Министерство образования

Республики Беларусь

Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

Кафедра: интеллектуальных информационных технологий

Отчёт

По дисциплине

«Средства и методы защиты информации в интеллектуальных системах»

Тема: «Открытое распространение ключей»

Написал: Проверил

Германенко В.В., гр. 321701 Сальников Д. А.

Минск 2025

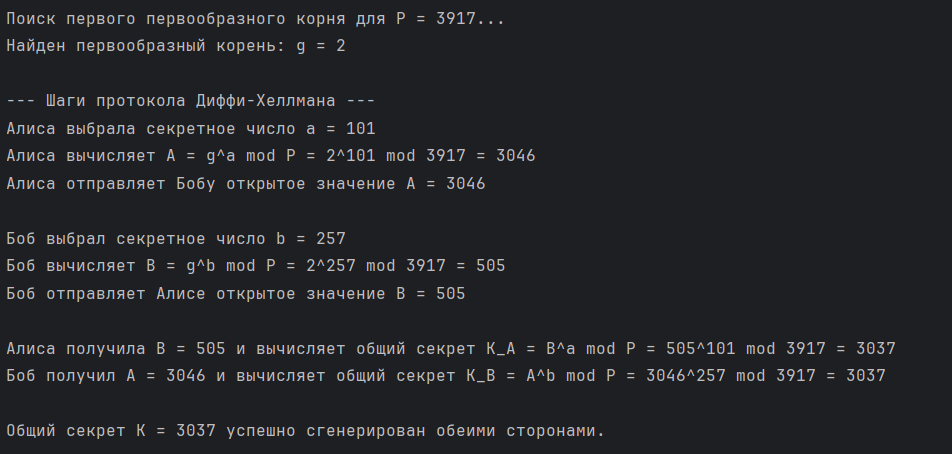
Цель: Практическое исследовать алгоритмы открытого распределения ключей.

Задача:

Для заданного простого P (в соответствии с вариантом) найти g – примитивный элемент конечного поля GF(P) и выполнить генерацию общего секрета. Для нахождения g воспользуйтесь методом перебора по возрастанию, возведения в степень по модулю P и проверки того факта, что все степени принимают значения от 0 до P - 1.

Вариант: 4) 3917

Работа программы:



**Работа протокола Диффи-Хеллмана**

Протокол Диффи-Хеллмана позволяет двум сторонам (Алисе и Бобу) получить общий секретный ключ, обмениваясь данными по открытому каналу связи, где возможно присутствие пассивного eavesdropper'а (подслушивающего).

**Исходные данные:**

* Простое число **P = 3917** (общее, известно всем, включая потенциального противника).
* Первообразный корень по модулю P: **g = [Здесь ваше найденное значение g, например, 2, 3, 5...]**.
  + \*Пояснение: Первообразный корень был найден методом перебора. Для каждого кандидата g проверялось, что его степени g^1 mod P, g^2 mod P, ..., g^(P-1) mod P порождают все числа от 1 до P-1, то есть являются циклической группой.\*

**Шаги протокола:**

1. **Генерация секретных ключей:**
   * **Алиса** генерирует свое **секретное число a** (большое случайное число, 1 < a < P-1).
   * **Боб** генерирует свое **секретное число b** (большое случайное число, 1 < b < P-1).
2. **Вычисление и обмен открытыми ключами:**
   * **Алиса** вычисляет свой **открытый ключ A** по формуле:  
     A = g^a mod P  
     и отправляет его Бобу.
   * **Боб** вычисляет свой **открытый ключ B** по формуле:  
     B = g^b mod P  
     и отправляет его Алисе.
3. **Вычисление общего секретного ключа:**
   * **Алиса**, получив B, вычисляет **общий секрет S**:  
     S = B^a mod P = (g^b)^a mod P = g^(a\*b) mod P
   * **Боб**, получив A, вычисляет **общий секрет S**:  
     S = A^b mod P = (g^a)^b mod P = g^(a\*b) mod P

**Результат:** И Алиса, и Боб независимо друг от друга получили одинаковое число **S**, которое и является их общим секретным ключом. Злоумышленник, перехвативший открытые ключи A и B, а также известные ему P и g, не сможет вычислить S за разумное время, так как задача вычисления a из A = g^a mod P (задача дискретного логарифмирования) является вычислительно сложной для больших P.

Вывод: В ходе работы был успешно реализован и протестирован протокол Диффи-Хеллмана. Практически подтвержден его основной принцип: возможность генерации идентичного секретного ключа двумя сторонами без его передачи по каналу связи. Установлено, что для обеспечения реальной безопасности необходимо использовать большие длины ключей и механизмы аутентификации для парирования угрозы "человека посередине".