Лабораторная работа №7

Математические основы защиты информации и информационной безопасности

Леонтьева Ксения Андреевна | 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.

Обозначим , - простое целое число и назовем конечным полем из элементов. Задача дискретного логарифмирования в конечном поле формулируется так: для данных целых чисел и , , найти логарифм - такое целое число x, что (если такое число существует). По аналогии с вещественными числами используется обозначение .

Безопасность соответствующих криптосистем основана на том, что зная числа вычислить легко, а решить задачу дискретного логарифмирования трудно. Рассмотрим p-метод Полларда, который можно применить и для задач дискретного логарифмирования. При этом случайное отображение должно обладать не только сжимающими свойствами, но и вычислимостью логарифма (логарифм числа можно выразить через неизвестный логарифм и . Для дискретного логарифмирования в качестве случайного отображения чаще всего используются ветвящиеся отображения, например:

При : , при : .

Более подробно см. в [1].

# 3 Выполнение лабораторной работы

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

*Вход.* Простое число , число порядка по модулю , целое число , отображение , обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.

*Выход.* Показатель , для которого , если такой показатель существует.

1. Выбрать произвольные целые числа , и положить , .
2. Выполнять , , вычисляя при этом логарифмы для и как линейные функции от по модулю вида , до получения равенства .
3. Приравняв логарифмы для и , вычислить логарифм решением сравнения по модулю . Результат: или “Решений нет”.

Код программы (рис. 1 - 3).

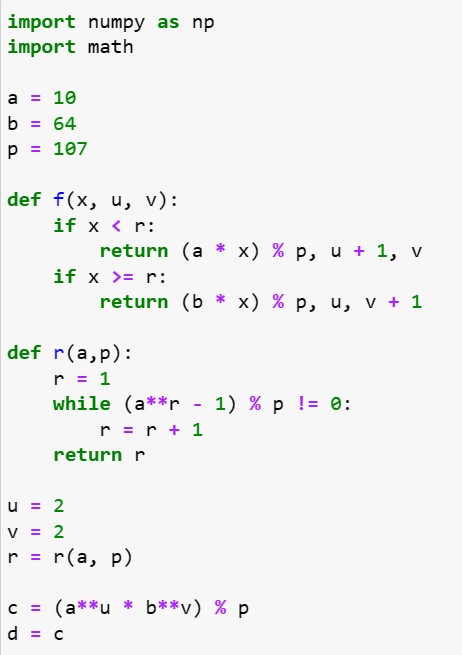


Рис. 1: p-метод Полларда для дискретного логарифмирования

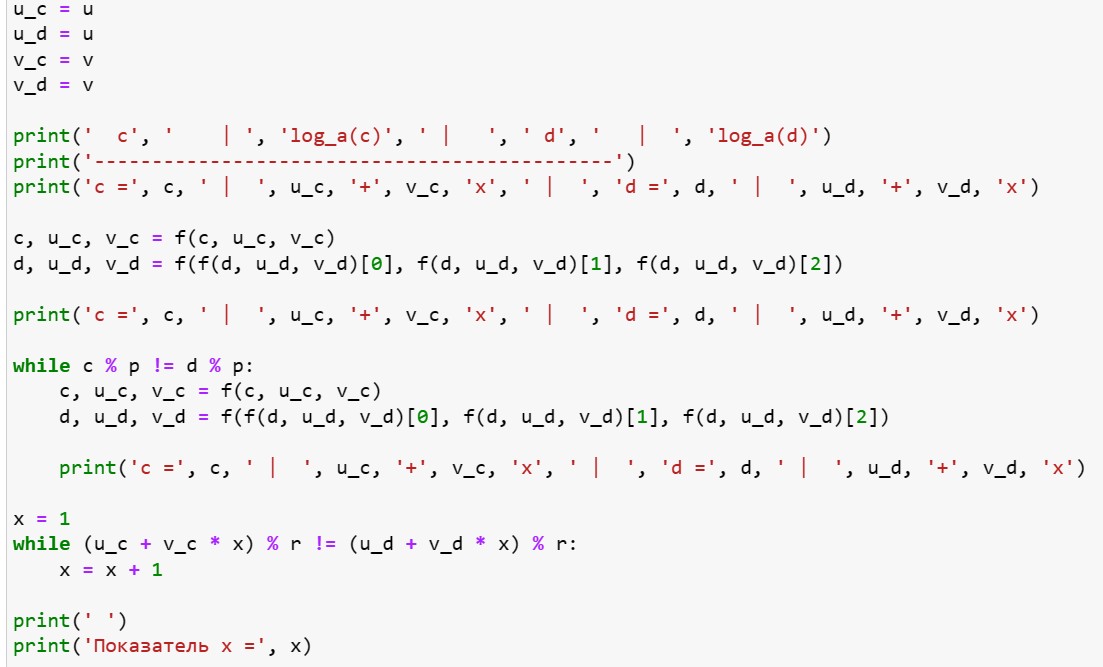


Рис. 2: p-метод Полларда для дискретного логарифмирования

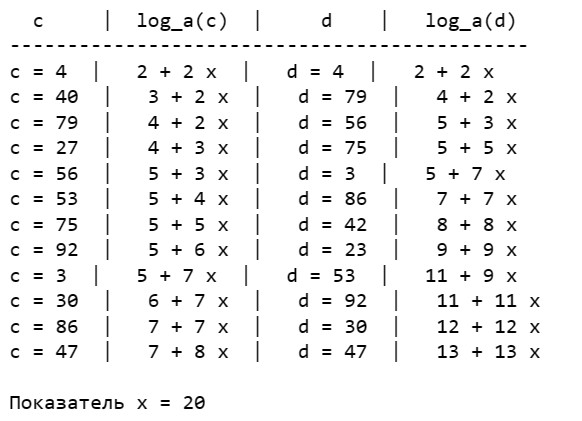


Рис. 3: p-метод Полларда для дискретного логарифмирования

# 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>.