Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационный технологий и управления

Кафедра интеллектуальных информационных технологий

Дисциплина: «Средства и методы защиты информации в  
интеллектуальных системах»

Лабораторная работа №4 по теме:  
«Открытое распространение ключей»

Студент гр. 121702

Колтович Д. С.

Проверил:

Сальников Д.А.

Минск 2023

**Тема**

Открытое распространение ключей

**Задание**

Разработать программу, реализующую следующие функции:

1. Для заданного простого P (в соответствии с вариантом) найти g – примитивный элемент конечного поля GF(P).
2. Выполнить генерацию общего секрета

**Выполнение задания**Вариант 10 – 7759

**Алгоритм  
Для получения общего секрета Алиса и Боб выполняют следующие действия**

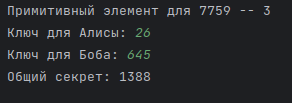
1) Алиса генерирует целое число a и держит его в секрете, затем вычисляет и пересылает его Бобу.

2) Боб генерирует целое число b и держит его в секрете, затем вычисляет и пересылает его Алисе.

3) Алиса вычисляет значение .

4) Боб вычисляет значение .

**По итогу они получают одинаковые значение = = . Данное значение и будет общим ключом для них, что позволит использовать его для зашифрования/расшифрования сообщения.**

**Результат работы программы**

Криптоаналитик может перехватить открытые ключи A, B, а также открытое простое число P, что позволяет вычислить первичное поле над ним G. Задача крипто аналитика состоит в решении уравнений . Из-за больших значений закрытых ключей и P нахождения решения этого уравнения не представляется возможным за обозримый срок.

**Вывод**

В ходе лабораторной работы были реализованы программные средства симуляции системы с открытым распространением ключей с генерацией общего секрета.