

Информационная безопасность. Лабораторная работа № 7 на тему “Дискретное логарифмирование”

Некпай Амруддин

RUDN University, Moscow, Russian Federation

Цели и задачи

Изучение задачи дискретного логарифмирования.

Выполнение лабораторной работы

Задача дискретного логарифмирования

Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа x , удовлетворяющего уравнению. Если оно разрешимо, у него должно быть хотя бы одно натуральное решение, не превышающее порядок группы.

- 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 $a^x = b(\text{mod } p)$, если такой показатель существует.
1. Выбрать произвольные целые числа u, v и положить $c = a^u b^v(\text{mod } p), d = c$
 2. Выполнять $c = f(c)(\text{mod } p), d = f(d)(\text{mod } p)$, вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r , до получения равенства $c = d(\text{mod } p)$
 3. Приняв логарифмы для c и d , вычислить логарифм x решением сравнения по модулю r . Результат x или РЕШЕНИЯ НЕТ.

Алгоритм полного перебора нашёл бы решение за число шагов не выше порядка данной группы.

Работа алгоритма

Figure 1: Работа алгоритма

Выводы

Изучили задачу дискретного логарифмирования.