ПРАВИТЕЛЬСТВО    РОССИЙСКОЙ    ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего профессионального образования Национальный исследовательский университет «Высшая школа экономики»

Московский институт электроники и математики Национального исследовательского университета «Высшая школа экономики»

Департамент Прикладной Математики

Кафедра «Компьютерная безопасность»

Лабораторная работа №1

по дисциплине «Программирование алгоритмов защиты информации»

Выполнил:

студент группы СКБ-171

Лисьев А. Н.

Проверил:

Нестеренко А. Ю.

МОСКВА – 2021

**Задание**

Реализовать алгоритм вычисления кратной точки для заданной кривой (Монтгомери), используя набор функций из библиотеки GMP.

**Математическое описание**

*ОПР*. Эллиптическая кривая над полем K — неособая кубическая кривая на проективной плоскости над задаваемая уравнением 3-й степени с коэффициентами из поля K и «точкой на бесконечности».

ОПР. точка эллиптической кривой, k∈Z, называется кратной точкой.

Алгоритм:

1. Получаем на вход k и P
2. k переводится в двоичное представление
3. Для каждого :
   1. Если
   2. Если

Операции сложения и удвоения зависят от эллиптической кривой, над которой происходит вычисление кратной точки.

ОПР. Кривая Монтгомери – это эллиптическая кривая над полем , заданная в аффинных координатах уравнением:

В аффинных координатах формулы сложения двух точек и удвоение требуют выполнения неэффективной операции деления. По этой причине осуществляется переход в проективные координаты:

Т. е. точка переходит в . Поскольку в ходе вычислений координата y не используется, ее опускают.

В проективных координатах требуемые формулы имеют вид:

1. Сложение:
2. Удвоение:

В конце алгоритма можно перевести точку обратно в аффинные координаты, но, поскольку Z в знаменателе, нужно рассмотреть два случая:

Тесты

p – характеристика простого поля, над которым определяется эллиптическая кривая;

q – порядок подгруппы простого порядка группы точек эллиптической кривой.

Перед вычислением кратной точки можно убедиться, что указанная точка P лежит на заданной кривой, с помощью символа Якоби. Для этого необходимо вычислить и посчитать значение символа Якоби для n и p. Если он равен 1, точка принадлежит эллиптической кривой.

Для тестирования алгоритма можно использовать следующие свойства:

1. ;
2. .

**Библиотека GMP**

Библиотека позволяет проводить вычисления над большими числами. Целые числа в GMP представлены типом .

Для инициализации и определения переменных типа будут использоваться следующие функции:

1. – инициализация одной переменной нулем;
2. – инициализация нескольких переменных нулем;
3. – установить значение равным
4. – установить значение равным в системе счисления с основанием ;
5. – проинициализировать переменную , а затем установить ее значение равным в системе счисления с основанием .

Для освобождения ресурсов будут использоваться следующие функции:

1. – очистить память, в которой хранится
2. – очистить память, в которой хранится

Вычисление необходимых математических операций будет осуществляться с помощью функций:

1. – сложить и , а результат записать в ;
2. – вычесть из , а результат записать в ;
3. – умножить на , а результат записать в ;
4. – привести по модулю , а результат записать в ;
5. – вычислить по модулю , а результат записать в ;
6. – вычислить по модулю , а результат записать в ;
7. – вычислить

В реализации алгоритма также используются некоторые вспомогательные функции:

1. – эквивалентно функции
2. – используется для инициализации рандомного состояния
3. – получение рандомного числа в диапазоне от до с помощью и запись результата в
4. – освобождение памяти, выделенной под
5. сравнение с нулем
6. *– проверяет значение бита*
7. – проверяет длину представления числа в системе счисления с основанием

Список литературы:

1. **Bernstein Daniel и Lange Tanja** Montgomery curves and the Montgomery ladder [В Интернете]. - Technische Universiteit Eindhoven, The Netherlands; University of Illinois at Chicago, USA. - <https://eprint.iacr.org/2017/293.pdf>.
2. **ГОСТ РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ** Параметры эллиптических кривых для криптографических алгоритмов и протоколов.
3. **Ю. Нестеренко А.** Курс лекций «Методы программной реализации СКЗИ»