Лабораторная работа №7

Математические основы защиты информации и информационной безопасности

Минов Кирилл Вячеславович| НПМмд-02-23

Содержание

# 1 Цель работы

Реализовать на языке программирования p-метод Полларда для дискретного логарифмирования.

# 2 Теоретическое введение

**Задача дискретного логарифмирования** применяется во многих алгоритмах криптографии с открытым ключом. Предложенная в 1976 году У. Дифии и М. Хеллманом для установления сеансового ключа, эта задача послежила основой для создания протоколов шифрования и цифровой подписи, доказательств с нулевым разглашением и других криптографических протоколов.

# 3 Выполнение лабораторной работы

p-метод Полларда для дискретного логарифмирования реализуем по следующей схеме:

Код программы (рис. 1 - 3).

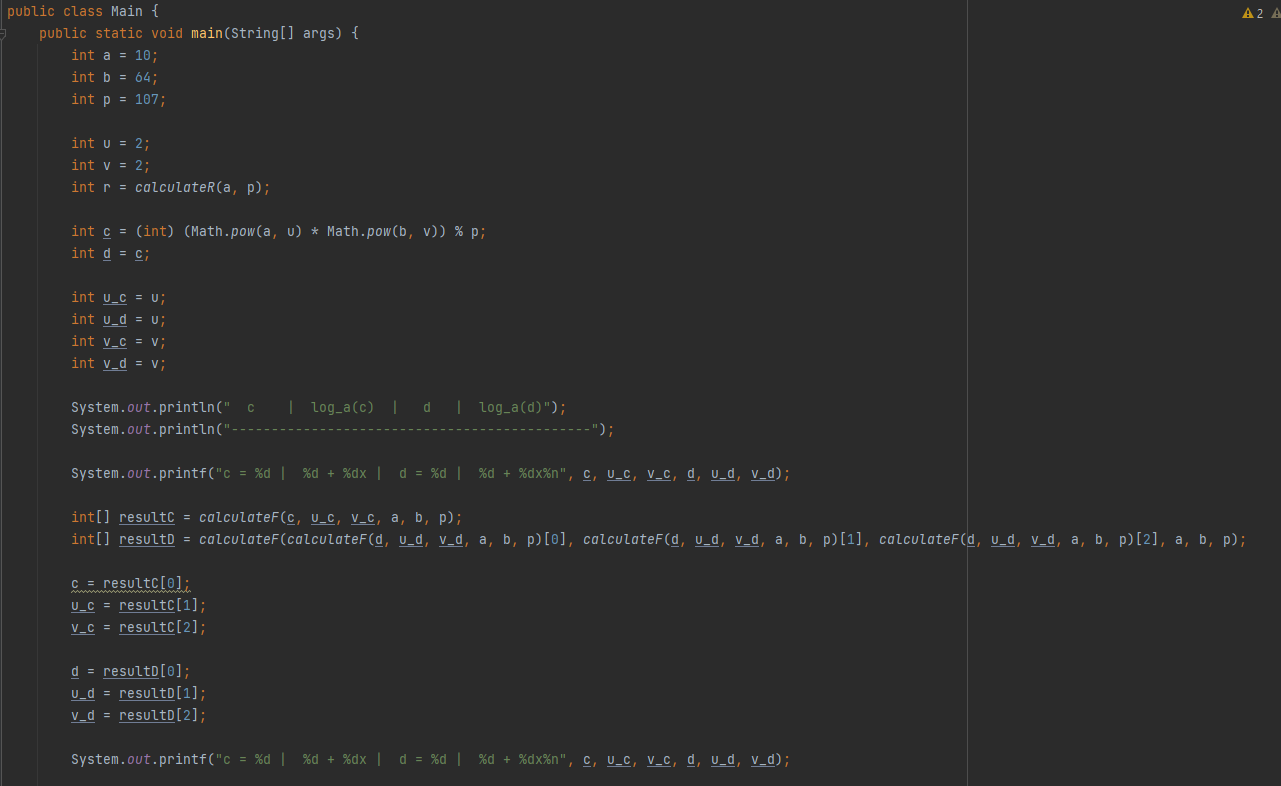


Рис. 1: p-метод Полларда для дискретного логарифмирования

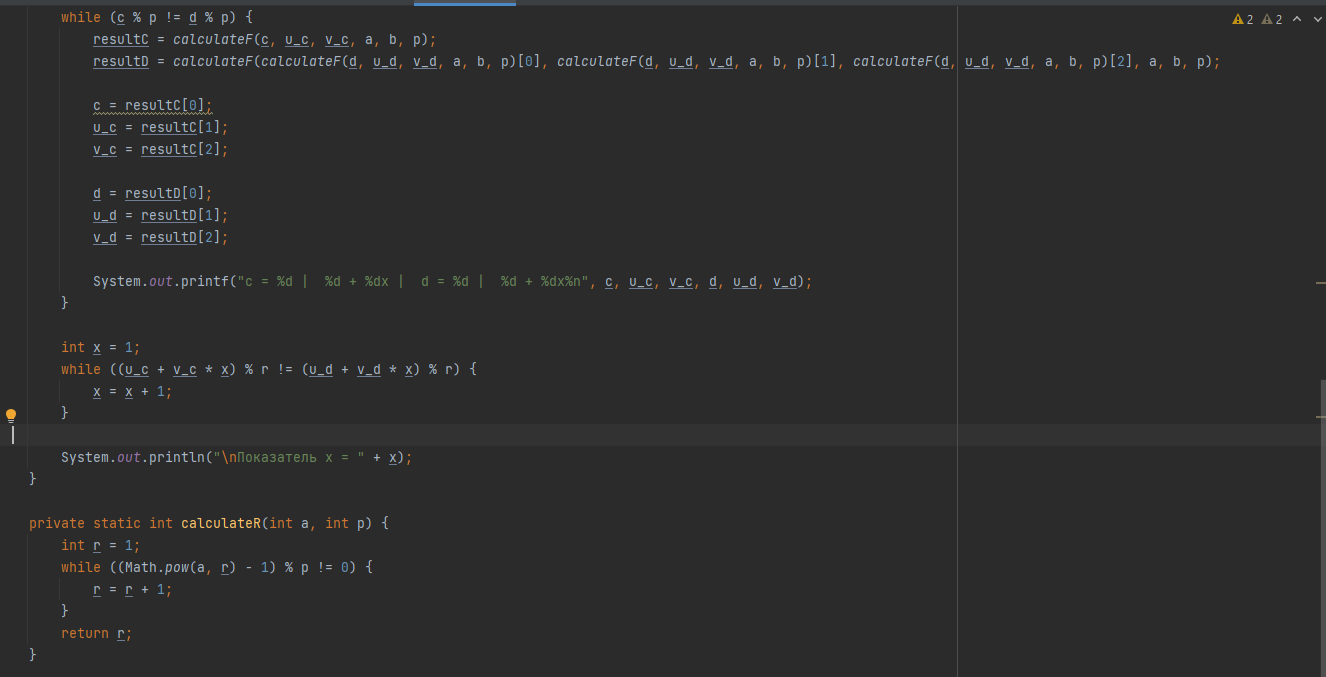


Рис. 2: p-метод Полларда для дискретного логарифмирования

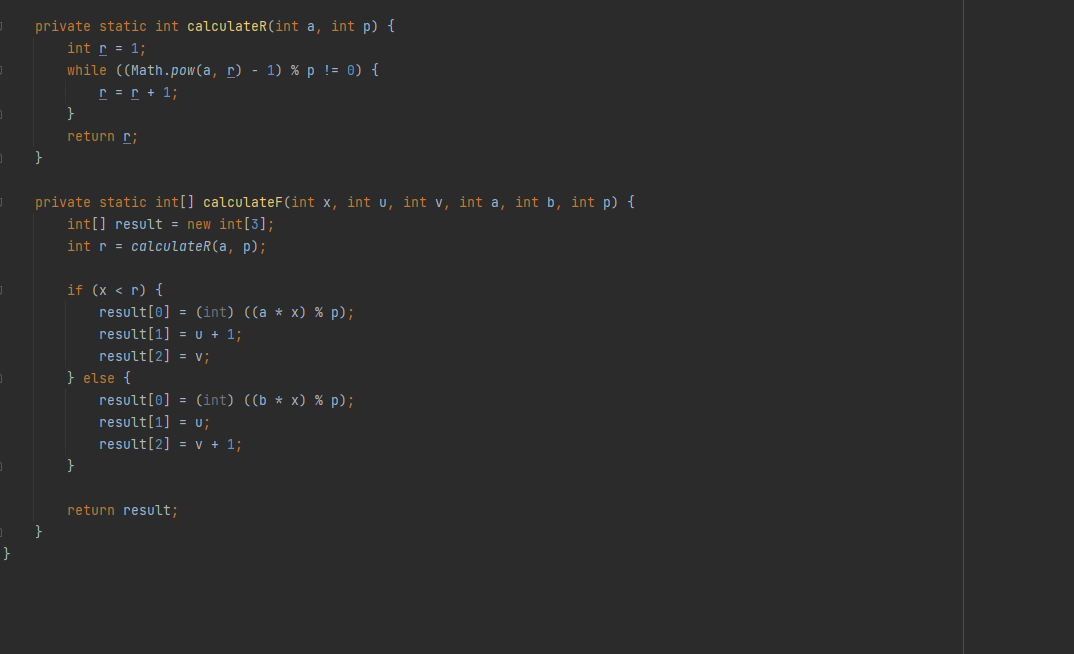


Рис. 3: p-метод Полларда для дискретного логарифмирования

# 4 Выводы

В ходе выполнения данной лабораторной работы был реализован p-метод Полларда для дискретного логарифмирования.

# Список литературы

1. p-метод Полларда для дискретного логарифмирования [Электронный ресурс]. URL: <https://en.wikipedia.org/wiki/Pollard%27s_rho_algorithm_for_logarithms>.