Методические указания по выполнению лабораторных работ, предусмотренных рабочей программой, и требования к порядку выполнения заданий по дисциплине «Теоретико-числовые методы в криптографии» для студентов 5-го курса (для специальности 10.05.01 – Компьютерная безопасность)

Лабораторная работа 1 **(4-я неделя)**

Арифметические операции в числовых полях

Цель работы — изучение основных операции в числовых полях и их программная реализация.

Порядок выполнения работы

1. Разобрать алгоритмы Евклида (обычный, бинарный и расширенный) вычисления НОД целых чисел и привести их программную реализацию ([1], глава 1).
2. Разобрать алгоритмы решения систем сравнений и привести их программную реализацию ([1], стр.28-31, [1], стр.270-273).
3. Рассмотреть метод Гаусса решения систем линейных уравнений над конечными полями и привести его программную реализацию ([5], стр.275-291).

Содержание отчета

1. Постановка задачи.
2. Теоретические сведения по рассмотренным темам с их обоснованием.
3. Результаты работы, в том числе:
   - описание алгоритмов Евклида вычисления НОД целых чисел ;
   - описание алгоритмов решения систем сравнений;
   - описание алгоритма решения систем линейных уравнений над конечными полями методом Гаусса;
   - псевдокоды рассмотренных алгоритмов;
   - коды программ, реализующей рассмотренные алгоритмы;
   - оценки сложности рассмотренных алгоритмов;
   - результаты тестирования программ.
4. Выводы по работе - см.образец ([2], стр.287-289).

Лабораторная работа 2 **(7-я неделя)**

Цепные дроби и квадратные сравнения

Цель работы — изучение основных свойств цепных дробей и квадратных сравнений.

Порядок выполнения работы

1. Разобрать алгоритм разложения чисел в цепную дробь и привести их программную реализацию ([1], глава 3).
2. Рассмотреть алгоритмы приложений цепных дробей и привести их программную реализацию ([1], глава 3).

3. Разобрать алгоритмы вычисления символов Лежандра и Якоби и привести их программную реализацию ([1], глава 2).
4. Рассмотреть алгоритмы извлечения квадратного корня в кольце вычетов ([1], р. 2.4.1).

Содержание отчета

1. Постановка задачи.
2. Теоретические сведения по рассмотренным темам с их обоснованием.
3. Результаты работы, в том числе:
   - описание алгоритмов разложения чисел в цепную дробь;
   - описание алгоритмов приложений цепных дробей ;
   - описание алгоритмов вычисления символов Лежандра и Якоби;
   - описание алгоритмов извлечения квадратного корня в кольце вычетов;
   - псевдокоды рассмотренных алгоритмов;
   - коды программ, реализующей рассмотренные алгоритмы;
   - оценки сложности рассмотренных алгоритмов;
   - результаты тестирования программ.
4. Выводы по работе - см.образец ([2], стр.287-289).

Лабораторная работа 3 **(10-я неделя)**

Проверка чисел на простоту

Цель работы — изучение основных методов проверки простоты чисел и их программная реализация.

Порядок выполнения работы

1. Рассмотреть тест Ферма проверки чисел на простоту и привести его программную реализацию ([2], стр.169-191; [1], глава 5),
2. Рассмотреть тест Соловея-Штрассена проверки чисел на простоту и привести его программную реализацию ([2], стр.169-191; [1], глава 5),
3. Рассмотреть тест Миллера-Рабина и привести его программную реализацию ([2], стр.169-191; [1], глава 5),

Содержание отчета

1. Постановка задачи.
2. Теоретические сведения по рассмотренным темам с их обоснованием.
3. Результаты работы, в том числе:
   - описание алгоритма теста Ферма проверки чисел на простоту;
   - описание алгоритма теста Соловея-Штрассена проверки чисел на простоту;
   - описание алгоритма теста Миллера-Рабина проверки чисел на простоту;
   - псевдокоды рассмотренных алгоритмов;
   - коды программ, реализующей рассмотренные алгоритмы;
   - результаты тестирования программ;
   - оценки сложности рассмотренных алгоритмов.
4. Выводы по работе - см.образец ([2], стр.290-296).

