САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

Институт компьютерных наук и технологий

Кафедра «Распределенные вычисления и компьютерные сети»

Курсовая работа

на тему: Метод Сильвера-Полига-Хеллмана

по дисциплине: Основы компьютерной алгебры

Выполнил студент

гр. 23507/1 <*подпись*> В.Б.Борисов

Руководитель

доц. кафедры <*подпись*> П.В.Трифонов

«___» _____ 2015 г.

Санкт-Петербург

2015

СОДЕРЖАНИЕ

Введение

Алгоритм Полига — Хеллмана (также называемый *алгоритм Сильвера — Полига — Хеллмана*) — детерминированный алгоритм дискретного логарифмирования в кольце вычетов по модулю простого числа. Одной из особенностью алгоритма является то, что для простых чисел специального вида можно находить дискретный логарифм за полиномиальное время.

Алгоритм Полига—Хеллмана крайне эффективен, если $p-1$ раскладывается на небольшие простые множители. Это очень важно учитывать при выборе параметров криптографических схем. Иначе схема будет ненадёжной.

Основная часть

Постановка задачи

Реализовать метод Сильвера-Полига-Хеллмана по модулю сколь угодно большого простого числа на языке C++.

Описание алгоритма

Пусть задано сравнение

$$a^x \equiv b \pmod{p},$$

и известно разложение числа $p-1$ на простые множители:

$$p-1 = \prod_{i=1}^{k} q_i^{\alpha_i}.$$

Необходимо найти число $x,\ 0 \le x < p-1$, удовлетворяющее сравнению.

Составить таблицу значений $\{r_{i,j}\}$, где $\{r_{i,j}\}=a^{j*\frac{p-1}{q_i}}, i\epsilon\{1,\dots.k\}, j\epsilon\{0,\dots.q_i-1\}$

Вычислить $loga^b mod q_i^{\alpha_i}$

Для i от 1 до k

Пусть

$$x \equiv loga^b \equiv x_0 + x_1 q_i + .. + x_{\alpha_{i-1}} q_i^{\alpha_i - 1} (mod q_i^{\alpha_i})$$

Где $0 \le x_i \le q_i - 1$

Тогда верно сравнение: $a^{x_0 * \frac{p-1}{q_i}} \equiv b^{\frac{p-1}{q_i}} (mod\ p)$

Вывод верхнего сравнения:

С помощью таблицы, составленной на шаге 1, находим x_0. Для j от 1 до $\alpha_i - 1$.
Рассматриваем сравнение

$$a^{x_j * \frac{p-1}{q_i}} \equiv (ba^{-x0-x1qi\ldots-xj-1q_i^{j-1}})^{q_i^{\frac{p-1}{j+1}}} (mod\ p)$$

Решение опять же находится по таблице

Конец цикла по j

Конец цикла по i

Найдя $loga^b mod q_i^{\alpha_i}$ для всех i, находим $loga^b mod(p-1)$

По китайской теореме об остатках

Тестирование

Чтобы убедиться в правильности написанной программы были проведены тесты, которые показали не только корректные результаты, но и время работы алгоритма. Ниже приведена таблица результатов.

Входные данные	Результат	Время работы алгоритма в секундах
3 13 17	4	0
2 5 7237	4085	0.015
2 40 37	Нет решений	0.015
71 210 251	197	0.015
123123 123123 999997	1	0.078
1231231 1231231 1982354	1	0.156

Заключение

Алгоритм и длинная арифметика к нему реализованы на C++. Программа протестирована так и на малых, так и на больших числах. Проверено корректность вычислений с помощью программного пакета Maple. Поставленная задача решена.

Список литературы

[1] П.В Трифонов, Построение и анализ алгоритмов