Отчёт по лабораторной работе №7. Дискретное логарифмирование в конечном поле

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Майорова О.А., 1032212322
Группа: НФИмд-02-21
Преподаватель: д.ф.-м.н., Кулябов Д. С.

Москва, 2021

Цель и задачи

Цель: Ознакомиться с задачей дискретного логарифмирования в конечном поле.

Задача: Программно реализовать ρ-метод Полларда для задач дискретного логарифмирования.

ρ-метод Полларда

Вход: Простое число p, число a порядка r по модулю p, целое число $b : 1 < b < p$, f - отображение, обл-ее сжимающими св-ми и сохраняющее вычислимость логарифма.

1. Выбрать произвольные целые числа u, v и положить $c \leftarrow a^u b^v (\mod p), d \leftarrow c$.
2. Выполнять $c \leftarrow f(c) (\mod p), d \leftarrow f(f(d)) (\mod p)$, вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r, до получения равенства $c \equiv d (\mod p)$.
3. Приравняв логарифмы для c и d, вычислить логарифм x решением сравнения по модулю r. Результат: x или “Решений нет”.

Реализация ρ-метода Полларда

Задача: $10^x \equiv 64(\mod 107)$

Пусть $u = 2, v = 2$

Отображение: $f(c) = \begin{cases} 10c(\mod 107) & c < 53 \\ 64c(\mod 107) & c \geq 53 \end{cases}$

Проверка функции ρ-метода Полларда для задач дискретного логарифмирования:

```
1 PollardLog(107, 10, 53, 64, 2, 2)
```

```
20.0
```

Заключение

Таким образом, была достигнута цель, поставленная в начале лабораторной работы.

- Было осуществлено знакомство с задачей дискретного логарифмирования в конечном поле.
- Также была получена реализация на языке Python ρ-метода Полларда для задач дискретного логарифмирования.

Спасибо за внимание