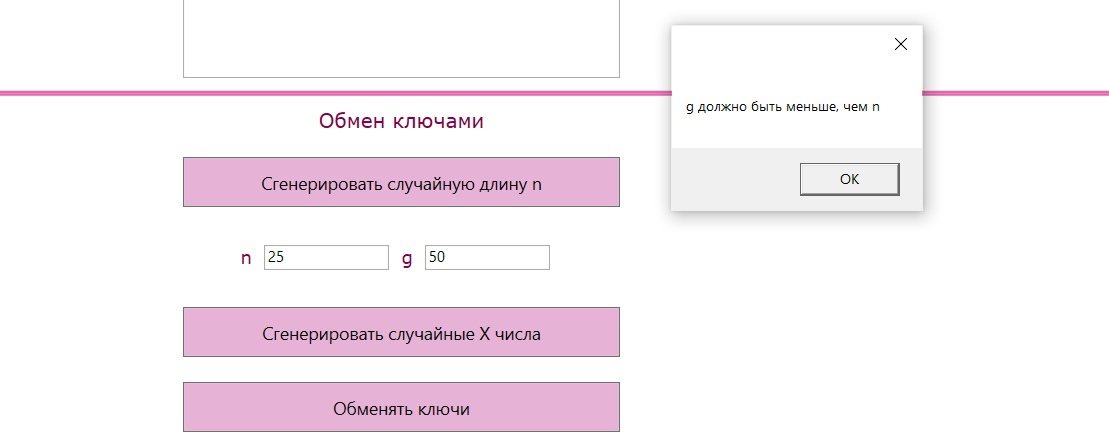


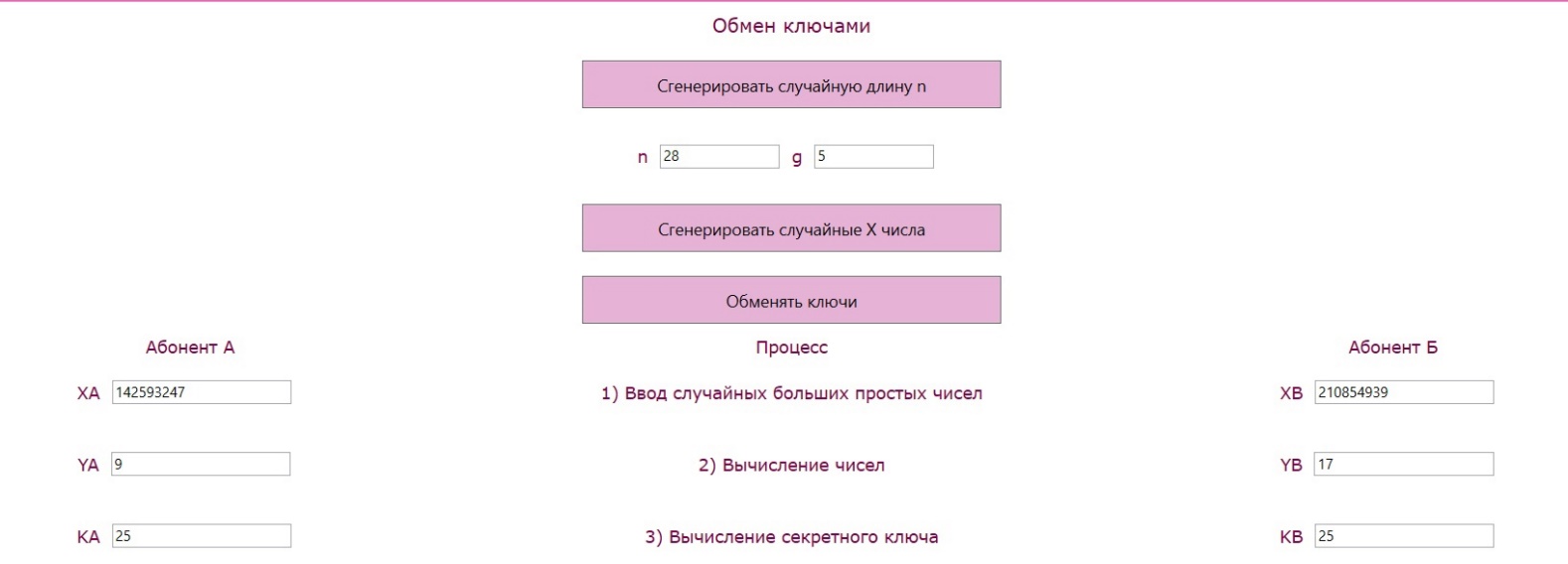




Тест 6. Обмен ключами по схеме Диффи-Хеллмана







1. **Вывод**

При выполнении лабораторной работы были изучены методы генерации больших простых чисел и методы их проверки на простоту. Также мы изучили теорему Эйлера и схему обмена ключами Диффи-Хеллмана.

В лабораторной работе мы реализовали приложение, позволяющее генерировать большие простые числа и первообразные корни по модулю n, а также осуществлять обмен ключами.