

# **Математические основы защиты информации и информационной безопасности. Лабораторная работа №7.**

## **Дискретное логарифмирование в конечном поле**

---

Масолова Анна Олеговна, НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич

11 декабря, 2021, Москва, Россия

Российский Университет Дружбы Народов

# Цели и задачи

---

## Цель лабораторной работы

Изучение алгоритма  $p$ -Полларда для задач дискретного логарифмирования.

Реализовать программно алгоритм, реализующий  $p$ -метод Полларда для задач дискретного логарифмирования

# **Выполнение лабораторной работы**

---

Задача обращения функции  $g^x$  в некоторой конечной мультипликативной группе  $G$ .

Наиболее часто задачу дискретного логарифмирования рассматривают в мультипликативной группе кольца вычетов или конечного поля, а также в группе точек эллиптической кривой над конечным полем. Эффективные алгоритмы для решения задачи дискретного логарифмирования в общем случае неизвестны.

Для заданных  $g$  и  $a$  решение  $x$  уравнения  $g^x = a$  называется дискретным логарифмом элемента  $a$  по основанию  $g$ .



## р-метод Полларда для задач дискретного логарифмирования

- Вход. Простое число  $p$ , число  $a$  порядка  $r$  по модулю  $p$ , целое число  $b$ ,  $1 < b < p$ ; отображение  $f$ , обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.
- Выход. Показатель  $x$ , для которого  $a^x \equiv b \pmod{p}$ , если такой показатель существует.

## р-метод Полларда для задач дискретного логарифмирования

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

## Пример работы р-алгоритма Полларда

```
10 ** 20 ≡ 64 (mod 107)  
Verify result: verified
```

**Figure 1:** Пример работы р-алгоритма Полларда

## **Выводы**

---

# Результаты выполнения лабораторной работы

В ходе выполнения работы был успешно изучен р-метод Полларда для задач дискретного логарифмирования, а также был реализован программно на языке Python.