Лабораторная работа 4 **(12-я неделя)**

Факторизация целых чисел

Цель работы — изучение основных методов факторизации целых чисел и их программная реализация.

Порядок выполнения работы

1. Рассмотреть ρ-метод Полларда разложения целых чисел на множители и привести его программную реализацию ([2], стр.209-224; [1], глава 6),
2. Рассмотреть (p-1)-метод Полларда разложения целых чисел на множители и привести его программную реализацию ([2], стр.169-191; [1], глава 6),
3. Рассмотреть метод цепных дробей разложения целых чисел на множители и привести его программную реализацию ([2], стр.169-191; [1], глава 6).

Содержание отчета

1. Постановка задачи.
2. Теоретические сведения по рассмотренным темам с их обоснованием.
3. Результаты работы, в том числе:
   - описание алгоритма ρ-метода Полларда разложения целых чисел на множители;
   - описание алгоритма (p-1)-метода Полларда разложения целых чисел на множители;
   - описание алгоритма вычисления числителей подходящих дробей квадратичной иррациональности;
   - описание алгоритма метода непрерывных дробей разложения целых чисел на множители;
   - псевдокоды рассмотренных алгоритмов;
   - коды программ, реализующей рассмотренные алгоритмы;
   - результаты тестирования программ;
   - оценки сложности рассмотренных алгоритмов.
4. Выводы по работе - см.образец ([2], стр.296-299).

Лабораторная работа 5 **(14-я неделя)**

Дискретное логарифмирование в конечном поле

Цель работы — изучение основных методов дискретного логарифмирования в конечном поле и их программная реализация.

Порядок выполнения работы

1. Рассмотреть метод Гельфонда-Шенкса вычисления дискретного логарифма и привести его программную реализацию ([1], стр.280-282; [2], глава 7).
2. Рассмотреть ρ-метод Полларда вычисления дискретного логарифма и привести его программную реализацию [1], стр.289-296; [2], глава 7).
3. Рассмотреть метод вычисления дискретного логарифма в конечных полях ([1], стр.297-305; [2], глава 7)..

Содержание отчета

1. Постановка задачи.
2. Теоретические сведения по рассмотренным темам с их обоснованием.
3. Результаты работы, в том числе:
   - описание алгоритма метод Гельфонда-Шенкса вычисления дискретного логарифма;
   - описание алгоритма ρ-метода Полларда вычисления дискретного логарифма;
   - описание алгоритма вычисления дискретного логарифма в конечном простом поле;
   - псевдокоды рассмотренных алгоритмов;
   - коды программ, реализующей рассмотренные алгоритмы;
   - результаты тестирования программ;
   - оценки сложности рассмотренных алгоритмов.
4. Выводы по работе - см.образец ([2], стр.299-303).

.

Лабораторная работа 6*

Дискретное преобразование Фурье

Цель работы — изучение свойств дискретного преобразования Фурье и программная реализация его приложений.

Порядок выполнения работы

1. Разобрать определения дискретного преобразования Фурье, обратного дискретного преобразования Фурье и алгоритмы этих преобразований Фурье. Привести программную реализацию быстрого преобразования Фурье и обратного быстрого преобразования Фурье ([6], p.1.10).
2. .Рассмотреть приложения дискретного преобразования Фурье и привести программную реализацию алгоритма Шенхаге-Штрассена для умножения целых чисел ([6], p.1.10.5).

