Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет Информационных технологий и управления

Кафедра Интеллектуальных информационных технологий

**ОТЧЁТ**

по дисциплине «Средства и методы защиты информации в интеллектуальных системах»

Лабораторная работа №4

Тема: Открытое распространение ключей

Вариант: 21

Выполнил: Самута Д. В.

гр. 221703

Проверил: Крищенович В. А.

Минск 2024

**Задание 1:**

Для заданного простого P (в соответствии с вариантом) найти g –

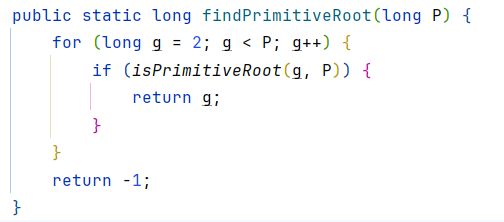
примитивный элемент конечного поля GF(P) и выполнить генерацию общего

секрета. Для нахождения g воспользуйтесь методом перебора по возрастанию,

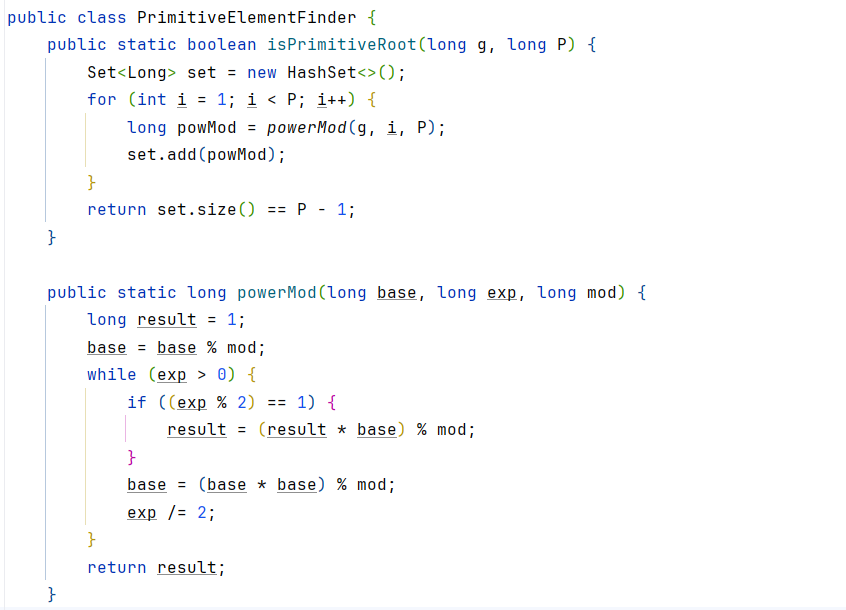
возведения в степень по модулю P и проверки того факта, что все степени

принимают значения от 0 до P - 1.

P = 4877



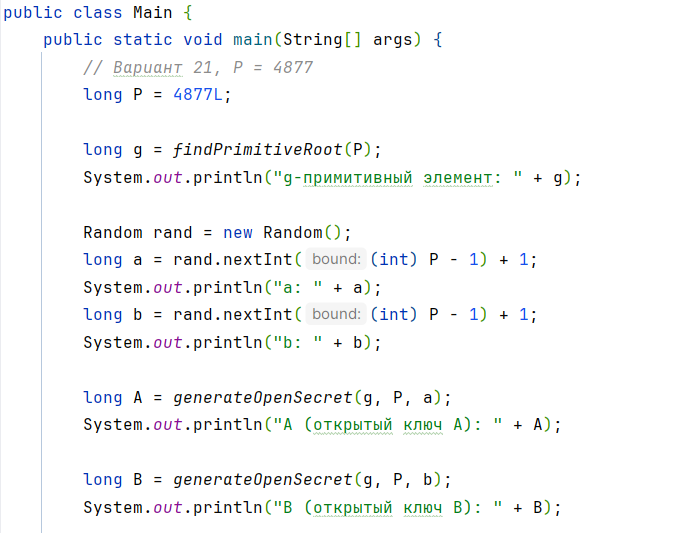
В этом методе с помощью перебора по возрастанию пытаемся найти g-примитивный элемент, в нем вызывается метод, который как раз и проверяет это. Он возводит это число во все степени до P и проверяет что при возведении в степень по модулю P оно дает все числа от 1 до P – 1.



В методе powerMod как раз происходит возведение в степень по модулю с использованием алгоритма быстрого возведения в степень методом повторяющихся возведений в квадрат и умножения.

Для P = 4877 – g-примитивный элемент равен 2.

Задание 2: Вычисление открытых ключей.



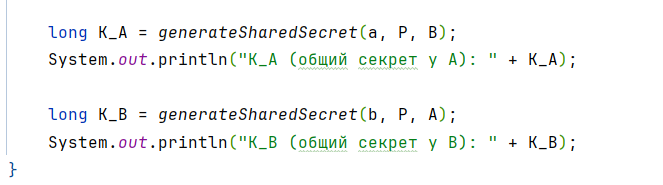
Для генерации открытых ключей две стороны числа должны выбрать случайное число.

После по формуле , где a – случайное число, вычисляется открытый ключ.

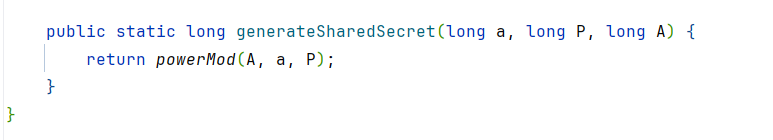


Он также вычисляется с использованием алгоритма быстрого возведения в степень методом повторяющихся возведений в квадрат и умножения.

**Задание 3:** Вычисление общего секрета.



Далее, стороны меняются открытыми ключами и вычисляют общий секрет.



**Задание 4:** Описание шагов Алисы и Боба.

1. Выбор параметров. Алиса и Боб договорились о простом числе P=4877 и примитивном элементе g = 2.
2. Генерация секретных ключей.Алиса выбирает случайное число a, а Боб — b.
3. Генерация открытых ключей.Алиса вычисляет и отправляет Бобу. Боб вычисляет и отправляет Алисе.
4. Вычисление общего секрета.Алиса вычисляет общий секрет . Боб вычисляет общий секрет . Оба получают одинаковый общий секрет:

**Выводы:**

а) Модель атакующего и оценка длины ключа.

Атакующий может наблюдать значения P, g, A, B, но не знает секретных ключей a и b. Для того чтобы найти общий секрет, атакующий должен решить задачу дискретного логарифмирования, которая является вычислительно сложной для больших значений P.

Оценка длины ключа: длина ключа зависит от выбора простого числа P. Чем больше P, тем сложнее атаки методом полного перебора. Для защиты в современных системах рекомендуют использовать P длиной не менее 2048 бит.

б) Возможные угрозы протоколу и защита.

1. **Атака "человек посередине".** Атакующий может перехватить значения A и B и подменить их своими. Для защиты от такой атаки используют цифровые подписи и сертификаты для аутентификации сторон.
2. Атаки на малые значения P. При малых значениях P возможны эффективные атаки перебором. Для защиты лучше выбирать большие значения P.
3. Угрозы на основе предсказуемых случайных чисел. Если случайные числа для выбора секретных ключей a и b плохо сгенерированы, это может ослабить протокол. Для защиты нужно использовать криптографически стойкие генераторы случайных чисел.