Отчёт по лабораторной работе №7

Дисциплина: Математические основы защиты информации и информационной безопасности

Полиенко Анастасия Николаевна, НПМмд-02-23

Содержание

# 1 Цель работы

Изучить дискретное логарифмирование в конечном поле.

# 2 Задание

Реализовать алгоритм p-метода Полларда.

# 3 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.

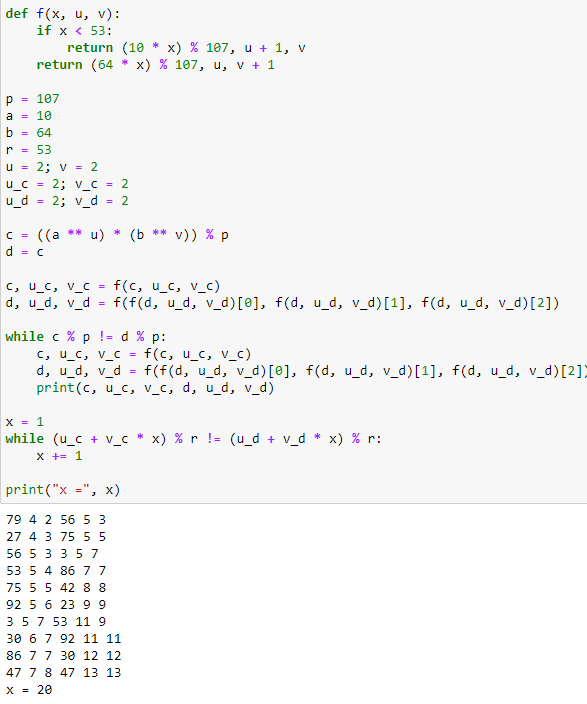
Обозначим , - простое целое число и назовем конечным полем из элементов. Задача дискретного логарифмирования в конечном поле формулируется так: для данных целых чисел и , , найти логарифм - такое целое число x, что (если такое число существует). По аналогии с вещественными числами используется обозначение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

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 .

Более подробно см. в [1–6].

# 4 Выполнение лабораторной работы

Реализуем алгоритм алгоритм p-метода Полларда. (рис. ??)



p-метод Полларда.

# 5 Выводы

Изучила дискретное логарифмирование в конечном поле.

# Список литературы

1. GNU Bash Manual [Электронный ресурс]. Free Software Foundation, 2016. URL: <https://www.gnu.org/software/bash/manual/>.

2. Newham C. [Learning the bash Shell: Unix Shell Programming](http://www.amazon.com/Learning-bash-Shell-Programming-Nutshell/dp/0596009658). O’Reilly Media, 2005. 354 с.

3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.

4. Robbins A. [Bash Pocket Reference](https://www.ncbi.nlm.nih.gov/pubmed/25246403). O’Reilly Media, 2016. 156 с.

5. Таненбаум Э. Архитектура компьютера. 6-е изд. СПб.: Питер, 2013. 874 с.

6. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.