пМинистерство 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

ОТКРЫТОЕ РАСПРОСТРАНЕНИЕ КЛЮЧЕЙ

Вариант 18

Выполнил: Робилко Т. М.

гр. 221701

Проверил: В. В. Захаров

Минск 2024

**Задание:**

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,

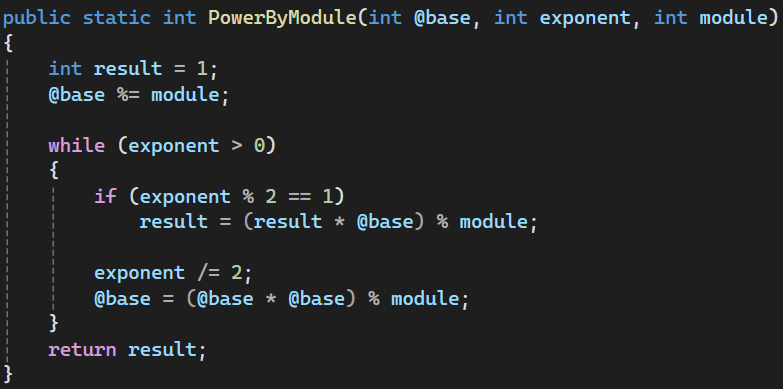
возведения в степень по модулю P и проверки того факта, что все степени

принимают значения от 0 до P - 1.

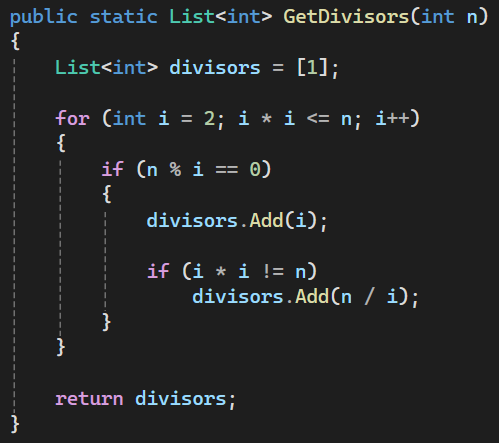
Вариант 18: простое число 8581

**Листинги программ:**

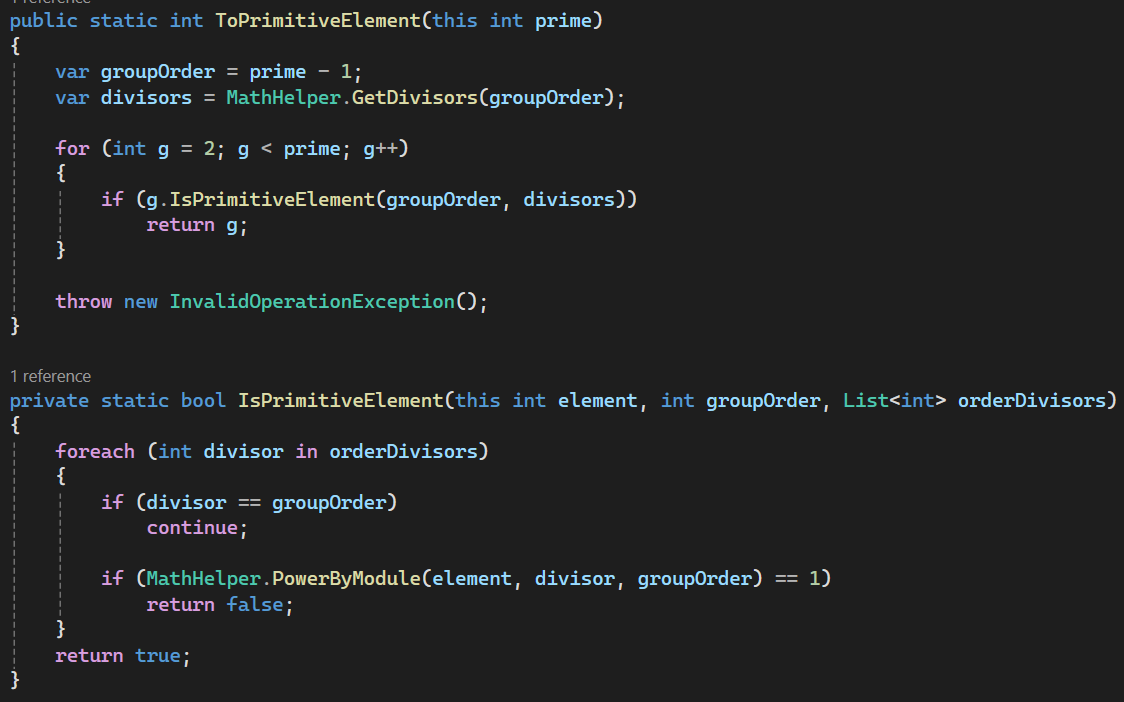
1. Функция возведения в степень по модулю



