МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

КАФЕДРА «ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

Традиционные и интеллектуальные информационные технологии

Методические указания к выполнению практических занятий и лабораторных работ для студентов специальности 1-40 03 01 «Искусственный интеллект»

Брест 2014

УДК 347 77/681ю3
ББК 67.404.3я 73/32.97

Методические указания содержат сведения, необходимые для освоения элементов методов информационных интеллектуальных технологий, которые используются в различных автоматизированных системах (проектирования, прогнозирования, безбумажного документирования, выполнения сетевых коммерческих операций и многих других). Особое внимание уделяется выработке практических навыков в использовании средств описания алгоритмов принятия решений и защите баз данных и знаний. В частности, с помощью средств современных интеллектуальных технологий описываются алгоритмы, процедуры защиты информации, сохранения коммерческой тайны, анализа результатов, моделирования и др.

Издание адресовано студентам, магистрантам, преподавателям и другим специалистам, использующим и разрабатывающим современные сетевые интеллектуальные компьютерные информационные технологии.

Составители: Л.П. Матюшков, к.т.н., доцент
В.А. Головко, д.т.н., профессор

Введение

Сетевые интеллектуальные компьютерные технологии все шире начинают использоваться в построении информационного общества: автоматизация проектирования, безбумажный документооборот, развитие электронных коммерческих операций, создание электронного правительства, борьба с контрафактной продукцией, системы электронного голосования, прогнозирование нейросетевыми методами и т.д.

Проблема доверия к результатам работы различных автоматизированных систем и средств связи становится одной из ключевых: ответственность за принятие решений с помощью интеллектуальных информационных систем, гарантия юридической силы сделок в виде электронных документов и т.п. Кроме того, работа различных систем становится ущербной, если они опираются лишь на процедуру идентификации взаимодействующих сторон, так как практика борьбы со злоумышленниками в различных компьютерных сетях и злоупотреблениями в различных операциях через банки и особенно при использовании банкоматов и мобильных телефонов показали необходимость не только идентификации пользователей (пароль, PIN-код и т.п.), но и их авторизацию.

Поэтому владение современными элементами защиты оказалось для специалистов по автоматизированной обработке информации важным с двух точек зрения: изучение принципов современной защиты передаваемой и хранимой информации в сетях на основе сертифицированных систем (ИСО СТБ) и получения навыков работы и применения отдельных элементов защиты, как в своей практической работе, так и пропаганде широкого применения защищенных тей среди пользователей для пояснения принципов, которые обеспечивают раскрываемость и целостность информации благодаря шифрованию и электронной цифровой подписи при использовании сертифицированных систем.

Поэтому содержание заданий практических занятий и лабораторных работ ориентировано на усвоение теоретических основ алгоритмизации управления на основе типовых задач дискретной математики и защиты информации в прикладной деятельности на предприятиях при создании важных документов для охраны интеллектуальной собственности в виде проектной документации и ведения систем безбумажного документооборота.

Учебное пособие построено с ориентацией на активную самостоятельную работу студентов за счет индивидуализации заданий и их ориентации на конкретные предприятия, где студент работает (заочник) или проходит различные виды практик, а иногда и работает по договору со свободным режимом посещения (очник).

Для выполнения заданий приводятся необходимые минимальные теоретические сведения и схемы их выполнения. Творческая часть состоит в создании цепочки конкретных вычислительных моделей на основе средств высокоинтеллектуальной системы Mathcad и формулировании выводов по результатам вычислительного эксперимента. Эта система позволяет быстро и эффективно реализовывать различные модели с участием экспериментатора.

1. Общие указания к выполнению заданий

Все задания можно условно разбить на три категории: освоение общего математического аппарата и программных систем, используемых в разработке информационных компьютерных технологий; получение навыков по применению базовых элементов математического и программного аппарата при моделировании простейших объектов; освоение методов защиты информации и их использования в создании документов и баз данных с электронной цифровой подписью. Особо следует выделить операции по обеспечению надежности коммерческих операций в сетях и идентификации(аутентификации) пользователей. Ключевыми элементами являются вопросы описания и реализации процессов. Система Mathcad (и её аналоги) хорошо подходит для первичного освоения навыков моделирования объектов и процессов, так как способствуют лучшему пониманию организации хода моделирования без его реализации в виде полной программы. Однако наличие развитой системы процедур позволяет реализовывать моделирование в смешанном человеко-машинном варианте, когда исследователь управляет процессом переходов между процедурами, описанными средствами Mathcad. По всем заданиям необходимо сделать краткое описание этого процесса и выводы о наблюдаемых его особенностях (регулирование количества итераций и точности, поведении заданной функции, причины остановки процесса или отсутствия решения).

Кратко охарактеризуем особенности ключевых элементов математического аппарата криптографии. В первую очередь – это аппарат, развиваемый в теории чисел, теории вероятностей и математической статистики.

Во многих операциях используется теория сравнений ($x=a \bmod p$), где a и p целые положительные числа, p – простое число, x при делении на p дает остаток a. На основе этого элемента легко показать реализацию односторонних функций, когда y=(остаток) легко вычисляется при знании конкретного x, но обратная задача по y (остатку) вычислить x является многозначной и только знание дополнительной секретной информации позволяет однозначно найти x. В том и другом случае решение прямой и обратной задач требует времени t как функции от некоторого полинома.

Вторым важным механизмом являются процедуры, основанные на применении подстановок и перестановок, чтобы менять исходный текст с использованием случайных чисел так, чтобы создать максимальные трудности криптоаналитику (злоумышленнику) при расшифровке закодированных сообщений.

В создании практических механизмов схем цифровой подписи и оплаты коммерческих сделок, а также банковских операций играют криптографические протоколы. Они применяются при обмене шифрованными сообщениями удаленных абонентов по открытым каналам связи. Часто бывает, что информация не является секретной, а для принимающей стороны (например, банка) важно убедиться, что информация действительно от его клиента, а клиенту важно убедиться, чтобы никто не изменил сумму в платежном поручении или кто-то послал поддельное поручение. Задача конфиденциальности информации решается ее шифрованием, а ее целостность и аутентификация участников при обмене сообщениями обеспечивается протоколами (совокупностью алгоритмов, которые скрупулезно должны выполнять участники обмена информацией).

Особую роль в протоколе для идентификации подписавшего сообщение лица играют хэш-функции для преобразования сообщений произвольной длины в более краткие хэш-значения требуемой длины.

Для создания дополнительных трудностей в расшифровке сообщений и аутентификации их авторов широко используются и генераторы случайных чисел, например, при наложении гаммы(случайных битов).

Варианты всех заданий подбираются в зависимости от индивидуальных характеристик студентов: Ф-количество букв в фамилии, И-в имени, О-в отчестве, №-численное значение номера в группе(подгруппе).

2. Задания для практических занятий 1-5

1. Составление численных и логических алгоритмов с демонстрацией их основных свойств.

2. Выбор машинно-ориентированных численных методов решения задач. Связность и восстанавливаемость алгоритмов

3. Разработка программы сложения двух чисел на машине Поста.

4. Задание с помощью конечного автомата движения робота по контуру.

5. Построение механизма поиска информации на основе формального языка.

6-8. Построение логистического алгоритма доставки груза на основе решения задачи коммивояжера методом ветвей и границ для трёх модификаций алгоритма с целью получения навыков адаптации теоретической модели к решению прикладной задачи.

Выполнение заданий №№1-8 предполагает обязательное описание студентом алгоритма любым известным ему методом (например, из[1]). Теоретическая основа для выполнения задаий №№1-5 известна из лекционного курса и достаточно полно описана в [1,2]. Поэтому для этих заданий подчеркнём лишь ключевые моменты, которые желательно выделить при оформлении результата:

– №1 главное отличие численных и логических алгоритмов, обеспечение конечности, однозначности и результативности процесса вычислений;

– №2 Особенности ЭВМ как вычислительного инструмента (учёт погрешностей из-за ограниченной разрядной сетки и перехода к двоичной форме представления чисел, необходимость экономии памяти при экспоненциальном росте промежуточных результатов, желательность автоматизации ввода больших массивов информации, возможность сбоев в работе, необходимость предусматривать эффективные пути восстановления в случае чрезвычайных ситуаций и т.д.).

–№3 В этой задаче в отчёте надо отметить сходство в программировании и реализации программ на абстрактной машине Поста и реальной ЭВМ.

–№4 Отметить особенности использования конечного автомата как универсального устройства для управления заданным классом процессов (движение по выбранному типу контуров) на базе описания переходов состояний автомата в виде своеобразной программы.

–№5 Необходимо отразить взаимозависимость построения структуры базы данных и механизма запросов на эффективность результата поиска.

В нашем случае $(X_0; Y_0)$=(0; 4) и $(X_1; Y_1)$ = (1; 3). Если робот, сориентированный в направлении *OX*, находится в состоянии покоя (C_1) в точке (0; 4) и готов к движению по прямой от точки (0; 4) к точке (1; 4), то нижеследующая программа обеспечит *выполнение* задачи (для наглядности будем писать в скобках соответствующие символы состояния, на которое шло входное воздействие символов P_i в виде цепочки смены состояний):

$P_3\ P_2\ P_3\ P_3\ P_4\ P_2\ P_3\ P_1\ P_3\ P_3\ P_3\ P_3\ P_1\ P_3\ P_3\ P_1,\ P_1,\ P_2\ (C_1\ C_4\ C_2\ C_3\ C_2\ C_5\ C_2\ C_3\ C_3\ C_2\ C_3\ C_3\ C_2\ C_3\ C_2\ C_2\ C_3\ C_2\ C_2\ C_2\ C_1)$

Чтение записи происходит на базе таблицы автомата *A* и рисунка контура. В таблице мы находим, что при входном воздействии P_3 на состояние C_1 автомат переходит в состояние C_4 (захват детали), затем по воздействию P_2 на C_4 он начинает движение на один шаг по контуру (состояние C_2) и приходит в точку (1; 4), по воздействию P_3 на C_4 обеспечивается переход в состояние C_3 (поворот на 90° по часовой стрелке), что соответствует ориентации робота для движения вниз по прямой и т.д. В итоге подачи всех сигналов входной последовательности робот, двигаясь по контуру, снова возвратится в точку (0; 4). Его состояние покоя C_1 во второй последовательности выделено особо (последнему символу C_1 нет никакого входного символа *P*). Это объясняется тем, что после подачи последнего входного сигнала робот будет находиться в состоянии покоя.

Естественно, что можно начать обход контура и в другую сторону (сначала идти по оси *Y*), но тогда изменится лишь цепочка входных воздействий. Можно пойти еще дальше и убедиться, что задача решается и для контуров другой конфигурации из избранного нами класса. Таким образом, на этом небольшом примере можно проиллюстрировать главное преимущество гибких автоматизированных производств с использованием роботов: для избранного класса задач меняются только управляющие программы, а оборудование остается тем же. Не составляет труда сделать и ряд других интерпретаций возможных функций робота, например: сварка деталей по контуру или какой-то линии, шлифовка заусенцев, покраска поверхностей, сверление отверстий в заданных точках и т.п.

№5 Построить ограниченную систему из 8 дескрипторов на базе учебника или конспекта и расположить литературные источники(6) по прямой и инверсной схеме[1] для их поиска: на примере одного источника показать шаги его отыскания.

№№6-8 Освоить реализацию метода ветвей и границ с прикладной ориентацией, используя в качестве исходной для выбора своего варианта таблицы, которая приводится далее по тексту.

Метод ветвей и границ в задаче коммивояжера используется во многих модификациях. Его относят к сложным дискретным задачам, которые в худшем случае точно решаются при полном переборе всех вариантов решений. Такого типа задачи называют NP полными. Такие задачи пытаются решать различными методами и используют их также в экспериментах и для решений нейросетевыми методами. Таковой является и задача коммивояжера. Ее постановка:

имеется n городов, между которыми заданы расстояния. Требуется из заданного города объехать все города по кратчайшему замкнутому маршруту, побывав в каждом городе только 1 раз, и возвратиться в исходный город.

Задание: решить эту задачу для заданных исходных данных

Суть метода ветвей границ заключается в развитии дерева решений по основному закону, когда следующая вершина дерева всегда строится в перспективном направлении на основании лучшего значения избранной функции оценки F, которая состоит из двух частей:

$F=F_{фактич}+F_{оптимистич.}$

Трудность решения задачи состоит в подборе функции быстровычислимой $F_{оптимистич}$ и получении любым авторским методом одного начального конечного решения $F=F_{фактич}+F_{оптимистич}(=0)$

Название метода связано с тем, что из одной избранной вершины строятся все продолжения и получаются их оценки (ветвление) и после получения оценок F вычеркиваются те вершины, которые имеют оценку $F \geq F_{TR}$(текущий рекорд-лучший результат решения задачи на данный момент).

Типовая структура описания графа: в вершине (кружок, прямоугольник) располагается три цифры: вверху номер достигнутой вершины, слева $F_ф$, а справа F_o, а на ветви номер вершины, из которой ветвь идет. Конечная вершина отмечается прямоугольником, на котором записано только $F_ф$, так как $F_o=0$.

Покажем решение задачи этим методом, когда F_{TR} получено по принципу FIFO (первым пришел – первый обсуживается, а F_o=сумме всех минимальных путей для конкретной вершины с учётом уже пройденного пути).

Разработка авторских вариантов алгоритмов решения задачи комивояжера методом ветвей и границ преследует несколько целей:

1) освоить подходы к выработке собственных принципов разработки построения вспомогательных функций для повышения эффективности вычислений (прекращение решения по времени, сокращение числа вариантов, выявление нерешаемости из-за жестких требований и др.). Смысл выполнения задания заключается в описании элементов алгоритма и проведении практических расчетов на основе авторских оценочных функций и методов расчетов F_{TR};

2) предложить модификацию алгоритма, когда появляется некоторое ограничение, например, время прибытия не позже заданного для ограниченного количества точек (до начала обеда в школе, после дойки коров, ремонтные работы на дорогах в заданные интервалы времени и т.п.).

Отчетность по работе:

1) граф-схема с отображением всего процесса вычислений по алгоритму до заключительного шага. В записях отобразить списки вершин на момент перехода с яруса на ярус, а также значение оценочных функций;

2) записать оптимальный маршрут (порядок прохождения точек);

3) описать свои модификации алгоритма и привести результаты вычислений, критически оценить эффективность алгоритма.

Таблица № 1.2 – Данные для решения задачи

i / j	1	2	3	4	5	Min
1	///	1	2	6	И	1
2	3	///	3	5	3	1
3	3	4	///	Ф	4	3
4	4	4	5	///	4	4
5	3	4	5	3	///	3

Примечание: Ф – количество букв в фамилии
И – количество букв в имени

3. Задания для лабораторных работ №№ 1-11

Этот раздел включает задания, которые необходимы для усвоения типовых элементов теории моделирования на ЭВМ базовых механизмов при реализации интеллектуальных компьютерных технологий. Основным средством выполнения работ является интеллектуальная система Mathcad, так как она содержит ряд полезных процедур для построения и адаптации моделей (символьное и численное решение большого класса задач прикладной математики, аппарат для реализации случайных процессов, механизмы округления чисел до целых с избытком и недостатком, возможность гибкого построения графиков в нужном масштабе и с одновременным построением графиков нескольких функций на одном чертеже). Наличие этих возможностей полезно и для построения криптографических процедур защиты информации, аутентификации пользователей, генерировании электронной цифровой подписи и т.д., так и для понимания механизмов защиты передаваемой информации в сетях ЭВМ.

Лабораторная работа №1

Построение графиков полиномов $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x^1 + a_0$ на отрезке [p,r] в системе Mathcad

Задание:

Его выполнение опирается на типовую структуру системы Mathcad для построения графиков в декартовой системе координат, которая, будучи однажды задана, позволяет управлять процессом вычислений для получения графика заданного полинома в изменённом масштабе для любого подотрезка, вызывающего интерес исследователя.

Исходя из этой возможности, следует построить необходимые графики для ответов на следующие вопросы:

1. Найти графическим методом отрезки убывания и возрастания полинома.
2. Найти приближённо, с точностью до $\varepsilon=0.1$, корни полинома.
3. Описать своими словами схему решения задачи и сделать выводы об особенностях исследований в вашем варианте функции.
4. Вычислить полином в корневых точках.

Одна из возможных схем построения декартова графика полинома:

Задаём значительное количество точек на данном отрезке (порядка 50).

n:=50 (при необходимости его можно в дальнейшем изменять).

i:=0..50 (запись обеспечивает цикл для вычислений 50 точек графика).

Две .. реализуются нажатием клавиши «Ж».

Далее задаём свой вариант

a:= b:= c:= d:=

и координаты начала и конца отрезка, на котором исследуется функция:

p:=-8

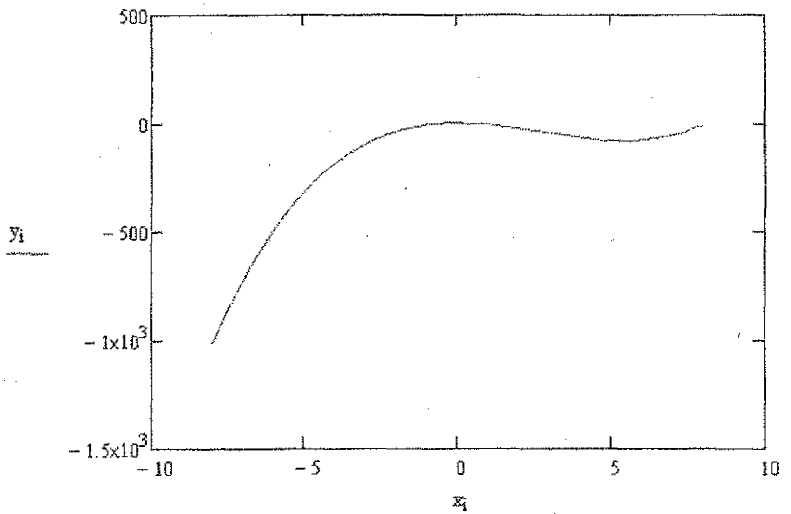
r:=8

Определяем текущие значения x и y в рассматриваемой точке:

$$x_i := p + \frac{r-p}{n} \cdot i$$

$$y_i := a \cdot x_i^3 + b \cdot x_i^2 + c \cdot x_i + d$$

После этого строим график. Для этого на панели инструментов выбираем «График» и в появившемся окне выбираем «График X-Y». После появления его шаблона на чёрных прямоугольниках заполняем x_i и y_i и щёлкаем левой клавишей мыши за пределами графика, что дает возможность получить первый график функции с целью определения последующих отрезков для более тщательного её исследования.



Новый исследуемый отрезок задается изменением p и r и результат отображения функции получается после щелчка рядом с графиком.

Варианты для выполнения лабораторной работы

Таблица 3 – Выбор варианта

№ варианта	a	b	c	d
1	1	-8	-1	1
2	1	-8	1	1
3	2	-16	1	1
4	1	-15	1	1
5	1	-9	1	15
6	2	-20	1	15
7	2	15	1	1
8	1	5	1	1
9	1	4	1	1
10	1	2	-1	1
11	1	-3	-4	-4
12	1	-2	0	-4

Оформление отчета

Оформление и предъявление отчета возможно в двух вариантах: в печатном, что лучше, или на компьютере на сайте студента, где будут храниться все лабораторные работы, которые дублируются на флешке студента с целью обеспечения их сохранности.

Лабораторная работа № 2

Решение уравнений n-й степени от одной переменной, содержащих простейшие трансцендентные функции (тригонометрические, логарифмические, показательные) на заданном отрезке [p, r] типа $a_n x^n+a_{n-1}x^{n-1}+\ldots+a_i x+a_0-k\sin(tx)$; ((klntx;$k^{tx}$))

Задание:

Требуется решить задачу для своего варианта тремя путями:

1. Графическим методом с точностью до 0,1 с одновременным построением графиков на заданном отрезке для двух функций (полинома и трансцендентной) найти координаты их точек пересечения. В качестве корней записываются все точки пересечения двух графиков, построенные по общей процедуре в Mathcad:

n:=50

i:=0..50

Далее для своего варианта указываются конкретные значения коэффициентов и координаты начала и конца отрезка, на котором исследуется функция:

a:= b:= c:= d:= k:= t:=

p:=-8

r:=8

(Определяется текущее значение x_i общее для двух графиков и значения функций y_i и z_i)

$$x_i := p + \frac{r-p}{n} \cdot i$$

$$y_i := a \cdot x_i^3 + b \cdot x_i^2 + c \cdot x_i + d$$

z_i:=ksin(tx_i)

После этого строим декартов график. Для этого на панели инструментов выбираем «График» и в появившемся окне выбираем «График X-Y». После появления его шаблона на чёрных прямоугольниках внизу заполняем x_i, а слева посередине записываем y_i, ставим запятую и далее z_i. Щёлкаем мышью рядом с графиком, что дает возможность получить первый график для определения отрезков для более тщательного исследования расположения корней уравнения. При необходимости путем изменения длины исследуемого отрезка получают более точные значения корней и записывают их с нужной точностью.

2. Каждый корень находится вновь с помощью процедуры root для отыскания одного корня. В качестве его начальной величины подставляются в порядке следования корни, найденные графическим путем и соответствующие отрезки для них. Последовательно фиксируются результаты, полученные с помощью процедуры root. Типовая структура для решения задачи (исходные данные используются те же: коэффициенты и длины отрезков), так как они фиксировались ранее и их можно использовать снова. Перед процедурой root задается соответствующее x, равное значению корня, и отрезок [p, r], на котором этот корень был найден, т.е.:

x:=

$f(x):= a \cdot x^3 + b \cdot x^2 + c \cdot x + d - k\sin(tx)$

root (f(x), x, p, r), где p и r – границы найденного корня, и щелчком получается результат.

3. Регулирование точности вычислений при применении процедуры root и любых других по количеству знаков делается так: открывается меню «формат», затем подменю «результат» и указывается требуемое число десятичных знаков в открывшемся окне (5 пять! 5 набирается с клавиатуры). После чего пересчитываются все корни с применением процедуры root.

4. Вычисляются все значения функции для всех найденных корней. Делаются выводы о степени приближения результатов к нулю в зависимости от точности. Для отчета по работе описывается ход эксперимента и делаются выводы.

Варианты для выполнения лабораторной работы

Таблица 4 – Выбор варианта

№ варианта	a	b	c	d	k	t
1	1	-8	-1	1	5	2
2	1	-8	1	1	6	2
3	2	-16	1	1	7	2
4	1	-15	1	1	5	3
5	1	-9	1	15	6	3
6	2	-20	1	15	7	3
7	2	15	1	1	5	4
8	1	5	1	1	6	4
9	1	4	1	1	7	4
10	1	2	-1	1	5	5
11	1	-3	-4	-4	5	6
12	1	-2	0	-4	5	7
13	1	-3	1	1	5	8

Лабораторная работа № 3

Символьные и чиćленные решения уравнений и неравенств, содержащих функции алгебраического типа

Задание:

Требуется освоить применение символьных вычислений с последующим получением конкретных результатов численными методами. Задача решается для функций в виде полиномов P(x) и алгебраических дробей P(x)/Q(x) в соответствии с заданными вариантами

Mathcad является полезной системой для изучения в рамках специальности «Искусственный интеллект», так как содержит процедуры символьных вычислений, когда результаты отображаются в символьной форме: вычисления производных, интегралов, уравнений, неравенств и др. Это позволяет решать ряд задач в общей алгебраической форме, а потом подбирать значения нужных параметров и вычислять конкретные значения для найденных решений в символьной форме. Для этой цели используются палитры символы, вставить функцию, матрица, математика и другие.

Отбор основных функций для изучения диктуется тем, что решение неравенства часто связано с необходимостью решить уравнение, упростить функцию в ее символьной записи или сделать преобразование для толкования результатов.

К таким процедурам для более глубокого изучения отнесем: simplfay (упростить), solve (решить уравнение или неравенство), factor (представление выражений в виде сомножителей), expand (разложение рациональных дробей P(x)/Q(x)) и некоторые другие.

Отбор и освоение этих инструментов диктуется необходимостью освоения полезной информации и навыков в решении неравенств и уравнений, содержащих в своем составе элементарные алгебраические функции. Главным объектом исследования являются полиномы, так как для них наиболее развит аппарат символьных вычислений. В частности, получение решения уравнений в символьной форме и различные преобразования алгебраических выражений. Поэтому основными исходными объектами для исследования выбираются алгебраические уравнения и неравенства типа:

$P(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0(=0$, или > 0, или $<0)$, а так же алгебраические дроби типа P(x)/Q(x), содержащие полиномы в числителе и знаменателе.

Конкретный вид объекта определяется вариантом лабораторной работы, который предусматривает получение символьного решения, а затем по полученному объекту с подстановкой данных варианта конкретного решения. Желательно проанализировать возможные границы их колебаний в рамках существования полученного решения и сделать выводы.

Задания для изучения имеют следующую структуру:

1. $P(x)=ax^3+bx^2+cx+d(=0$, или > 0, или $<0)$
2. $P(x)/Q(x) =(ax^3+bx+c)/ax^2+bx+c) > 0$

По первому заданию получить символьное и численное решение, воспользовавшись процедурой solve с представлением d в буквенной форме при получении символьного решения. Далее против строки слева с символьным решением присваивается конкретное значение d, вычисляются корни и после этого записывается решение неравенства P(x)> 0 по известным из средней школы методам. Далее при конкретных a,b,c,d для полинома P(x) применяется процедура solve и получается решение неравенства в символьной форме. Требуется сравнить оба результата.

По третьему заданию вычисляется предел дроби P(x)/Q(x) с помощью оператора lim, когда x стремится к n, а затем вычисляется лимит при n=d.

Описать ход работы и сделать выводы.

Таблица № 5 – Выбор варианта задания

№ варианта	a	b	c	d
1	1	2	-1	-2
2	1	0	-3	-2
3	1	-3	-1	3
4	1	-4	-1	4
5	1	-1	-4	4
6	1	-3	-4	12
7	1	-4	-4	16
8	1	-6	3	10
9	1	-6	11	-6
10	1	-7	14	-8
11	1	-8	17	-10
12	1	-9	20	-12
13	1	-8	19	-12

Лабораторная работа № 4

Символьное дифференцирование функций в системе Mathcad и его применение (частные производные в градиентных методах оптимизации)

Задание:

Требуется вычислить определитель 3-го порядка в символьной форме, содержащей цифровые и буквенные элементы (x, y, z). От полученной функции F(x, y, z) найти частные производные F'_x, F'_y, F'_z как будущие компоненты градиента (вектора, указывающего своим направлением наискорейшее возрастание функции: $F'_x \cdot \vec{i} + F'_y \cdot \vec{j} + F'_z \cdot \vec{k}$). Далее вычислим их нужное количество раз в требуемых точках. Найти локальные минимум и максимум F(x, y, z), когда $a-\varepsilon \le x \le a+\varepsilon$, $b-\varepsilon \le y \le b+\varepsilon$, $c-\varepsilon \le z \le c+\varepsilon$. Начальная точка для вычисления частных производных равна количеству букв в Ф, И, О, т.е. x=Ф=a, y=И=в, z=О=c , $\varepsilon = 0{,}1$. Первая строка определителя – (1, x, 2), вторая – (3, 4, y), третья – (z, 5, 6). Сделать вывод о возможном существовании определителя, равного нулю, так как смысл решения задачи состоит в установлении факта возможности

отсутствия решения системы линейных уравнений из-за того, что переменные x, y, z замерялись приборами с ошибкой ε и в скрытой форме может существовать определитель, равный нулю.

Опишем процедуры отыскания локального минимума (максимума): в полученной текущей точке вычисляются знаки производных по переменным x, y, z для построения следующей точки. Учитывая, что структура исследуемой функции F(x, y, z) такова, что ее максимум (минимум) достигается на концах отрезков области изменения переменных, то допустимо применение метода наискорейшего спуска, когда по знаку частной производной для данной переменной больше нуля при поиске минимума выбирается левая сторона отрезка, а для максимума правая и, наоборот, в противном случае. Процесс поиска обрывается при зацикливании, т.е. при получении одной и той же точки (x, y, z) второй раз. Одновременно ведется вычисление значения функции в каждой полученной точке. Зацикливание соответствует прекращению нарастания (убывания) функции. Все шаги протоколируются по итоговым результатам. Процедура вычисления определителя представляет собой символьные действия над векторами и матрицами (вычисление определителей, транспонирование и др.). Будем рассматривать все операции над матрицами, так как вектор можно считать однострочной или одностолбцовой матрицей. Матрица может задаваться следующим образом: на панели управления набирается «вставка» и в ее меню отмечается матрица и на экране можно задать количество строк и столбцов. Аналогичный результат получим сразу, если щелкнем в меню по изображению незаполненной матрицы. Заполним конкретными данными матрицу $n \times n (3 \times 3)$. Через панель управления (символика) можно вызвать подменю «матрица» и в нем выбрать нужную операцию (транспозиция, инвертирование, определитель).

Обратившись к меню «символика», выполним операцию по вычислению определителя и в итоге получим F(x, y, z)=54-5y-18x+zxy-8z, соответствующее значению det A в символьной форме. После этого вычислим в символьной форме общий вид частных производных F'_x, F'_y, F'_z и, подставляя в них конкретные значения текущих точек, приступим к процедуре выполнения оптимизации.

Описать процесс вычислений и сделать выводы. Дополнительно для связи с задачами, решаемыми в курсе высшей математики, вычислить обратную и транспонируемую матрицу для вашего задания. Для контроля результата лабораторной работы можно применить процедуру Minimize (Maximize) по следующей схеме:

f(x, y, z) := значение символьного определителя.

x:=2; y:=5; z:=8 (любые числа, по возможности близкие к min, max)

Given

$a - \varepsilon \le x \le a + \varepsilon$

$b - \varepsilon \le y \le b + \varepsilon$

$c - \varepsilon \le z \le c + \varepsilon$

P:= Maximize (Minimize) (f, x, y, z) P= (обыч. равно) f(P_0, P_1, P_2)=(обыч. равно).

Лабораторная работа № 5

Отыскание экстремумов функций многих переменных в системе Mathcad

Задание:

Требуется вычислить max и min F(x, y, z)=$x^3y^2z-2x^2yz+3xy+c$. От полученной функции F(x, y, z) найти частные производные F'_x, F'_y, F'_z как будущие компоненты градиента (вектора, указывающего своим направлением наискорейшее возрастание функции: $F'_x \cdot \vec{i} + F'_y \cdot \vec{j} + F'_z \cdot \vec{k}$). Далее вычислим их нужное количество раз в требуемых точках. Найти локальные минимум и максимум F(x, y, z), когда $\Phi-2 \le x \le \Phi+2$, $И-2 \le y \le И+2$, $О-3 \le z \le О+3$. Начальная точка для вычисления частных производных равна $(b-a)\gamma$ (вычисляется как x(y,z)= a+ $rnd(b-a)$, где $(b-a)$ величина отрезка для соответствующей переменной; Ф, И, О – количество букв в фамилии, имени, отчестве).

Опишем процедуры отыскания локального минимума (максимума): в полученной текущей точке вычисляются знаки производных по переменным x, y, z для построения следующей точки. Учитывая, что структура экстремумов исследуемой функции F(x, y, z) неизвестна, требуется испытать разный шаг h по каждой переменной, по знаку частной производной для данной переменной больше нуля при поиске минимума выбирается движение к левой стороне (x-h) отрезка, а для максимума к правой (x+h) и наоборот в противном случае. Процесс поиска обрывается при зацикливании, т.е. при получении одной и той же точки (x, y, z) второй раз (при выходе за пределы отрезка в качестве значения переменной выбирается пересекаемая граница). Одновременно ведется вычисление значения функции в каждой полученной точке. Зацикливание соответствует прекращению нарастания (убывания) функции. Все шаги протоколируются по итоговым результатам. Процедура вычисления F служит дополнительным критерием движения к цели.

Вычислим в символьной форме общий вид частных производных F'_x, F'_y, F'_z и, подставляя в них конкретные значения текущих точек, приступим к процедуре выполнения оптимизации. Рекомендуем начать с шага h=1, понижая его в процессе после зацикливания постепенно до уровня 0.1.

Описать процесс вычислений и сделать выводы. Для контроля результата лабораторной работы можно применить процедуру Minimize (Maximize) по следующей схеме:

f(x, y, z) := $x^3y^2z-2x^2yz+3xy+c$

x:=; y:=; z:= (любые числа, по возможности близкие к точкам min, max)

Given

$\Phi-2 \le x \le \Phi+2$,

$И-2 \le y \le И+2$,

$О-3 \le z \le О+3$

P:= Maximize (Minimize) (f, x, y, z) P= (обычное равно) f(P_O, P_1, P_2)=(обычное равно).Знак = ставится в момент чтения результата.

Вторая попытка делается из новой случайной точки $(a+rnd(b-a))$ при повторном решении первым методом.

Лабораторная работа № 6

Моделирование информационных процессов со случайными компонентами

Задание:

Освоить механизм моделирования независимого от исследователя выбора хода процесса методом статистических испытаний, сделать выводы об особенностях таких вычислений с учётом излагаемой далее теории. Модель – представляемая мысленно или материально реализованная система, которая в процессе познания, анализа замещает реальный объект, сохраняя важные для исследования его черты. По сути дела модель является упрощенным образом реального объекта для более глубокого изучения действительности. Метод исследований, базирующийся на разработке и использовании моделей, называется моделированием. Модель всегда предполагает участие в ее создании (конструировании) исследователя, так как на нем лежит ответственность за адекватность модели объекту с позиции изучаемых его свойств.

Смысл использования моделей состоит в упрощении и удешевлении процессов изучения, а иногда их использование практически представляет почти единственный путь к получению необходимых результатов (угроза взрыва, дороговизна натурного эксперимента и т.п.). Обычно различают методы материального (существует связь с материальными объектами модели) и идеального моделирования (рассматриваются мысленные связи между объектом и моделью).

Среди формализованных моделей выделяют знаковые модели, в которых используются системы знаков с правилами их преобразования и интерпретации. Его частным случаем является математическое моделирование, которое характерно тем, что разные процессы (объекты) могут описываться одинаковыми формулами и уравнениями. Например, законы о течении жидкостей и газов, расширении твердых тел и т.п.

Во всех случаях и видах моделирования соблюдается главный принцип: модель должна соответствовать оригиналу в главном только в том, что интересует исследователя, а несущественное можно отбросить.

Математическое моделирование наиболее важно при использовании вычислительной техники. Это связано с тем, что с его помощью можно получить доказательство существования решения задачи и оценить время получения результата, диапазон изменения переменных, возможную точность результата и т.д.

При математическом моделировании на ЭВМ возможно формировать базы данных для других задач, из типовых элементов строить прочие модели. Корректное построение всех видов моделей невозможно без участия специалистов: выбор переменных, формирование ограничений.

Среди многочисленных видов моделей важнейшая роль отводится моделям принятия решений и их оптимизации. Наибольшую трудность обычно вызывают задачи многокритериальной оптимизации, которые поддаются получению приемлемых решений с применением ЭВМ, а иногда и с участием человека, который формирует путь поиска решений.

Особая роль отводится вероятностным моделям и реализации на их основе вероятностных процессов. Эти модели используются в имитационном моделировании, когда требуется изучить характеристики процесса, на который влияют случайные факторы, путем его многократного воспроизведения по элементарным шагам и фиксирования различных средних характеристик в целом путем подсчета количества воспроизводимых явлений в изучаемом процессе (например, отыскание емкости резервного бункера заготовок для обработки на автоматической линии по причине поломок или затупления инструмента, поиска показателей реальных случайных процессов для статистических оценок разброса измерений и т.п.

Вероятностное моделирование на ЭВМ обычно опирается на использование генератора случайных чисел, равномерно распределенных в диапазоне (0, 1) или (0, a), который содержится в большинстве вычислительных систем в виде стандартной процедуры. На его основе обычно строятся случайные процессы с использованием стандартных процедур для воспроизведения элементов моделей в виде конкретных случайных законов (экспоненциальный, нормальный и др.).

Второй путь использования генератора случайных чисел состоит в выборе случайных условий или путей продолжения процессов, когда требуется исключить влияние исследователя на выбор текущего продолжения процесса, например, стартовых точек для различных итерационных процессов вычислений для многомерных функций и т.п.

Информационные модели – знаковые модели, описывающие процессы получения, передачи, преобразования и использования информации. Их основой во многих случаях являются вычислительные модели, на базе которых разрабатываются алгоритмы и программы. При машинном моделировании всегда реализуются знаковые модели. Иногда говорят, что компьютерное моделирование – это моделирование теории изучаемого объекта. В этом смысле нейронная сеть является теорией для грубого представления функционирования мозга. Имитационные модели воспроизводят (имитируют) процессы функционирования объекта. Программа для ЭВМ – формализованная информационная модель деятельности. Фотография – статическая информационная модель.

В данной работе предлагается повторить лабораторную работу №5 многократно при случайном выборе координат 5 начальных точек(в вашем варианте функция $F(x.y,z)=x^3 y^2 z+3x^2 y-yz$ с областью определения(Ф-2<=x<=Ф, И-3<=y<=И, О-1<=z<=О) градиентным методом найти минимум и максимум функции (лучшие результаты из 5 попыток, их же вычислить с помощью процедуры Maximize (Minimize). Шаг изменения каждой координаты может быть разным в диапазоне от 1до 0.1). Протокол одной попытки поиска результата можно представлять в укрупнённой форме в виде логической цепочки векторов, каждый из которых должен содержать значения компонент: координаты точки, значение функции и частных производных, рекомендуемый следующий шаг по каждой координате(0 или-h или+h). При обобщении шагов координаты одного знака суммируются. Для эффективной работы полезно построить такую структуру: первая строка-переменные с присвоением текущих значений коор-

динт, вторая строка-функция в алгебраической форме и в 3-5 строках аналогично записываются частные производные. Такая структура позволяет сразу вычислить весь вектор за исключением шагов, подбираемых исследователем. Оформить выводы, обобщив результаты всех попыток и проверок.

Лабораторная работа № 7

Моделирование решения задач методом Монте-Карло

Задание:

Освоить метод вычисления площадей и сложных функций на основе моделирования случайных процессов, осветить проблемы достижения точности результатов и провести их сравнительный анализ с обычными численными методами для различных типов функций.

Метод Монте-Карло (статистических испытаний) – численный метод решения математических задач при помощи моделирования случайных процессов и событий. Его название происходит от города Монте-Карло, известного своими игорными домами.

Для реализации случайной величины используют датчики, генерирующие случайную последовательность чисел, равномерно распределенных на интервале (0, 1). Различают чаще всего два типа генераторов случайных чисел: физические датчики (источник – реальные физические процессы типа шумов электронных приборов, радиоактивные излучения и т.п.); программные датчики псевдослучайных чисел (эти числа по своим свойствам практически неотличимы от полученных физическими датчиками).

Чтобы обеспечить получение цепочки случайных событий, обычно их воспроизводят используя набор стандартных программ для моделирования известных случайных событий с фиксированными параметрами (математическое ожидание, дисперсия и т.п.).

Это порождает проблему доказательности доверия к результату, полученному методом Монте-Карло. Поэтому в серьезных исследованиях проверяются источники моделирования на соответствие теоретическим параметрам при выполнении заданного количества вычислительных опытов (обычно от 100 до 10 000). Это связано с тем, что ошибка вычислений обычно пропорциональна величине $1/\sqrt{N}$, где N – количество опытов, например, при 400 опытах можно ожидать ошибку до 0,05 от конечного результата.

В данном случае ставится задача проверить на пригодность модели для получения чисел, распределенных по равномерному закону, который моделируется для базовых параметров в интервале (0,1) и математического ожидания 0,5 и среднего квадратичного отклонения 0,083.

Практическое применение в различных математических задачах метод нашел при вычислении площадей, ограниченных сложными контурами, когда обычным интегрированием решить задачу очень сложно, а иногда отсутствуют и готовые методы ее решения. Идея предлагаемого метода заключается в следующем: сложную фигуру неизвестной площади помещают в квадрат (круг,

прямоугольник), площадь которого известна. После этого моделируют вбрасывание N случайных точек в квадрат и фиксируют количество точек n, попавших в искомую фигуру. При большом числе точек справедливо равенство $S_{фигуры}/S_{квадрата} \approx n/N$. Этот способ можно использовать для проверки качества генератора случайных чисел из интервала (0,1).

Для этих целей возьмем квадрат со стороной 1 и впишем в него четверть круга единичного радиуса. Тогда $S_{кв} = 1$; $\frac{1}{4}S_{кр} = \frac{1}{4}\pi R^2 = \frac{1}{4}\pi$. Тогда при получении n/N приближенно равно 0,78 ($\pi/4$) можно сделать вывод о работоспособности генератора. С целью выполнения такой проверки вбрасывают N случайных точек. Если хотят обеспечить точность 0,01, то для доверия к результату необходимо вбросить около 10 000 точек.

Проверить на практике, при скольких точках может быть достигнута заданная точность E, и построить график зависимости точности от N. (N=100,200, …1000). Один из возможных вариантов реализации этой проверки можно осуществить по следующей схеме, позволяющей получить для любого N декартов график и n/N:

N:= T_0:=0
i:=1..N
t_i:=(rnd(1))^2+(rnd(1))^2
T_i:=T_{i-1}+(2-ceil(t_i))
K_i:=i
R_i:=T_i/K_i

Замечания: N – задаваемое количество точек, t_i – сумма квадратов координат текущей точки, T_i – попавшие в четверть круга точки, R_i – результат, на графике по оси x записывается K_i,а по оси y – R_i. Для вычисления интегралов материал подбирается самостоятельно из курса высшей математики. Для f(x)>0 на отрезке (a,в) можно при a>0, maxf(x)=c воспользоваться формулой S=c(b-a)n/N. В этом случае в качестве x вбрасывается координата a +rnd (b-a), а в качестве y – координата rnd(c). Считается, что испытание прошло успешно (случайная точка попала под кривую или на неё: f(a+rnd(b-a))-rnd(c)>=0), а в противном случае она выпала над кривой в площади окаймляющего прямоугольника.

Лабораторная работа № 8

Одноключевая система шифрования Диффи и Хеллмана

Задание:

Построить систему шифрования Диффи и Хеллмана для a=(количество согласных букв в фамилии студента), p больше или равно количеству всех букв в фамилии. Подобрать a и p самостоятельно методом проб и ошибок, выбрать два секретных числа X_i и X_j и для связи пользователей сети i и j вычислить числа Z_{ij} и Z_{ji}.

Описание метода.

Диффи и Хеллман реализовали идею использования функций с лазейкой для построения криптосистемы в сети с открытым распределением ключей. Для

решения этой задачи они предложили использовать функцию $F(x) = a^x \bmod p$, где p – большое простое число, x – произвольное натуральное число из множества $\{1,2,...,(p-1)\}$, a – целое число из множества $\{2,3,...,p\}$, для которого выполняется требование, чтобы все степени a от 1 до $(p-1)$ в произвольном порядке по модулю p дали все числа из множества $\{1,2,...,(p-1)\}$.

Например, при модуле $p = 7$ можно выбрать $a = 3$

$(f(1) = 3^1 (\bmod 7) = 3, f(2) = 3^2 \bmod 7 = 2, f(3) = 3^3 (\bmod 7) = 6, f(4) = 3^4 (\bmod 7) = 4,$

$f(5) = 3^5 (\bmod 7) = 5, f(6) = 3^6 (\bmod 7) = 1)$

Предполагается, что всем пользователям сети известны a и p. Пользователь i случайным образом выбирает число x_i (свою лазейку), т.е. секретное число, известное только ему из множества $\{1,2,...,(p-1)\}$. Далее он вычисляет $y_i = a^{x_i} (\bmod p)$ и помещает его в открытый для доступа всех пользователей сети справочник. При желании установить секретную связь с пользователем j он берет из справочника его число y_j и с помощью своего секрета x_i для обмена сообщениями с j вычисляет ключ $Z_{ij} = (y_j)^{x_i} (\bmod p)$. После установления контакта аналогичную работу проделывает пользователь j, который с помощью своего секретного числа x_j вычисляет $Z_{ji} = (y_i)^{x_j} \bmod p$. Ограничения, наложенные на выбор a, обеспечивают получение равенства $Z_{ij} = Z_{ji}$, т.е. одинаковых ключей для обмена сообщениями. В самом деле, $Z_{ij} = y_j^{x_i} \bmod p = (a^{x_j})^{x_i} \bmod p = a^{x_j x_i} \bmod p$ и $Z_{ji} = a^{x_i x_j} (\bmod p)$.

Пример $(p = 7, a = 3, x = \{1,2,3,4,5,6\}$

$x_i = 3$ (секрет i) $y_i = 3^3 \bmod 7 = 6$

$x_j = 4$ (секрет j) $y_j = 3^4 \bmod 7 = 4$

$Z_{ij} = 4^3 \bmod 7 = 1$

$Z_{ji} = 6^4 \bmod 7 = 1296 \bmod 7 = 1$

Цифра 1 может означать некоторую функцию, которая используется при кодировании; страницу в заранее разосланных пользователям материалах и т.д.

Недостаток описанной криптосистемы с открытым распространением ключей состоит в том, что она требует абсолютного доверия партнеров по связи друг к другу, так как в этой одноключевой системе они могут изменять переданный текст. Поэтому она непригодна, например, для не доверяющих друг другу удаленных абонентов. Вычисление остатков x при делении целых чисел на модуль y можно выполнять с помощью функции mod(x,y).

Лабораторная работа № 9

Двухключевая система RSA

Задание:

Построить двухключевую систему с использованием алгоритма RSA и выполнить в ней операцию шифрования и дешифрования трех первых букв фами-

лии студента (при количестве букв меньше 3, недостающие буквы берутся из имени). Пара простых чисел P и Q выбирается из диапазона ближайших к количеству букв в фамилии и имени студента.

Например, Петров Владимир, P (5 или 7), Q (7 или 11). Методом испытаний подбирается также ближайшая пара чисел Е и Д.

В нашем случае это могут быть P=5; Q=7.

В случае неудачных сочетаний из названного диапазона берутся рядом другие ближайшие простые числа, например, P=5, Q=13

Описание метода. В системе RSA каждый пользователь имеет свой ключ шифрования. Ключи дешифрования известны всем, а шифрующий ключ держится в секрете. Криптографические системы типа RSA подходят для реализации цифровой подписи, применяемой в системах электронных платежей и при передаче сообщений с помощью устройств телесвязи.

К недостаткам системы RSA и аналогичных ей относят ее существенно более низкое быстродействие и потребность в более длинных ключах. Наиболее эффективные реализации RSA характеризуются скоростью шифрования порядка нескольких тысяч бит в секунду. Тогда как аналогичные реализации более простых систем шифруют несколько миллионов бит в секунду. В связи с этим наиболее целесообразным применением RSA считается организация обмена секретными ключами, необходимыми для обеспечения безопасности в сетях связи.

Основная проблема для системы RSA – генерация соответствующей пары ключей. Для генерации используется следующая процедура:

1. Выбрать 2 простых числа P и Q.

2. Найти произведение N=PQ и число L=(P-1)(Q-1).

3. Выбрать случайное число D такое, что оно должно быть взаимно простым с числом L (числа называются взаимно простыми, если они не имеют общего делителя).

4. Определяют другое число E такое, что (ED) modL=1.

5. Как только все числа найдены, мы имеем: секретный ключ – E; открытый ключ – пара чисел D и N.

Тогда при шифровании сообщения его разбивают на блоки M. В результате шифрования для каждого блока M получим число

$C = (M^E) \bmod N$.

При дешифрации получаем:

$M^* = (C^D) \bmod N$.

Рассмотрим это на примере алфавита из букв {А,О,Я}={1,2,3} для передачи текста «ОЛЯ» (или 2,1,3). Цифровые обозначения букв или блоков обязательны, так как метод основывается на обработке натуральных чисел.

1. Выберем P=3 и Q=11.

2. Найдем N=PQ, N=33; L=(P-1)(Q-1); L=20.

3. Выберем D взаимно простое с L: D=3.

4. Выберем E такое, что $(ED) \bmod L = 1$: E=7, действительно,

$(7 \cdot 3) \bmod 20 = 1$.

5. Тогда открытый ключ $\left.\begin{matrix} D=3 \\ N=33 \end{matrix}\right\}$ секретный $E=7$.

Производим шифрацию своим закрытым ключом 7:

$$C1=(2^7)\bmod 33=29$$

$$C1=(M1^B)\bmod N:\ C2=(1^7)\bmod 33=1$$

$$C3=(3^7)\bmod 33=9$$

Зашифрованный текст получается (29,1,9).

Расшифровка текста открытым ключом 3 и33:

$$M1^x=29^3\bmod 33=2$$

$$M1^*=(C1^D)\bmod N:\quad M2^x=1^3\bmod 33=1$$

$$M3^x=9^3\bmod =3$$

В результате мы получили исходный текст.

Остается только добавить, что для получения достаточно стойкой шифровки необходимо брать очень большие простые числа.

Выполнение соотношения $(ED)\bmod L=1$ позволяет использовать этот факт для проверки подлинности подписи без знания секретного ключа E с помощью аппарата ХЭШ-функций.

В практической работе необходимо идентифицировать автора электронного документа и предприятие не по особенностям подписи и печати (например, по образцам подписей и печатей в банковской карточке клиента), а по наличию у него электронного ключа для подписывания документов. В этом случае конкретное число-подпись под данным документом в фиксированное время может сделать только законный обладатель ключа (E).

Процедура электронной подписи включает в себя два этапа: первый – подписывание (вычисление параметров подписи, зависящих от текста конкретного документа, один из которых (E) хранится в секрете); второй – проверка получателем с помощью несекретных параметров (D,N) подлинности сообщения (подписи).

Сообщение шифруется по алгоритму RSA, где E подбирается и известно только отправителю, а D, N знает и получатель. Получатель должен иметь возможность с помощью открытого ключа проверить подлинность сообщения. Для этой цели в сообщение добавляется еще одно число, которое является результатом вычисления хэш-функции h (T), зависящей от текста T.

Лабораторная работа №10

Обеспечение подлинности сообщений

Задание:

Подобрать хэш-функции h (T) или применить из теоретического материала и, используя секретный ключ E из предыдущего задания и зашифрованное сообщение (три буквы), вычислить m=h(T) и $S=(m^E)\bmod N$. Далее, пользуясь открытым ключом Д, вычислить m из соотношения $(S^D)=m \bmod N$ и убедиться в

его совпадении с m владельца секретного ключа. В конечном виде передаваемое m<N.

Описание теоретических основ метода.

К хэш-функции предъявляется ряд требований:

– невозможность (или за очень длительное время) найти по значению h(T) само T(т.е. требуется построить практически необратимую функцию);

– для заданного T нельзя найти такое T', чтобы h (T)=h (T');

– вообще нельзя найти пару различных слов T и T' такую, что h(T)=h(T');

– сообщение T (например, текст договора, платежного поручения и т.п.) по заданной функции сжимается в целое число m=h(T), причем 1<h(T)<N.

Число m позволяет с помощью открытого ключа констатировать подлинность документа.

С этой целью автор документа с помощью своего секретного ключа E получает второй параметр подписи $S = (m^E) \bmod N$. Параметры m и s вставляются в текст сообщения на место подписи и печати. Все сообщение по телекоммуникационным каналам передается получателю. Он проверяет правильность цифровых параметров m и s, исходя из знания функции h(T), полученного символьного объема зашифрованного сообщения (T1) и «лазейки» для вычисления h(T), h(T1).

Проверка параметра S производится путем идентификации условия:

$(S^D) = m \bmod N$

Математически доказано, что результат проверки m и s будет положительным в том случае, когда в их формировании использовался секретный ключ E, соответствующий открытому ключу D. Вероятность расшифровки секретного ключа E по открытым параметрам s, m, D и N считается ничтожно малой из-за затрат времени на решение задачи взлома системы велико по сравнению со временем полезного действия сообщения.

Покажем в упрощенном варианте проверку подписи сообщения T=(ОЛЯ), с дополнением его параметрами m и s. В качестве функции хеширования h(T) возьмем произведение П сумм из двух элементов каждого шифруемого знака: его номера позиции в тексте с его числовым кодированием. В нашем случае их позиции О=1, Л=2, Я=3, а коды Л=1, 0=2, Я=3, т.е. П=(1+2)(2+1)(3+3)=54, чтобы получить m вычисляем его так: $m = П \bmod N = 54 \bmod (33) = 21$. Можно убедиться, что эта функция удовлетворяет требованиям к ней по крайней мере для любого сообщения из 3-х букв. Это обнаруживается при вычислении всех возможных 6 разнобуквенных сообщений T: (ОЛЯ)–21, (ОЯЛ)–14, (ЛОЯ)-15, ЛЯО (20), ЯОЛ (31), ЯЛО (27), т.е. нет равных h(T)

Если взять любые сообщения из трех букв типа ООО, ЯОО и т.п., тоже совпадающих h(T) не будет. Следует заметить, что с ростом длины сообщения может оказаться, что такая функция не удовлетворяет требованию, когда два сообщения разной длины имеют одинаковое значение, т.е. h(T)= h(T'). Чтобы избежать такого явления, можно разбивать сообщения на блоки заранее ограниченной длины. Поэтому выбор хорошей функции h(T) является очень трудной задачей, и ее решением занимаются специалисты, которые разрабатывают

стандарты шифрования. В описанном нами примере ограничимся лишь демонстрацией процедуры признания подписи.

Текст T, который получает партнер, позволяет проверить подлинность подписи по параметрам m, s и D=3 (известно как открытая часть ключа), s и m приходят с текстом отправителя ($s = m^E \bmod N = 21^7 \bmod 33 = 21; m = 21 < 33$). Проверка подлинности сообщения:

$S^D = m \bmod N; 21^3 = 21 \bmod 33$, т.е. результат проверки положителен и подпись подлинна. Кроме того, если получатель тоже знает как вычислить функцию хеширования от текста, то по прочитанному тексту он может ее вычислить.

В настоящее время в Республике Беларусь выпущен предварительный стандарт СТБ П34, 101.25-2008 для электронной подписи, в котором алгоритм RSA один из трех рекомендуемых для применения.

Лабораторная работа №11

Методы борьбы с контрафактной продукцией на основе БД

Задание:

Проверить штрих-код любого предприятия по описанному далее алгоритму и отметить его полезные функции в автоматизированных системах управления, логистике, создании баз данных. Предложить скрытую часть кода (пломбируемую или защищенную краской), например, какую-то функцию от серийного номера изделия, гаммированный передаваемый в двоичной форме серийный номер изделия. Гаммирование можно выполнить с помощью части таблицы случайных двоичных чисел: 01011000101110101011100010101l0. В этом случае передающая и принимающая стороны знают начальную строку и позицию цифры в ней, с которой начинать отсчет. Пусть требуется гаммировать блок 10101111010011100110 с помощью таблицы с пятой цифры в ней. Тогда, например, запись 7624 переводится в двоично-десятичный код каждой из шифр: 0111011000100100 и получим гаммированный блок:1000001011000010.

Особенности использования штрих-кодов в борьбе с контрафактной продукцией (подделки от имени предприятия –производителя) можно использовать также особого рода протоколы.

В основе борьбы от подделок лежат скрытые и открытые маркировки производителя. Обычно такие маркировки состоят из двух и боле частей. Открытая часть может содержать штрих-код (например, EAN-13), из этого используемого в Европейской практике международного классификатора видна страна происхождения товара по первым трём цифрам, по следующим 4-м код продукта и ещё по следующим 4-м код предприятия и последняя цифра является контрольной. Всей этой информации достаточно, чтобы обратиться к производителю. Кодирование скрытой части индивидуально для каждого изделия и представляет собой набор случайных генерируемых программой цифр и машиночитаемых знаков. Скрытую часть невозможно прочитать без нарушения целостности изделия или упаковки или без удаления стирающегося слоя краски (подобно защите лотерейных билетов Спортлото).

Производитель создаёт уникальную электронную базу данных с неповторяющимися идентификаторами, тождественными скрытой маркировке на изделии. При первом запросе покупателя на предприятие для подтверждения подлинности кода изделия, этот код удаляется в другую базу данных, т.е. вторая и последующие авторизации невозможны, а при несоответствии первого предъявления уникального кода или его повторном предъявлении можно приступить к борьбе с авторами подделок.

Эта же система исключает и продажу неучтённой продукции, выпущенной на самом предприятии. Кроме того, исключаются и грубые подделки штрихкода. Существует простой алгоритм проверки кода EAN-13.

Алгоритм проверки кода:

1. Сложить цифры, стоящие на четных местах Sr.
2. Умножить Sr*3=S1.
3. Сложить цифры на нечетных местах Sн (без контрольной).
4. Получить S=S1+Sн.
5. Оставить от S только число в младшем разряде (t).
6. Найти разность P=10-t.

При правильном коде P должно совпасть с контрольной цифрой.

Пример. 8590721001209

1. Sr=5+0+2+0+1+0=8
2. S1=8*3=24
3. Sн=8+9+7+1+0+2=27
4. S=24+27=51
5. t=1
6. P=10-1=9 (совпадает с контрольной цифрой)

Изменим любую цифру кода, например 7 на 5.

Тогда

3. Sн=8+9+5+1+0+2=25
4. S=24+25=79
5. t=9
6. P=10-9=1, т.е. контрольная цифра говорит о чувствительности кода (она не совпала).

Важность этого типа кода определяется еще и тем, что ряд банков Республики Беларусь используют для счетов предприятий 13-разрядные коды типа EAN-13. Ошибка персонала предприятия при заполнении документов тогда легко вскрывается по контрольному разряду, и банк не выполняет перевод денег.

Идея скрыть некоторые элементы передаваемой информации или сам факт ее передачи и хранения оказалась плодотворной в создании сложных многоступенчатых систем защиты информации.

Многоступенчатость защиты информации выражается как в смене средств защиты информации по блокам, использовании разных ключей, поэтапном сочетании методов стеганографии и криптографии.

Компьютерная стеганография – это сокрытие сообщения или файла в другом сообщении или файле. Информация может быть в виде текста, изображения, звука или их сочетания. Для сокрытия хранимой или передаваемой информации используется контейнер – специально подобранная другая информация. Защищаемая информация встраивается в контейнер по заданным правилам так, чтобы на фоне контейнера она ничем не выделялась. Для сокрытия зашифрованной защищаемой информации применяется секретный стегоключ.

Часто в шифровании используется и **операция гаммирования**, когда по определенному закону перед шифрованием на открытые данные (обычно в двоичном виде) делается наложение гаммы – псевдослучайный последовательности ($D_г^i$). Процесс шифрования тогда содержит процедуру генерации гаммы шифра и ее наложении на исходный текст обратимым образом. Обычно гаммирование исходного двоичного текста выполняется путем его сложения с гаммой по модулю 2 ($\oplus$). **Процедура гаммирования характерна для блочного шифрования**, когда открытые данные разбиваются на блоки D_o^i одинаковый длины (чаще всего 64 бита). Каждый открытый блок D_o^i путем сложения с гаммой преобразуется в гаммированный блок $D_ш^i$ аналогичной длины, готовый для шифрования. Уравнение гаммирования для каждого блока i из набора k блоков тогда записывается так $D_ш^i = D_o^i \oplus D_г^i$. Обратная процедура на приемном конце сводится к повторной генерации гаммы по известному для принимающего закону. Тогда расшифрованный текст легко получается по формуле: $D_o^i = D_ш^i \oplus D_г^i$. Такой метод позволяет изменять гамму для каждого шифруемого блока случайным образом за счет генерации псевдослучайных чисел.

Для компьютерных продуктов характерна защита интеллектуальной собственности в форме ноу-хау, так как эти объекты пока не патентуются.

Частью системы правовой охраны промышленной собственности в Республике Беларусь является защита от недобросовестной конкуренции.

«Недобросовестная конкуренция – любые направленные на приобретение преимуществ в предпринимательской деятельности действия хозяйствующих субъектов, которые противоречат требованиям добросовестности и разумности и могут причинить или причинили убытки другим хозяйствующим субъектам - конкурентам либо нанести ущерб их деловой репутации».

Любые действия, направленные на ограничение или устранение конкуренции путем нарушения прав других хозяйствующих субъектов на свободную конкуренцию, а также нарушающие права и законные интересы потребителей, не допускаются:

– незаконное использование фирменного наименования, товарного знака, копирование внешнего вида товара другого хозяйствующего субъекта;

– введение в гражданский оборот товаров другого хозяйствующего субъекта с использованием собственных средств индивидуализации товара;

– неправомерные утверждения при осуществлении предпринимательской деятельности, способные дискредитировать хозяйствующий субъект, товары или предпринимательскую деятельность конкурента.

Объекты промышленной собственности охватывают результаты интеллектуальной деятельности, имеющие производственную направленность.

К **объектам промышленной собственности** относят изобретения, полезные модели, промышленные образцы, селекционные достижения, топологии интегральных микросхем, нераскрытую информацию.

Заключительные общие рекомендации.

При необходимости использования результатов в конкретных целях (в выполнении курсовой, дипломной, магистерской или другой работы, носящей исследовательский характер) полезно прибегнуть к дополнительному изучению литературы из списка источников [1-15]. Смысл их использования состоит в необходимости системной увязки вопросов защиты информации и интеллектуальной собственности с экономических и юридических позиций. Это необходимо при подготовке объектов для выхода на международные рынки, так как здесь решающим фактором становятся экономические и правовые вопросы: первые используются для оценки затрат на рыночное продвижение продукта, а вторые – для его защищенности (патентование объектов промышленной собственности, регистрация товарного знака, патентная чистота объекта и т.д.). Вторым важным объектом являются различные дистанционные операции в сетях ЭВМ (электронная коммерция и платежи между субъектами хозяйствования, выполнение дистанционных совместных работ и заказов).

Литература

1. Головко, В.А. Основы вычислительных систем: методическое пособие / В.А. Головко [и др.]. – Брест: Издательство УО «БрГТУ», 2013. – 148 с.

2. Основы искусственного интеллекта: учебно-методический комплекс / Л.П. Матюшков, В.А. Головко, В.Н. Шуть. – Брест: БрГТУ, 2010. – 116 с.

3. Положение о коммерческой тайне (утв. СМ РБ 06.11.1992 №-670)

4. Алиев, Ю.А. Алгоритмизация и языки программирования Pascal, C++, Visual Basik: учебно-справочное пособие / Ю.А. Алиев, О.А. Козлов.– М.: Финансы и статистика, 2002. – 328 с.

5. Информационные технологии. Стандарт электронной цифровой подписи: предварительный государственный стандарт Республики Беларусь СТБ П 34.101.25-2008.

6. Математические и компьютерные основы криптографии: уч. пособ / Ю.С. Харин [и др.]. – Мн.: Новое знание, 2003.– 382 с.

7. Экономическая безопасность предприятия / В.Б. Зубик [и др.]. – Мн.: Выш. школа, 1998. – 391 с.

8. Головко, В.А. Нейронные сети: обучение, организация и применение: учебное пособие для вузов / В.А. Головко – М.: ИПРЖР, 2001. – 256 с.

9. Головко, В.А. Основы защиты информации и управления интеллектуальной собственностью: учебно-методический комплекс / В.А. Головко, Л.П. Матюшков. – Брест: Изд-во «БрГТУ», 2011.–76 с.

10. Корнеев, В.Г. Базы данных. Интеллектуальная обработка информации / В.Г.Корнеев [и др.]. – М.: Нолидж, 2001. – 496 с.

11. Макаров, Е.Г. Инженерные расчеты в Matcad-14 / Е.Г. Макаров. – СПб.: Питер, 2007 – 592 с.

12. Мацукевич, В.В. Основы управления интеллектуальной собственностью. Учебно-методический комплекс / В.В. Мацукевич, Л.П. Матюшков.– 2-е изд. – Минск: Выш. шк., 2013.– 224 с.

13. Об электронном документе и электронной цифровой подписи. Закон Республики Беларусь от 28 декабря, 2009 года, №113-З – 10 с.

14. