Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий
Кафедра информационной безопасности и теории управления

А.В. Аминаров, А.М. Иванцов, С.М. Рацеев

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО МАТЕМАТИЧЕСКИМ МЕТОДАМ ЗАЩИТЫ ИНФОРМАЦИИ

Ульяновск
2015

УДК 004.056 (075.8)
ББК 32.972.53 Я 73
А 62

Печатается по решению Ученого совета
факультета математики, информационных и авиационных
технологий Ульяновского государственного университета
(протокол № 9/15 от 20.11.2015)

Рецензенты:
доктор технических наук, профессор **А.А. Смагин**.

Аминаров А.В., Иванцов А.М., Рацеев С.М.

Учебно-методические указания для проведения лабораторных работ по математическим методам защиты информации для студентов специальностей «Компьютерная безопасность» и «Математическое обеспечение и администрирование информационных систем» / А.В. Аминаров, А.М. Иванцов, С.М. Рацеев. – Ульяновск: УлГУ, 2015 – 61 с.

Рассматриваются методические указания для проведения лабораторных работ по освоению основных математических методов защиты информации.

Предназначено для студентов 2-5 курсов, осваивающих практические вопросы защиты информации.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В учебно-методическое пособие входят двадцать шесть лабораторных работ, направленных на освоение студентами основных математических методов защиты информации и сопутствующих им вспомогательных теоретико-числовых алгоритмов.

Данное учебно-методическое пособие разработано в соответствии с учебными планами курсов «Вычислительные методы в алгебре и теории чисел», «Криптографические методы защиты информации», «Теоретико-числовые методы в криптографии», «Теория псевдослучайных генераторов» и «Системный анализ».

Лабораторные работы скомпонованы в 5 глав (название главы соответствует названию дисциплины), каждая из которых включает лабораторные работы по указанной дисциплине.

Главы 1-5 посвящены лабораторным работам, которые проводятся в ходе изучения дисциплин по специальности «Компьютерная безопасность», глава 2 включает лабораторный практикум по направлению бакалавриата «Математическое обеспечение и администрирование информационных систем».

ГЛАВА 1. ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В АЛГЕБРЕ И ТЕОРИИ ЧИСЕЛ

Лабораторная работа №1

ДИОФАНТОВЫ УРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ

Цель работы: освоение методов решений линейных диофантовых уравнений первой степени вида $ax + by = c$ на основе обобщенного алгоритма Евклида.

Задание

Требуется составить программу, которая для любых целых чисел a, b и c находит все решения линейного диофантова уравнения первой степени вида $ax + by = c$. Если данное уравнение не имеет решений, то вывести сообщение об этом. Если уравнение $ax + by = c$ имеет решение, то решений будет бесконечно много. В этом случае результатом работы программы должна быть формула, с помощью которой описываются все решения рассматриваемого уравнения.

Методические указания

Для нахождения частного решения использовать обобщенный алгоритм Евклида. Теоретический материал для выполнения работы можно найти в учебном пособии [16].

Контрольные вопросы

1. Теорема о разложении одного целого числа по модулю другого (основная теорема делимости целых чисел).
2. q-ичные системы счисления (представление и единственность).
3. Отношение делимости в кольце целых чисел и его свойства.
4. Наибольший общий делитель и его свойства.

5. Алгоритм Евклида. Расширенный алгоритм Евклида.

6. Диофантовы уравнения первой степени. Критерий существования решения. Формула общего решения.

Лабораторная работа №2

КОНЕЧНЫЕ ЦЕПНЫЕ ДРОБИ

Цель работы: освоение методов представлений рациональных чисел в виде конечных цепных дробей и, наоборот, представление конечных цепных дробей рациональными числами.

Задание

Требуется составить программу, которая для любых целых чисел a и b, причем b не равно нулю, представляет рациональное число $\frac{a}{b}$ в виде конечной цепной дроби. И обратно, представить конечную цепную дробь в виде рационального числа вида $\frac{a}{b}$.

Методические указания

Для представления рационального числа $\frac{a}{b}$ в виде конечной цепной дроби использовать алгоритм Евклида. Для представления конечной цепной дроби рациональным числом использовать так называемые подходящие дроби. Теоретический материал для выполнения работы можно найти в учебном пособии [16].

Контрольные вопросы

1. Конечные цепные дроби. Представление рационального числа конечной цепной дробью.
2. Подходящие дроби, их вычисление и основные свойства.

Лабораторная работа №3

МУЛЬТИПЛИКАТИВНЫЕ ФУНКЦИИ

Цель работы: освоение методов работы с мультипликативными функциями.

Задание

Требуется составить программу, которая для любого натурального числа a находит значения мультипликативных функций $\tau(a)$, $s(a)$, $\varphi(a)$, где $\tau(a)$ – количество всех делителей числа a, $s(a)$ – сумма всех делителей числа a, φ – функция Эйлера.

Методические указания

Пусть $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ – каноническое разложение числа a. Тогда

$$\tau(a) = (1+\alpha_1)(1+\alpha_2)\ldots(1+\alpha_n),$$

$$S(a) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}\,\frac{p_2^{\alpha_2+1}-1}{p_2-1}\ldots\frac{p_n^{\alpha_n+1}-1}{p_n-1},$$

$$\varphi(a) = a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_n}\right).$$

Теоретический материал для выполнения работы можно найти в учебном пособии [16].

Контрольные вопросы

1. Взаимно простые числа и их свойства.
2. Простые числа и их свойства.
3. Каноническое разложение целого числа.
4. Мультипликативные функции и их свойства. Примеры мультипликативных функций.
5. Леммы о мультипликативных функциях.

6. Функция Мебиуса и ее свойства.
7. Функция Эйлера и ее вычисление.

Лабораторная работа №4

СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ

Цель работы: освоение методов решений сравнений первой степени.

Задание

Требуется составить программу, которая для любых целых чисел a, b и m, $m > 0$, находит все решения сравнения $ax \equiv b(m)$ следующими способами:

– с помощью функции Эйлера;

– с помощью обобщенного алгоритма Евклида;

– с помощью конечных цепных дробей.

Методические указания

При нахождении решения сравнения $ax \equiv b(m)$ с помощью функции Эйлера использовать быстрый (бинарный) алгоритм возведения в степень. Теоретический материал для выполнения работы можно найти в учебном пособии [16].

Контрольные вопросы

1. Отношение сравнимости в кольце целых чисел и его свойства.
2. Полная и приведенная системы вычетов и их свойства.
3. Теорема Эйлера.
4. Теорема Ферма.
5. Сравнения первой степени $ax \equiv b(\mathrm{mod}\, m)$. Случай $(a, m) = 1$.
6. Сравнения первой степени $ax \equiv b(\mathrm{mod}\, m)$. Случай $(a, m) > 1$.

Лабораторная работа №5

СИСТЕМЫ СРАВНЕНИЙ ПЕРВОЙ СТЕПЕНИ

Цель работы: освоение методов решений систем сравнений первой степени.

Задание

Требуется составить программу, которая для любого натурального s, любых натуральных попарно взаимно простых чисел $m_1,...,m_s$ и любых целых чисел $b_1,...,b_s$ находит решение системы сравнений первой степени вида

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \quad\quad ... \\ x \equiv b_s \pmod{m_s} \end{cases}$$

Методические указания

Для нахождения решения системы сравнений первой степени использовать китайскую теорему об остатках. Теоретический материал для выполнения работы можно найти в учебном пособии [16].

Контрольные вопросы

1. Системы сравнений первой степени и методы их решения.
2. Китайская теорема об остатках.
3. Схема разделения секрета на основе китайской теоремы об остатках.

Лабораторная работа №6

ПЕРВООБРАЗНЫЕ КОРНИ

Цель работы: освоение методов нахождения первообразных корней по простому модулю.

Задание

Требуется составить программу, которая для любого простого числа p находит все первообразные корни по модулю p.

Методические указания

Использовать следующий критерий первообразного корня по простому модулю. Пусть $p-1=p_1^{\alpha_1}p_2^{\alpha_2}...p_n^{\alpha_n}$ – каноническое разложение числа $p-1$, где p – некоторое простое число. Тогда некоторое число a является первообразным корнем по модулю p тогда и только тогда, когда

$$a^{\frac{p-1}{p_1}} \not\equiv 1 \ (mod\ p).\ldots.\ a^{\frac{p-1}{p_n}} \not\equiv 1 \ (mod\ p).$$

Теоретический материал для выполнения работы можно найти в учебном пособии [16].

Контрольные вопросы

1. Сравнения произвольной степени по простому модулю.
2. Сравнения по составному модулю.
3. Степенные вычеты. Показатель числа.
4. Первообразные корни по простому модулю. Критерий проверки первообразного корня.

ГЛАВА 2. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Лабораторная работа №1

ШИФРЫ ЗАМЕНЫ И ПЕРЕСТАНОВКИ

Цель работы: изучение классических криптографических алгоритмов одноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты открытых текстов.

Задание

Разработать криптографическую защиту информации, содержащейся в текстовом (двоичном) файле данных, с помощью алгоритма шифрования, указанного в варианте. Для этого:

1. Разработать алгоритмы шифрования и расшифрования открытого текста из алфавита A на заданном ключе с помощью метода, указанного в варианте.

2. Определить алфавит A криптосистемы (открытого текста и шифртекста). Если алфавит A не задан в варианте, выбрать его самостоятельно, так, чтобы он включал в себя символы используемого в примере открытого текста. Например, русский, английский, ASCII.

3. Написать функцию генерации случайных ключей шифра, оценить размерность ключевого пространства.

4. Написать функцию, реализующую шифрование на заданном ключе открытого текста, состоящего из символов заданного алфавита. Открытый текст, ключ и шифртекст должны быть представлены отдельными файлами.

5. Написать функцию для реализации алгоритма расшифрования полученного шифрованного файла при известном ключе.

Варианты заданий

1. Шифр простой замены.

2. Шифр сдвига с числовым ключом для двоичных файлов. Алфавит A – кольцо вычетов по модулю 256.

3. Шифр сдвига с символьным ключом. Алфавит A – латинские буквы и символ пробела.

4. Аффинный шифр для двоичных файлов. Алфавит A – кольцо вычетов по модулю 256.

5. Преобразование биграмм аффинным шифром для двоичных файлов. Алфавит A – кольцо вычетов по модулю $65536 = 256^2$.

6. Шифр Виженера с ключевым словом. Алфавит A – латинские буквы и символ пробела.

7. Шифр Виженера с числовым ключом для двоичных файлов. Алфавит A – кольцо вычетов по модулю 256.

8. Многопетлевые подстановки. Алфавит A – латинские буквы и символ пробела.

9. Многопетлевые подстановки для двоичных файлов. Алфавит A – кольцо вычетов по модулю 256.

10. Аффинный блочный шифр для 3-грамм для двоичных файлов, Алфавит A – кольцо вычетов по модулю 256.

11. Аффинный блочный шифр для 4-грамм для двоичных файлов. Алфавит A – кольцо вычетов по модулю 256.

12. Шифр Хилла для 3-грамм для двоичных файлов. Алфавит A – кольцо вычетов по модулю 256.

13. Шифр гаммирования с линейным конгруэнтным генератором ключей. Алфавит A – латинские буквы и символ пробела.

14. Шифр гаммирования с линейным конгруэнтным генератором ключей, Алфавит A – кольцо вычетов по модулю 256.

15. Шифр перестановки.

16. Шифр пропорциональной замены (шифр омофонов).

Методические указания

Теоретический материал для выполнения работы можно найти в учебном пособии [15].

Контрольные вопросы

1. Одноалфавитные шифры замены: шифр простой замены, шифр сдвига. Методы взлома данных шифров.
2. Одноалфавитные шифры замены: аффинный шифр, преобразование биграмм аффинным шифром. Методы взлома данных шифров.
3. Многоалфавитные шифры замены. Шифр Виженера. Криптоанализ шифра Виженера.
4. Многоалфавитные шифры замены: многопетлевые подстановки, аффинный блочный шифр, шифр Холла. Криптоанализ аффинного блочного шифра.
5. Многоалфавитные шифры замены. Шифр пропорциональной замены (шифр омофонов).

Лабораторная работа №2

МОДЕЛИРОВАНИЕ РАБОТЫ n-РАЗРЯДНОГО СКРЕМБЛЕРА

Цель работы: ознакомиться с методами генерации случайных чисел с использованием регистров сдвига с линейными обратными связями (LFSR) и шифром Вернама.

Задание

Написать программу, реализующую n-разрядный скремблер. Для этого:

1. Написать функцию генерации ключей шифра с помощью n-разрядного скремблера (значение n зависит от степени многочлена, указанного в индивидуальном варианте (см. табл. 1)).

2. Написать функцию, реализующую шифрование на заданном ключе двоичного файла с помощью шифра Вернама.

3. Написать функцию для реализации алгоритма расшифрования полученного шифрованного файла при известном ключе.

Варианты заданий

#	Скремблер	#	Скремблер
1.	$x^8+x^4+x^3+x^2+1$	2.	x^7+x+1
3.	$x^8+x^5+x^3+x^2+1$	4.	$x^7+x^5+x^2+1$
5.	x^9+x^4+1	6.	$x^{12}+x^6+x^4+x+1$
7.	x^9+x^3+1	8.	$x^{12}+1$
9.	$x^{10}+x^3+1$	10.	$x^8+x^4+x^3+x^2+1$
11.	$x^{10}+x^7+1$	12.	$x^8+x^6+x^2+1$
13.	x^5+x^2+1	14.	$x^{11}+x^2+1$
15.	x^5+x^4+x+1	16.	$x^{11}+x^3+x^2+1$
17.	$x^{11}+x^2+1$	18.	x^6+x+1
19.	$x^{11}+x^5+x^2+1$	20.	x^6+x^5+x+1

Таблица 1. Скремблер.

Методические указания

Простейшей и в то же время наиболее надежной из всех схем шифрования является так называемая *схема однократного гаммирования,* изобретение, которое чаще всего связывают с именем Вернама.

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

В данной лабораторной работе алфавитом A, в котором записываются открытые и шифрованные тексты, является кольцо вычетов по модулю два, т.е. открытые и шифрованные тексты рассматриваются как двоичные последовательности. В этом случае «наложение» гаммы – не что иное, как выполнение операции сложения $\oplus$ по модулю 2 (*XOR*), которая, например, в языке программирования С обозначается знаком ^.

Скремблером называется программная или аппаратная реализация алгоритма, позволяющего шифровать побитно непрерывные потоки информации.

Рассмотрим *сдвиговый регистр с линейными обратными связями* (Linear Feedback Shift Register, сокращенно LFSR) – логическое устройство, схема которого изображена на рис. 1.

Сдвиговый регистр представляет собой последовательность битов. Каждый бит нумеруется справа налево, начиная с нуля. В свою очередь, ячейки, содержащие биты сдвигового регистра, нумеруются слева направо, начиная с нуля.

Количество битов определяют *длину* сдвигового регистра. Если длина равна n битам, то регистр называется n-битовым сдвиговым регистром. Сдвиговый регистр осуществляет работу следующим образом. Вначале предварительно определяется новый крайний левый бит – он является функцией всех остальных битов регистра. После того, как новый крайний левый бит вычислен,

из ячейки $n-1$, являющейся одновременно и выходом сдвигового регистра, извлекается очередной сгенерированный бит, а все биты сдвигового регистра сдвигаются вправо на одну позицию. Наконец, после сдвига бит сдвигового регистра на одну позицию вправо, “пустующий” левый правый бит обретает свое новое предварительно вычисленное значение.

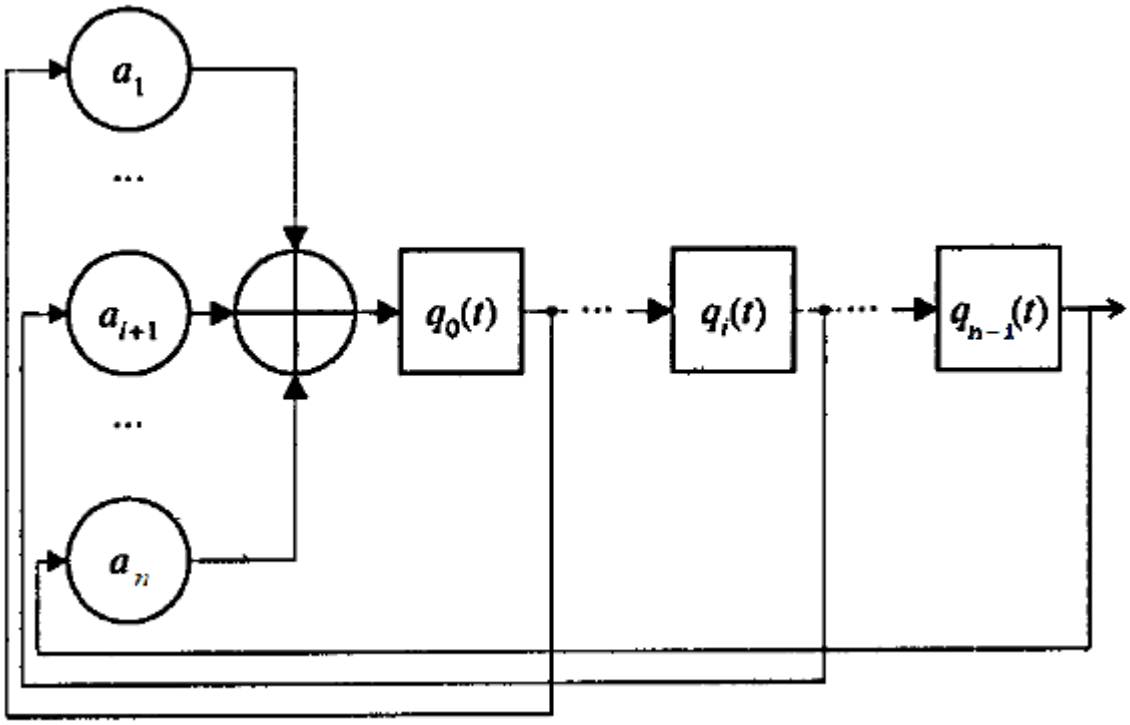

Рис. 1. Схема LFSR (в конфигурации Фибоначчи):

$q_i(t) \in \{0,1\}, i = 0,...,n-1$ – состояние i-й ячейки в момент времени t ($t = 0,1,2...$);

$a_i \in \{0,1\}, i = 1,...,n$ – коэффициенты, определяющие наличие или отсутствие обратных связей.

При достаточно долгой работе скремблера неизбежно возникает его зацикливание. По выполнении определенного числа тактов в ячейках скремблера создастся комбинация бит, которая в нем уже однажды оказывалась, и с этого момента кодирующая последовательность начнет циклически повторяться с фиксированным периодом. Данная проблема неустранима по своей природе, так как в n разрядах скремблера не может пребывать более 2^n комбинаций бит,

и, следовательно, максимум, через $2^n - 1$ циклов повтор комбинации обязательно произойдет. Последовательность бит, генерируемая таким скремблером, называется *последовательностью наибольшей длины* (ПНД).

Чтобы построить n-разрядный скремблер, создающий ПНД, пользуются примитивными многочленами.

Примитивный (базовый) многочлен степени n по модулю 2 – это неприводимый многочлен, который является делителем $x^{2^n-1}+1$, но не является делителем x^d+1 для всех d, являющихся делителями 2^n-1. *Неприводимый многочлен степени* n нельзя представить в виде произведения многочленов кроме него самого и единичного.

Приведем пример семиразрядного скремблера, генерирующего двоичную последовательность: $x^7 + x^3 + 1$. Начальное значение (начальный ключ) возьмем равным $(79)_{10} = (1001111)_2$. Для этого сдвигового регистра новый бит генерируется с помощью операции XOR нулевого и четвертого битов (см. рис. 2).

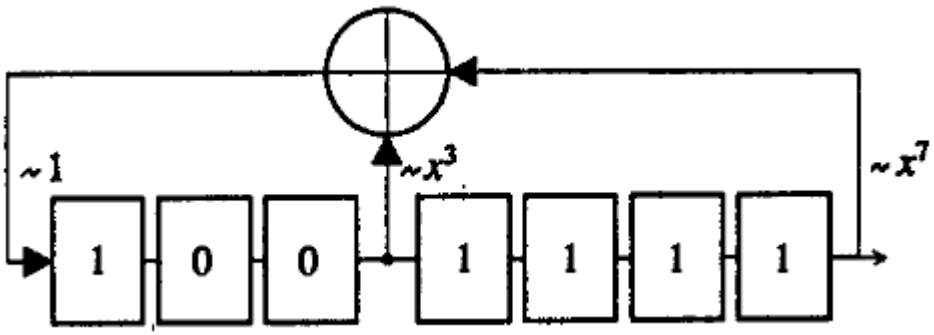

Рис. 2. Схема LFSR (в конфигурации Фибоначчи)
для многочлена $x^7 + x^3 + 1$, начальное состояние $(1001111)_2$.

Контрольные вопросы

1. Многоалфавитные шифры замены: табличное гаммирование,
2. Многоалфавитные шифры замены: модульное гаммирование.
3. Шифр Вернама.

Лабораторная работа №3

РОССИЙСКИЙ СТАНДАРТ СИММЕТРИЧНОГО ШИФРОВАНИЯ ГОСТ Р 34.12-2015

Цель работы: ознакомиться с шифрованием и расшифрованием информации при помощи алгоритма ГОСТ Р 34.12-2015.

Задание

Написать программу, которая шифрует/расшифровывает произвольный файл с помощью шифра ГОСТ Р 34.12-2015 в режиме, соответствующему индивидуальному варианту.

Варианты заданий

1. Реализовать шифр ГОСТ Р 34.12-2015 с длинами блоков 128 бит в режиме простой замены.
2. Реализовать шифр ГОСТ Р 34.12-2015 с длинами блоков 128 бит в режиме гаммирования.
3. Реализовать шифр ГОСТ Р 34.12-2015 с длинами блоков 128 бит в режиме гаммирования с обратной связью.
4. Реализовать шифр ГОСТ Р 34.12-2015 с длинами блоков 64 бит в режиме простой замены.
5. Реализовать шифр ГОСТ Р 34.12-2015 с длинами блоков 64 бит в режиме гаммирования.
6. Реализовать шифр ГОСТ Р 34.12-2015 с длинами блоков 64 бит в режиме гаммирования с обратной связью.

Методические указания

Теоретический материал для выполнения работы можно найти в учебном пособии [15].

Контрольные вопросы

1. Итеративные блочные шифры. Обратимость итеративного блочного шифра.
2. Шифры Фейстеля и их обратимость.
3. Построение цикловой функции. Входное и выходное отображения.
4. Слабые ключи итеративного блочного шифра.
5. Режимы использования симметричных блочных шифров.
6. Шифр ГОСТ Р 34.12-2015 с длинами блоков 128 бит.
7. Шифр ГОСТ Р 34.12-2015 с длинами блоков 64 бит.

Лабораторная работа №4

СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА

Цель работы: изучение (n,t)-пороговых схем разделения секрета.

Задание

Реализовать схему разделения секрета в соответствии с индивидуальным вариантом. Программа должна уметь, как разделять секрет s на n участников в соответствии с порогом t, так и восстанавливать его.

Варианты заданий

1. Схема разделения секрета Шамира.
2. Схема разделения секрета на основе равновесных двоичных кодов.
3. Схема разделения секрета на основе китайской теоремы об остатках.

Методические указания

Теоретический материал для выполнения работы можно найти в учебном пособии [16].

Контрольные вопросы

1. Понятие (n,t)-пороговой схемы разделения секрета. Пример (n,n)-пороговой схемы.
2. Схема разделения секрета на основе решения СЛАУ.
3. Схема разделения секрета Шамира.
4. Схемы разделения секрета на основе n-разрядных равновесных двоичных кодов.
5. Схема разделения секрета на основе китайской теоремы об остатках.

Лабораторная работа №5

ОБМЕН КЛЮЧАМИ ПО СХЕМЕ ДИФФИ-ХЕЛЛМАНА

Цель работы: освоить протокол обмена ключами по схеме Диффи-Хеллмана с использованием первообразных корней.

Задание

Реализовать программу, реализующую алгоритм обмена ключами по схеме Диффи-Хеллмана. Ключи должны автоматически формироваться в файлы.

Методические указания

Теоретический материал для выполнения работы можно найти в учебном пособии [16].

Контрольные вопросы

1. Алгоритм быстрого возведения в степень.
2. Задачи, приводящие к криптографии с открытым ключом и их решение.
3. Система Диффи-Хеллмана.

Лабораторная работа №6

АСИММЕТРИЧНЫЕ ШИФРЫ

Цель работы: освоить принципы работы ассиметричных алгоритмов шифрования, где существует два ключа – один для шифрования, другой для расшифрования.

Задание

Реализовать программу, работающую по алгоритму согласно индивидуальному варианту. Программа должна уметь работать с открытым текстом произвольной длины.

Варианты заданий

1. Шифр RSA.
2. Шифр Эль-Гамаля.
3. Шифр Шамира.

Методические указания

Теоретический материал для выполнения работы можно найти в учебном пособии [16].

Контрольные вопросы

1. Криптосистема без передачи ключа (шифр Шамира).
2. Шифр Эль-Гамаля.
3. Шифр RSA.
4. Рюкзачные криптосистемы.
5. Методы взлома шифров, основанных на дискретном логарифмировании: полный перебор, метод «Шаг младенца, шаг великана».
6. Методы взлома шифров, основанных на дискретном логарифмировании: метод исчисления порядка.

Лабораторная работа №7

ЭЛЕКТРОННАЯ ПОДПИСЬ

Цель работы: освоить принципы работы алгоритмов электронной подписи.

Задание

Реализовать программу, подписывающую сообщение с помощью алгоритма цифровой подписи согласно индивидуальному варианту. Программа должна уметь работать с сообщением произвольной длины. Также в программе должна осуществляться проверка электронной подписи.

Варианты заданий

1. Электронная подпись RSA.
2. Электронная подпись Эль-Гамаля.
3. Электронная подпись Фиата-Шамира.
4. Электронная подпись Шнорра.

Методические указания

Теоретический материал для выполнения работы можно найти в учебном пособии [16].

Контрольные вопросы

1. Хеш-функции. Оценка вероятности пропустить факт искажения сообщения x или его свертки $y = h(x)$.

2. Криптографические хеш-функции и их основные свойства. Оценка вероятности нахождения коллизии и вероятности нахождения второго прообраза.

3. Минимальное число элементов для нахождения коллизии с наперед заданной вероятностью. Парадокс дней рождений.

4. Построение хеш-функций.

5. Электронная подпись RSA.
6. Электронная подпись Фиата-Шамира.
7. Электронная подпись Эль-Гамаля.
8. Электронная подпись Шнорра.
9. Электронная подпись с доверенным посредником на основе симметричной криптосистемы.

ГЛАВА 3. ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лабораторная работа №1

АРИФМЕТИКА КОЛЕЦ ВЫЧЕТОВ И АЛГОРИТМ ЕВКЛИДА

Цель работы: повторить основные алгоритмы арифметики колец вычетов.

Задание

Разработать приложение, решающее поставленную задачу согласно индивидуальному варианту.

Варианты заданий

1. Дана последовательность целых чисел вида $[x \cdot n^2 + 3n]$, где x – параметр, задаваемый с клавиатуры. Проверить первые n чисел последовательности на взаимную и попарную простоту при помощи стандартного алгоритма Евклида.

2. Реализовать алгоритм решения диофантова уравнения вида $ax + by = c$ в целых числах при помощи расширенного алгоритма Евклида.

3. Реализовать вычисление функции Эйлера $\varphi(n)$ алгоритмом, использующим разложение n на простые множители. Для разложения числа n на простые множители использовать метод простого деления.

4. Реализовать вычисление функции Эйлера $\varphi(n)$ алгоритмом, использующим разложение n на простые множители. Для разложения числа n на простые множители использовать метод Монте-Карло.

5. Реализовать алгоритм разложения любого действительного числа в цепную дробь при помощи алгоритма Евклида.

6. Реализовать алгоритм вычисления символа Лежандра $\left(\frac{p}{q}\right)$.

7. Реализовать алгоритм решения системы сравнений по модулю первой степени вида $ax \equiv b \pmod{m}$.

8. Разработать приложение, реализующее алгоритм Монтгомери возведения в степень вида $a^m \pmod{n}$ для больших чисел a, n, m.

Методические указания

Теоретический материал для выполнения работы можно найти в учебном пособии [16] и в учебнике [11].

Контрольные вопросы

1. Аксиоматика Пеано.
2. Делимость, делитель, деление нацело, Н.О.Д., Н.О.К и их свойства.
3. Алгоритм Евклида. Свойства и модификации алгоритма Евклида.
4. Решение сравнений первой степени.
5. Решение систем сравнений первой степени.
6. Символы Лежандра и Якоби. Свойства символов Лежандра и Якоби.
7. Решение сравнений второй степени.
8. Цепные дроби. Свойства цепных дробей.
9. Алгоритм Монтгомери.

Лабораторная работа №2

ОБЩИЕ МЕТОДЫ ПРОВЕРКИ ПРОСТОТЫ ЧИСЕЛ

Цель работы: освоить основные методы проверки простоты целого числа.

Задание

Разработать приложение, осуществляющее согласно индивидуальному варианту:

– реализацию детерминированной проверки числа на простоту;

– реализацию вероятностной проверки числа на простоту.

После реализации приложения исследовать вероятностный тест проверки числа на простоту относительно числа ошибок, допускаемых им в зависимости от следующих факторов:

– вида числа;

– числа прогонов вероятностного теста.

Варианты заданий

Элементарные / детерминированные методы проверки чисел на простоту:

1. Метод пробных делений.
2. Решето Эратосфена.
3. Алгоритм Миллера.
4. Тест простоты Люка.

Вероятностные методы проверки чисел на простоту:

1. Тест Ферма.
2. Тест Соловея – Штрассена.
3. Тест Миллера – Рабина.

Методические указания

Теоретический материал для выполнения работы хорошо освещен в пособии [9], представляющем собой достаточно полный “путеводитель” по методам проверки простоты чисел, и учебниках [7] и [11]. Более подробное и основательное изложение теоретического материала можно найти в монографии [4].

Контрольные вопросы

1. Простейшие методы проверки чисел на простоту и их эффективность.
2. Различия между детерминированным и вероятностным методами проверки чисел на простоту: достоинства и недостатки каждого вида методов, эффективное применение на практике.
3. Алгоритм Миллера.
4. Тест простоты Люка.
5. Тест Ферма.
6. Числа Кармайкла и их критерий (критерий Корселта).
7. Тест Соловея – Штрассена.
8. Тест Миллера – Рабина.
9. Эйлеровы псевдопростые и сильно псевдопростые числа. Свойства данных чисел.

Лабораторная работа №3

МЕТОДЫ ФАКТОРИЗАЦИИ ЦЕЛЫХ ЧИСЕЛ

Цель работы: освоить основные методы факторизации целых чисел.

Задание

Разработать приложение, осуществляющее согласно индивидуальному варианту:

– реализацию методов факторизации целых чисел экспоненциальной сложности;

– реализацию метода факторизации целых чисел субэкспоненциальной сложности.

Варианты заданий

Методы факторизации целых чисел *экспоненциальной сложности:*

1. Метод пробных делений.
2. Метод Ферма.
3. $P-1$ метод Полларда.
4. $P+1$ метод Уильямса.
5. Ро-метод Полларда.
6. Метод Полларда – Штрассена.
7. Метод Шермана – Лемана.
8. Метод Шэнкса.

Методы факторизации целых чисел *субэкспоненциальной сложности*:

1. Алгоритм Диксона.
2. Алгоритм Бриллхарта – Моррисона.
3. Метод квадратичного решета Померанса.

Методические указания

Теоретический материал для выполнения работы можно найти в учебниках [7] и [11]. Более подробное и основательное изложение теоретического материала можно найти в монографии [4].

Контрольные вопросы

1. Простейшие методы факторизации целых чисел и их эффективность.
2. $P-1$ метод Полларда.
3. $P+1$ метод Уильямса.
4. Ро-метод Полларда.
5. Метод Полларда – Штрассена.
6. Метод Шермана – Лемана.
7. Метод Шэнкса.

Лабораторная работа №4

БЫСТРОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ

Цель работы: освоить быстрое и обратное преобразования Фурье.

Задание

Разработать приложение, осуществляющее согласно индивидуальному варианту:

– реализацию быстрого и обратного преобразований Фурье;

– реализацию решения дополнительной задачи на основе быстрого и обратного преобразований Фурье.

Варианты заданий

1. Быстрое умножение многочленов.
2. Заданы два массива a и b. Найти всевозможные числа вида $a[i]+b[j]$ и для каждого такого числа найти количество способов его получения.
3. Заданы два вектора a и b в виде массивов размера n. Найти значения каждого скалярного произведения вектора a на очередной циклический сдвиг вектора b.
4. Заданы два массива a и b со значениями 0 или 1. Найти все такие индексы для первого массива, что если «приложить» начиная с этого индекса второй массив, ни для одной последующей пары ячеек у обоих массивов не будет одновременно значения 1.

Методические указания

Теоретический материал для выполнения работы можно найти в учебнике [11]. Более подробное и основательное изложение теоретического материала можно найти в монографии [4].

Контрольные вопросы

1. Дискретное преобразование Фурье и его свойства.
2. Обратное преобразование Фурье.
3. Быстрое преобразование Фурье.
4. Умножение многочленов с использованием быстрого преобразования Фурье.

Лабораторная работа №5

МЕТОДЫ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

Цель работы: освоить основные методы дискретного логарифмирования.

Задание

Разработать приложение, осуществляющее согласно индивидуальному варианту:

– реализацию простейшего метода дискретного логарифмирования;

– реализацию метода дискретного логарифмирования экспоненциальной сложности;

– [*] реализацию метода дискретного логарифмирования субэкспоненциальной сложности.

Примечание:

[*] отмечена часть задания *повышенной сложности* – выполнение данной части задания не является строго обязательной и согласуется с преподавателем.

Варианты заданий

Простейшие методы дискретного логарифмирования в кольце вычетов по модулю простого числа.

1. Метод последовательного перебора.
2. Алгоритм согласования.

Методы дискретного логарифмирования в кольце вычетов по модулю простого числа *экспоненциальной сложности*.

1. Алгоритм Полига – Хеллмана.
2. Ро-метод Полларда.
3. Алгоритм Шэнкса.

[*] Методы дискретного логарифмирования в кольце вычетов по модулю простого числа *субэкспоненциальной сложности*.

1. Алгоритм Адлемана.
2. Алгоритм Копперсмита – Одлыжко – Шреппеля.

Методические указания

Теоретический материал для выполнения работы можно найти в учебниках [7] и [11]. Более подробное и основательное изложение теоретического материала можно найти в монографии [4].

Контрольные вопросы

1. Простейшие методы дискретного логарифмирования по модулю простого числа.
2. Алгоритм Полига – Хеллмана.
3. Ро-метод Полларда.
4. Алгоритм Шэнкса.

ГЛАВА 4. ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ

Лабораторная работа №1

КОНГРУЭНТНЫЕ ГПСЧ

Цель работы: изучить основные виды конгруэнтных генераторов псевдослучайных чисел (ГПСЧ).

Задание

Разработать приложение, осуществляющее согласно индивидуальному варианту реализацию указанных конгруэнтных генераторов псевдослучайных чисел.

Параметры для генератора необходимо выбрать самостоятельно из соображений достижения максимального периода для генерируемой последовательности чисел и согласовать с преподавателем.

Варианты заданий

Исследуемые *конгруэнтные* генераторы псевдослучайных чисел:

1. Линейный конгруэнтный генератор псевдослучайных чисел.
2. Полиномиальный генератор псевдослучайных чисел.
3. Аддитивный генератор Фибоначчи.
4. Мультипликативный генератор Фибоначчи.
5. Инверсивный конгруэнтный генератор.
6. Регулярный рандомизационный конгруэнтный генератор.

Методические указания

Теоретический материал для выполнения работы можно найти в монографии [10] и учебнике [8].

Контрольные вопросы

1. Линейная конгруэнтная последовательность.
2. Выбор модуля для линейной конгруэнтной последовательности.
3. Выбор множителя для линейной конгруэнтной последовательности.
4. Критерий максимального периода для линейной конгруэнтной последовательности.
5. Потенциал.
6. Достоинства и недостатки линейного конгруэнтного генератора.
7. Полиномиальный конгруэнтный генератор.
8. Аддитивный генератор Фибоначчи.
9. Мультипликативный генератор Фибоначчи.
10. Инверсивный конгруэнтный генератор.
11. Рандомизация перемешиванием.

Лабораторная работа №2

ГПСП НА РЕГИСТРАХ СДВИГА С ЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ

Цель работы: изучить основные виды генераторов псевдослучайных последовательностей (ГПСП) на регистрах сдвига с линейными обратными связями.

Задание

Разработать приложение, осуществляющее согласно индивидуальному варианту реализацию указанных генераторов псевдослучайных последовательностей бит на регистрах сдвига с линейными обратными связями.

Параметры для генератора необходимо выбрать самостоятельно из соображений достижения максимального периода для генерируемой последовательности бит и согласовать с преподавателем.

Варианты заданий

Исследуемые генераторы псевдослучайных последовательностей бит на *регистрах сдвига с линейными обратными связями*:

1. Генератор Фибоначчи.
2. Генератор Галуа.
3. Каскадный генератор Голлманна.
4. Генератор Геффа.
5. Самопрореживающий генератор Чамберса.
6. Сжимающий генератор.

Методические указания

Общие принципы работы регистра сдвига с линейными обратными связями описаны в методических указаниях к лабораторной работе №2 главы 2 данного пособия.

Более детальное описание принципов работы генераторов псевдослучайных последовательностей на регистрах сдвига с линейными обратными связями можно найти в книге [8].

Контрольные вопросы

1. Генератор Фибоначчи.
2. Генератор Галуа.
3. Каскадный генератор Голлманна.
4. Генератор Геффа.
5. Самопрореживающий генератор Чамберса.
6. Сжимающий генератор.
7. Достоинства и недостатки генераторов псевдослучайных последовательностей на регистрах сдвига с линейными обратными связями.

Лабораторная работа №3

КРИПТОГРАФИЧЕСКИЕ ГПСП

Цель работы: изучить основные виды криптографических генераторов псевдослучайных последовательностей.

Задание

Разработать приложение, осуществляющее согласно индивидуальному варианту реализацию указанных криптографических генераторов псевдослучайных последовательностей бит.

Варианты заданий

Исследуемые генераторы псевдослучайных последовательностей бит *с использованием функций блочных и поточных шифров*:

1. Генератор на основе ГОСТ 28147-89 в режиме Counter.
2. Генератор на основе AES-128.
3. Генератор RC4 в режиме OFB.

Используемые ГПСЧ на *односторонней функции*:

1. Генератор BBS.
2. Генератор RSA.

Методические указания

Теоретический материал для выполнения работы может быть найден в книге [8].

Контрольные вопросы

1. Генератор на основе ГОСТ 28147-89 в режиме Counter.
2. Генератор на основе AES-128.
3. Генератор RC4 в режиме OFB.
4. Генератор BBS.

5. Генератор RSA.

6. Достоинства и недостатки криптографических генераторов псевдослучайных последовательностей.

Лабораторная работа №4

ГРАФИЧЕСКИЕ ТЕСТЫ КАЧЕСТВА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Цель работы: изучить основные графические тесты качества псевдослучайных последовательностей.

Задание

Разработать приложение, осуществляющее согласно индивидуальному варианту реализацию указанных графических тестов качества псевдослучайных последовательностей.

После реализации графических тестов качества псевдослучайных последовательностей, необходимо произвести тестирование псевдослучайных последовательностей, получаемых при помощи генераторов из лабораторных работ №1 – №3, и сделать соответствующие выводы о качестве данных генераторов.

Варианты заданий

Исследуемые *графические* тесты качества псевдослучайных последовательностей:

1. Гистограмма распределения элементов псевдослучайной последовательности (ПСП).
2. Распределение элементов псевдослучайных последовательностей на плоскости.
3. Проверка серий псевдослучайной последовательности.
4. Проверка псевдослучайной последовательности на монотонность.
5. Метод автокорреляционных функций.
6. Проверка линейной сложности псевдослучайной последовательности.
7. Графический спектральный тест псевдослучайной последовательности.

Методические указания

Теоретический материал для выполнения работы может быть найден в книге [8].

Контрольные вопросы

1. Графический тест ПСП при помощи гистограммы распределения элементов ПСП.
2. Графический тест ПСП анализом распределения элементов ПСП на плоскости.
3. Графический тест ПСП при помощи проверки серий ПСП.
4. Графический тест ПСП проверкой ПСП на монотонность.
5. Графический тест ПСП методом автокорреляционных функций.
6. Графический тест ПСП проверкой линейной сложности ПСП.
7. Графический спектральный тест ПСП.

Лабораторная работа №5

СТАТИСТИЧЕСКИЕ ТЕСТЫ КАЧЕСТВА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Цель работы: изучить основные статистические тесты качества псевдослучайных последовательностей.

Задание

Разработать приложение, осуществляющее согласно индивидуальному варианту реализацию указанных статистических тестов качества псевдослучайных последовательностей.

После реализации статистических тестов качества псевдослучайных последовательностей, необходимо произвести тестирование псевдослучайных последовательностей, получаемых при помощи генераторов из лабораторных работ №1 – №3, и сделать соответствующие выводы о качестве данных генераторов.

Варианты заданий

Исследуемые статистические тесты качества псевдослучайных последовательностей *Д. Кнута*:

1. Тест несцепленных серий.
2. Проверка интервалов.
3. Проверкой комбинаций.
4. Тест собирателя купонов.
5. Проверка перестановок.
6. Проверка на монотонность.
7. Проверка корреляции.

Используемые статистические тесты качества псевдослучайных чисел *НИСТ (NIST)*:

1. Частотный (монобитный) тест.
2. Частотный тест в подпоследовательностях ПСП.
3. Тест “дырок”.
4. Тест “блоков” в подпоследовательностях ПСП.
5. Проверка рангов матриц.
6. Спектральный тест.
7. Проверка непересекающихся шаблонов.
8. Проверка пересекающихся шаблонов.
9. Универсальный тест Маурера.
10. Проверка сжатия при помощи алгоритма Лемпела – Зива.
11. Проверка линейной сложности.
12. Проверка серий.
13. Проверка аппроксимированной энтропии.
14. Проверка кумулятивных сумм.
15. Проверка случайности отклонений №1.
16. Проверка случайности отклонений №2.

Методические указания

Теоретический материал для выполнения работы может быть найден в книге [8] и частично – в монографии [10].

Контрольные вопросы

1. Критерий χ^2.
2. Статистические тесты Д.Кнута.
3. Достоинства и недостатки каждого из тестов Д.Кнута.
4. Статистические тесты НИСТ.
5. Выбор параметров и интерпретация результатов тестов НИСТ.
6. Достоинства и недостатки каждого из тестов НИСТ.

ГЛАВА 5. СИСТЕМНЫЙ АНАЛИЗ

Лабораторная работа №1

ПРИМЕНЕНИЕ МЕТОДОЛОГИИ СИСТЕМНОГО ПОДХОДА ДЛЯ ИССЛЕДОВАНИЯ ВЫБРАННОГО ОБЪЕКТА

Цель работы:

– Научиться применять методологию системного подхода для исследования выбранного объекта (системы) (в соответствии с вариантом).

– Приобрести навыки исследования в соответствии с этапами методологии системного подхода.

Задание

Произвести исследование выбранного объекта согласно индивидуальному варианту, используя методологию системного подхода, а именно:

1. *Сформулировать четкие цели исследуемого объекта (системы).* Цели исследования определяют границы выделения системы из внешней среды. Изменение целей приводит к изменению системы. При одной и той же цели, у различных исследователей, как правило, получаются различные системы.

2. *Дать точное и полное определение предназначения системы (цели функционирования системы).* Это один из основных моментов системного исследования. На этом этапе определяется общая (глобальная) цель системы и частные цели системы (глобальную цель берут из суперсистемы). Далее определяется возможность реализации (осуществимости) этих целей и ресурсов, необходимых для этого. Каждая подсистема системы может иметь свою частную цель, которые не всегда совпадают с общей целью. Между частными целями в системе существует взаимосвязь и состязательность. Всю совокупность целей, стоящих перед системой, представляет в виде дерева целей. Корень дерева – глобальная цель, далее – частные. Цели верхнего уровня формируются на качественном уровне, далее – конкретика.

3. *Осуществить выделение системы и изучить ее структуру.* На этом этапе осуществляется определение состава системы, состава элементов среды, определение и характеристика внутренних и внешних связей. Внутренние связи более сильные по отношению к внешним связям. Процесс выделения элементов системы и связей между ними называется структуризацией. На выходе этапа – структура. При изучении структуры исследуются связи, типы структур и класс сложности системы в целом. Процесс структуризации носит итеративный характер.

4. *Осуществить последовательное раскрытие механизма функционирования системы.* На этом этапе определяются функции, которые реализует система и алгоритм функционирования системы в целом, и алгоритмы функционирования входящих в нее подсистем. На этом же этапе определяется важность исследуемой системы, ее место в суперсистеме и взаимодействие с другими системами.

5. *Рассмотреть систему на всех этапах жизненного цикла (исторический анализ объекта).* Осуществляется анализ возникновения системы, ее развитие и прогноз на будущее.

6. *Сравнение исследуемой системы с другими, близкими по целям.* Системный подход (СП) обязывает исследователя двигаться от целого к частям, а затем снова к целому. В этом отличие СП от обычного аналитического подхода.

Варианты заданий

1. Межсетевой экран.
2. Система защиты информации от несанкционированного доступа.
3. Система защиты от компьютерных вирусов.
4. Система видеонаблюдения.
5. Система противопожарной сигнализации.
6. Система обнаружения вторжений (IDS).
7. Система предотвращения вторжений (IPS).

8. Система криптографической защиты.

9. Система физической защиты.

10. Система защиты от побочных электромагнитных излучений и наводок (ПЭМИН).

11. Система идентификации и аутентификации пользователей информационной системы.

12. Система электропитания объекта.

13. Компьютер.

14. Телевизор.

15. Система жизнеобеспечения объекта информатизации.

16. Система передачи данных.

17. Система защиты сайтов.

Методические указания

Для выполнения лабораторной работы необходимо использовать методологию системного анализа. Теоретический материал для выполнения работы можно найти в учебном пособии [2].

Контрольные вопросы

1. Дать определение системного подхода.
2. Объяснить, в чем заключается сущность системного подхода (системной концепции).
3. Дать характеристику основных этапов системных исследований.
4. Пояснить предназначение основных принципов системного подхода.
5. Перечислить основные свойства систем.

Лабораторная работа №2

ПРИМЕНЕНИЕ МЕТОДОЛОГИИ РЕШЕНИЯ ПРОБЛЕМ ДЛЯ ВЫБРАННОГО ОБЪЕКТА (СИСТЕМЫ)

Цель работы:

– Научиться применять методологию решения проблем.

– Приобрести навыки использования методологии решения проблем для конкретных объектов (систем).

Задание

Произвести выявление и анализ проблем для выбранного объекта согласно индивидуальному варианту, используя методологию решения проблем, а именно:

1. *Уточнить качество результатов общего анализа системы, полученных в лабораторной работе №1.* Уяснить, что лабораторная работа № 1 – это лишь первый этап методологии решения проблем, который является основой для дальнейшего исследования. В результате выполнения этого этапа Вы получили представление о системе (*концептуальная модель существующей системы* (сжатое представление о системе)).

2. *Определение проблемы.*

- *Определить состав показателей качества системы:*

– построение дерева существенных свойств системы (необходимо определить существенные свойства Вашей системы). Например, для антивирусной системы (вариант задания №3) к существенным свойствам следует отнести: быстродействие сканирования, удобство работы и др.;

– формирование показателей качества системы (например, для свойства “быстродействие сканирования” – показателем будет количество файлов (байтов), проверяемых в единицу времени).

- *Определить требования к системе.*

– определение требуемых значений показателя качества системы (если есть требования, то хорошо, если нет – то необходимо их обосновать). Например, для систем пожарной сигнализации (вариант задания №5) есть специальные ГОСТ–ы, где имеются требования;

– выбор (разработка) методик определения требований к системе (если их нет).

- *Оценить качество существующей системы.*

– выбирается простая модель, по которой производится оценка качества;

– выбор или разработка методик оценки качества существующей системы на простой модели.

Например, имеются две ЭВМ, между которыми существует канал связи (КС). Скорость передачи данных по КС составляет 100 символов в секунду. Необходимо определить время решения задачи (исходные данные передаются из ЭВМ-1 в ЭВМ-2). Затем результат возвращается в ЭВМ-1. Тогда время решения задачи $T_з = T_{ЭВМ1} + T_{ЭВМ2} + 2 \cdot T_{КС}$. *Задача должна решаться за* $T \le 2$ *мин. – требование.*

10 000 символов нужно передать по каналу связи. В существующей системе задача будет решаться 1 мин. 40 сек. Следовательно, проблема существует, так как требование ($T \le 2$ *мин.*) *не выполняется.*

- *Определить несоответствия существующей системы требованиям и вскрыть причины его возникновения:*

– сравнение требуемых и фактических значений показателей качества;

– вскрытие основных симптомов несоответствия и причин их возникновения.

Если в примере предыдущего подпункта сократить время передачи информации по КС, то мы решим проблему. Итак, КС – узкое место.

- *Сформулировать проблему.*

– вскрытие несоответствия;

– описание важности и актуальности проблемы.

- *Выявить связь проблемы с другими (аналогичными) проблемами.*
- *Осуществить прогнозирование развития проблемы.*

3. Определение путей, направлений и этапов решения проблемы.

- *Произвести структуризацию проблемы:*

– выделение подпроблем;

– установление связей между подпроблемами;

– определение значимости выделенных подпроблем.

- *Выявить «узкие места» в системы.*

– установление зависимостей между характеристиками и показателями качества системы;

– определение степени влияния характеристик системы на показатели качества;

– нахождение подсистем (элементов), являющихся «узкими местами» в системе.

- *Исследовать альтернативных путей решения проблемы.* (на данном этапе необходимо определиться: либо совершенствовать старую систему, либо создавать новую).

– оценка эффективности совершенствования системы (сколько стоит, сколько времени понадобится и др.);

– оценка эффективности создания новой системы (сколько стоит, сколько времени понадобится и др.);

– выбор окончательного пути решения проблемы.

Для примера, рассмотренного в третьем подпункте пункта 2 задания, альтернативными могут быть следующие пути:

– сокращение времени передачи информации по КС (другая АПД, новый вид связи, дополнительные КС и др.);

– увеличение быстродействия ЭВМ;

– уменьшение объема передаваемой информации (сжатие данных).

- *Определить направления совершенствования системы:*

– определение направлений совершенствования системы в целом;

– определение направлений совершенствования подсистем или видов обеспечения;

– формирование вариантов новой системы (концептуальной и формальной моделей будущей системы);

– сравнение и выбор наиболее предпочтительного варианта (с помощью показателей качества).

- *Выделить этапы решения проблемы:*

– определение числа и содержания этапов решения проблемы;

– определение продолжительности этапов решения проблемы.

Варианты заданий

1. Межсетевой экран.
2. Система защиты информации от несанкционированного доступа.
3. Система защиты от компьютерных вирусов.
4. Система видеонаблюдения.

5. Система противопожарной сигнализации.
6. Система обнаружения вторжений (IDS).
7. Система предотвращения вторжений (IPS).
8. Система криптографической защиты.
9. Система физической защиты.
10. Система защиты от побочных электромагнитных излучений и наводок (ПЭМИН).
11. Система идентификации и аутентификации пользователей информационной системы.
12. Система электропитания объекта.
13. Компьютер.
14. Телевизор.
15. Система жизнеобеспечения объекта информатизации.
16. Система передачи данных.
17. Система защиты сайтов.

Методические указания

Для выполнения лабораторной работы необходимо использовать методологию решения проблем. Теоретический материал для выполнения работы можно найти в учебном пособии [2].

Контрольные вопросы

1. Дать определение проблемы.
2. Классификация проблем. Дать характеристику слабоструктурированных проблем.
3. Объяснить, в чем заключается концепция решения проблем.
4. Объяснить, что такое методология решения сложных проблем.
5. Перечислить основные пути решения проблем.

Лабораторная работа №3

ПРИМЕНЕНИЕ ТЕОРИИ ГРАФОВ ДЛЯ МОДЕЛИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Цель работы: овладение навыками создания математических моделей для решения профессиональных задач в области защиты информации.

Задание

Имеется ориентированный граф, узлами которого являются состояния объекта защиты, а дугами – переходы из одних состояний объекта защиты в другие. Граф представлен матрицей смежности (см. таблицу №2), а всякой дуге, исходящей из любого узла, приписаны:

– Вероятности реализации угрозы объекту защиты при переходе в смежный узел ($P_{угр}$).

– Цена средств защиты (в условных единицах), нейтрализующих угрозу перехода между смежными узлами ($Ц_{сз}$).

– Время перехода состояния объекта защиты (в минутах) между смежными узлами (t_{ij}).

0	0.7; 15; 08	0.8; 25; 15	0.6; 16; 12	0.5; 32; 06	0.1; 05; 04
0.7; 12; 08	0	0.2; 02; 10	0.6; 30; 02	0.7; 12; 11	0.4; 08; 14
0.8; 40; 15	0.2; 15; 10	0	0.9; 35; 04	0.8; 60; 15	0.6; 40; 02
0.6; 15; 12	0.6; 25; 02	0.9; 58; 04	0	0.8; 45; 11	0.4; 60; 04
0.5; 15; 06	0.7; 25; 11	0.8; 45; 15	0.8; 90; 11	0	0.2; 15; 16
0.1; 05; 04	0.8; 60; 14	0.6; 55; 02	0.4; 12; 04	0.2; 10; 16	0

Таблица 2. Матрица смежности: элемент матрицы $a_{ij} = \left(P_{угр}; Ц_{сз}; t_{ij}\right)$.

Необходимо произвести анализ объекта защиты, а именно:

1. В соответствии с заданными исходными данными привести 3-4 примера моделей систем защиты информации с использованием теории графов.

2. Определить (расположив по возрастанию) все реализуемые пути между указанными узлами согласно индивидуальному варианту (см. таблицу №3) с точки зрения вероятности реализации угроз для объекта защиты. По результатам моделирования сформулировать выводы.

3. Определить минимальную и максимальную стоимости средств защиты при реализации указанной траектории пути согласно индивидуальному варианту (см. таблицу №3). По результатам моделирования сформулировать выводы.

4. Определить минимальное и максимальное время перехода состояния объекта защиты между указанными узлами согласно индивидуальному варианту (см. таблицу №3). По результатам моделирования сформулировать выводы.

Варианты заданий

№	Узлы	№	Узлы
1.	1,2	2.	3,5
3.	1,3	4.	3,6
5.	1,4	6.	4,5
7.	1,5	8.	5,2
9.	2,4	10.	4,1
11.	2,5	12.	2,1

Таблица 3. Узлы в исследуемом графе.

Методические указания

Для выполнения лабораторной работы необходимо использовать основные понятия и алгоритмы теории графов. Теоретический материал для выполнения лабораторной работы можно найти в учебнике [13].

Контрольные вопросы

1. Перечислить математические методы, используемые для моделирования систем защиты.
2. Пояснить, что такое адекватность математических моделей.
3. Перечислить и объяснить основные виды представления графов.
4. Объяснить алгоритм поиска кратчайших путей в графе.
5. Объяснить метод прямого построения кратчайших остовых деревьев.

ЛИТЕРАТУРА

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2005.

2. Анфилатов В.С., Емельянов А.А., Кукушкин А.А. Системный анализ в управлении: Учебное пособие. – М.: Финансы и статистика, 2002.

3. Бухштаб А.А. Теория чисел. – СПб.: Издательство «Лань», 2008.

4. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003

5. Виноградов И.М. Основы теории чисел. – СПб.: Издательство «Лань», 2006.

6. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра: в 2 т.– М.: Гелиос-АРВ, 2003.

7. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. – СПб.: Издательство «Лань», 2011.

8. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003.

9. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие. – Казань: Казан. ун., 2011.

10. Кнут Д.Э. Искусство программирования, том 2. Получисленные алгоритмы, 3-е изд. – М.: Издательский дом «Вильямс», 2003.

11. Маховенко Е.Б. Теоретико-числовые методы в криптографии. Учеб. пособие для вузов. – М.: Гелиос АРВ, 2006.

12. Нестеренко Ю.В. Теория чисел: Учеб. для студ. высш. учеб. заведений. – М.: Издательский центр «Академия», 2008.

13. Новиков Ф.А. Дискретная математика для программистов: Учеб. пособие для вузов.– СПб.: Питер, 2009.

14. Рацеев С.М. Программирование на языке Си. – Ульяновск: УлГУ, 2015.

15. Рацеев С.М. Элементы криптографии. Часть 1. – Ульяновск: УлГУ, 2012.

16. Рацеев С.М. Элементы криптографии. Часть 2. – Ульяновск: УлГУ, 2013.

17. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. – М.: Горячая линия – Телеком, 2005.

18. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии. – М.: Горячая линия – Телеком, 2010.

19. Фомичев В.М. Методы дискретной математики в криптологии. – М.: Диалог-МИФИ, 2010.

20. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009.

21. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002.