1. Функция получения списка делителей числа



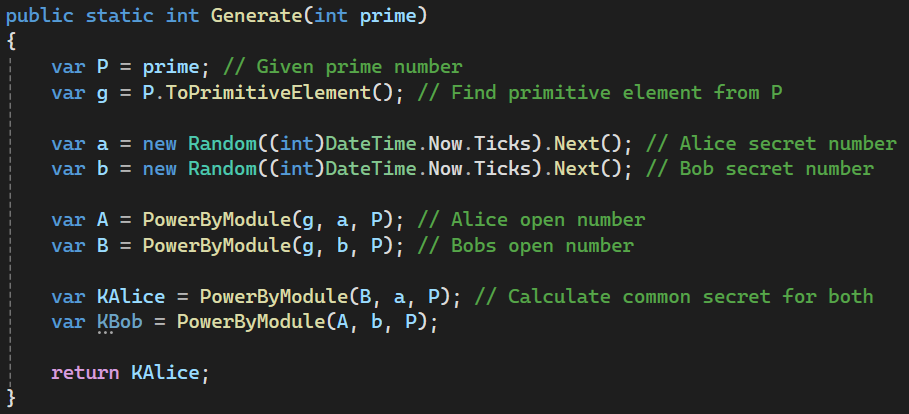
1. Для проверки g (первообразный корень по модулю P)



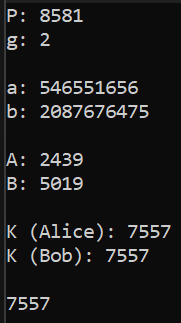
1. Для вычисления Ba mod P = gab mod P и Ab mod P = gab mod P использована функция возведения в степень по модулю.

**Описание шагов, выполняемых участниками протокола – Алисой и**

**Бобом для вычисления общего секрета:**

****

**Результат работы алгоритма для данного по варианту числа:**

****

**Выводы, модель атакующего, угрозы протоколу, предложения по защите**

Модель атакующего:

1. Активный атакующий (человек по середине): Злоумышленник может вмешаться в процесс обмена ключами, подменяя открытые ключи сторон.
2. Пассивный атакующий: Перехватывает обмен сообщениями, не вмешиваясь, пытается вычислить общий ключ, основываясь на перехваченных данных.

Оценки длины ключа:

Использование ключей, приведённых в лабораторной работе, **не является** достаточным для обеспечения безопасности. Для представления чисел был использован тип данных int, занимающий 4 байта в памяти (32 бит). С учётом мощности современных компьютеров перебор такого количества значений является нетрудной вычислительной задачей.

Для скорости подбора 10^18 попыток в секунду, что актуально для суперкомпьютеров, время подбора использованного ключа не превысит 4,3 \* 10E-9 секунд.

Использование ключей длиной 2048 бит и более дает 22048 вариантов для перебора возможного значения дискретного логарифма, что делает подбор крайне длительным (превышает время существования вселенной).

Предложения по защите:

1. Аутентификация: Используйте цифровые подписи или другие методы аутентификации отправителя сообщений.
2. Использование безопасных параметров: Применяйте стойкие к атаке параметры (например, большие простые числа)
3. Обновление ключей: Регулярно обновляйте ключи и используйте разные ключи для каждой сессии.