Содержание отчета

1. Постановка задач.
2. Теоретические сведения по рассмотренным темам с их обоснованием.
3. Результаты работы, в том числе:
   - описание алгоритма построения дискретного преобразования Фурье;
   - описание алгоритма вычисления произведения многочленов с помощью быстрого преобразования Фурье;
   - описание вычисления произведения целых чисел с помощью алгоритма Шенхаге-Штрассена;
   - псевдокоды рассмотренных алгоритмов;
   - коды программ, реализующей рассмотренные алгоритмы;
   - результаты тестирования программ для полученных у преподавателя наборов данных;
   - оценки сложности рассмотренных алгоритмов.
4. Выводы по работе.

Лабораторная работа 7*

Алгоритм Ленстры-Ленстры-Ловаша

Цель работы — изучение алгоритма минимизации базиса решетки и его программная реализация.

Порядок выполнения работы

1. Рассмотреть алгоритм Гаусса редукции решеток размерности 2 и привести его программную реализацию ([3], p.9.2.2).
2. Рассмотреть Алгоритм Ленстры-Ленстры-Ловаша (LLL-алгоритм) и привести его программную реализацию ([3], p.9.4.1).
3. Реализовать алгоритм решения задачи целочисленного программирования с помощью LLL-алгоритма ([3], p.9.4.2).

Содержание отчета

1. Постановка задачи.
2. Теоретические сведения по рассмотренным темам с их обоснованием.
3. Результаты работы, в том числе:
   - описание и псевдокод алгоритма редукции решеток размерности 2;
   - описание и псевдокод LLL-алгоритма;
   - описание и псевдокод алгоритма решения задачи целочисленного программирования;
   - коды программ, реализующей LLL-алгоритм;
   - результаты тестирования программ;
   - оценки сложности рассмотренных алгоритмов.
4. Выводы по работе - см.образец ([4], стр.303-307).

Для зачета каждой лабораторной работы необходимо представить письменный отчет с изложением изученных теоретических вопросов, ***программной реализацией не менее половины разработанных алгоритмов*** и результатами тестирования компьютерных программ.

Выполнение лабораторных работ 6*,7* будет зависеть от прочитанных лекций.

Задания для контрольной работы

Контрольная работа выполняется в конце 9 семестра по следующему образцу.

1. Представить рациональное число $\frac{323}{17}$ в виде непрерывной дроби и выписать все ее подходящие дроби. (3 *балла*)
2. Вычислить символ Якоби $\left(\frac{532}{2739}\right)$. (3 *балла*)
3. Найти общее и одно частное решение для следующей системы линейных уравнений:

$$\begin{cases} x_1 + 3x_2 + x_3 + 4x_4 = 2, \\ x_1 + 5x_3 + x_4 = 0, \\ 3x_1 + x_2 + x_4 = 3, \end{cases}$$ в поле Z_5. (3 *балла*)

4. Решим систему линейных сравнений:

$$\begin{cases} x \equiv 4 (\mathrm{mod}\, 9) \\ x \equiv 3 (\mathrm{mod}\, 4) \\ x \equiv 2 (\mathrm{mod}\, 7). \end{cases}$$

(*3 балла*)

5. Определить порядок элемента $a = 3$ в группе $\boldsymbol{Z}_{37}^{*}$. (*4 балла*)
6. Вычислить $x = \log_2 8$ в группе Z_{13}^{*} методом сведения к собственным подгруппам. (4 *балла*)

Всего 20 баллов:
10-13 – удовлетворительно,
14-17 – хорошо,
18-20 – отлично.

Рекомендуемый библиографический список

1. Глухов М. М. и др. Введение в теоретико-числовые методы криптографии: учеб. пособие - Москва : Лань, 2011.
2. Маховенко Е.Б. Теоретико-числовые методы в криптографии. М.: Гелиос АРВ, 2006.
3. Черемушкин, А. В. Лекции по арифметическим алгоритмам в криптографии. - Москва : МЦНМО, 2002.
4. Панкратова И.А. Теоретико-числовые методы в криптографии. Томск, 2009.
5. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.:МЦНМО, 2003.
6. Венбо Мао. Современная криптография: теория и практика. М.:Вильямс, 2005.