1. 7Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский политехнический университет Петра Великого
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 2**

1. «Поиск длин циклов в последовательностях»
2. по дисциплине «Быстрые вычислительные алгоритмы»
3. Выполнил
4. студент гр. 5151001/00201 Устюгов А.А.

<*подпись*>

1. Преподаватель д.т.н. Шенец Н.Н.

<*подпись*>

1. Санкт-Петербург
2. 2024

# Цель работы

Изучение алгоритмов поиска длин циклов в последовательностях, порождаемых некоторым случайным отображением, и их применения в криптографии.

# Задание

1. Написать программу, которая реализует один их алгоритмов поиска длины цикла отображения. Вариант 6: алгоритм Брента.
2. Написать программу, которая решает задачу дискретного логарифмирования в группе точек эллиптической кривой в соответствии с вариантом задания.

# Ход работы

Обе программы были написаны на языке c++, с использованием библиотеки Miracl для сложения точек эллиптической кривой.

В программе 1 необходимо реализовать алгоритм Брента с заданным отображением. Заданное отображение представляет собой композицию двух подстановок, одна из них задается в входном файле программы, другая генерируется с помощью ЛКГ с следующими параметрами: m=16, a=5, c=7.

Основная идея алгоритма Брента состоит в том, что необходимо фиксировать элемент с индексом и проверять следующих элементов.

Был реализован алгоритм, предложенный в методическом пособии. Так как подстановки 4-битные, то длины циклов последовательности небольшие. Результат работы представлен на рисунке 1

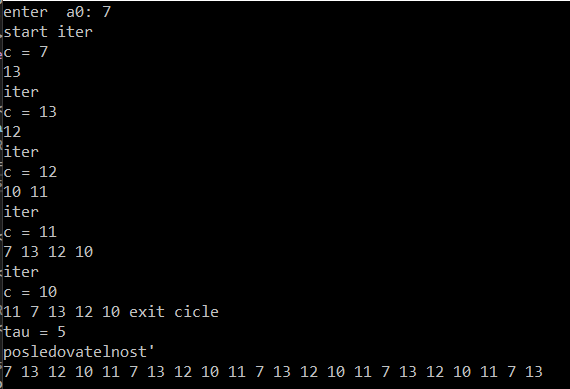


Рисунок 1 – найденная длина цикла последовательности

Далее необходимо реализовать метод Госпера для решения задачи дискретного логарифмирования в группе точек эллиптической кривой. Основная идея метода состоит в поиске коллизии двух точек, то есть необходимо найти такие точки, для которых выполняется следующее равенство:

*,* где точки *P* и *Q = d\*P* заранее известны.

Для поиска коллизии необходимо разбить все множество точек эллиптической кривой на не пересекаемые множества. Экспериментально показано, что в данном методе необходимо разбить точки на 500 и более подмножеств. В своей программе я разбиваю на 500 подмножеств, и в *i-*тое множество попадают точки, у которых совпадает остаток от деления на 500 *x*-координаты точки. После разбиения, необходимо определить отображение *f,* которое необходимо для построения графа*.* В моей программе задано следующие отображение: где *i –* номер множества, которому принадлежит точка *R.*

После того, как мы задались отображением, то мы пользуемся алгоритмом Госпера для поиска длины цикла, только здесь нам важна не сама длина цикла, а совпадение точек и соответствующие этим точкам коэффициенты. Из них и находится секретный показатель *d*.

После написанный метод был протестирован на некоторых кривых. Первым тестом был предложенный в методическом пособии со следующими параметрами:

Результат работы программы представлен на рисунке 2.



Рисунок 2 – результат для теста из методического пособия

Далее были сгенерированы 3 кривые с разным количеством числа точек. В следующих тестах число точек соответствуют числам длиной 30, 35, 46, 70 бит.

Тест для числа точек длиной 30 бит. Параметры:

Результат представлен на рисунке 3.



Рисунок 3 – результат теста для числа точек длины 30 бит.

Тест для числа точек длиной 35 бит. Параметры:

Результат представлен на рисунке 4.



Рисунок 4 – результат теста для числа точек длины 35 бит.

Тест для числа точек длиной 46 бит. Параметры:

Результат представлен на рисунке 5.



Рисунок 5 – результат теста для числа точек длины 46 бит

Тест для числа точек длиной 70 бит. Параметры:

Данный тест работал около 150 минут, и за это время не было найдено решение.

# Контрольные вопросы

1. Что такое цикл и подход к циклу?

Циклом называют такую последовательность подряд идущих элементов, для которых справедливо для некоторого , называемого периодом цикла. Соответственно, подходом к циклу называется последовательность

1. Какой из алгоритмов поиска длины цикла предпочтительнее и почему?

Нет универсального ответа, все зависит от того, какими вы обладаете вычислительными способностями, что вы изначально знаете о данных, с которыми придется работать и какую задачу вам необходимо решать. Если вы обладаете достаточным объемом памяти, то предпочтительнее воспользоваться алгоритмом Госпера. Если же при достатке памяти вы еще и знаете, что у вас на множестве можно задать или задано отношение упорядоченности, то можно воспользоваться алгоритмом Ниваша, который гарантирует что будет не более двух проходов по циклу. В случае, если памяти не хватает, то на свое усмотрение можно воспользоваться как алгоритмом Флойда, так и алгоритмом Брента.

1. Какие задачи решаются с применением поиска длины цикла последовательности?

С помощью поиска длины циклов решаются задачи дискретного логарифмирования, факторизации целых чисел, поиска коллизий хэш-функции, а также анализируют блочные шифры.

# Вывод

В ходе выполнения лабораторной работы были изучены алгоритмы поиска длин циклов. Были реализован алгоритм Брента для поиска длины цикла и метод Госпера для решения задачи дискретного логарифмирования в группе точек эллиптической кривой.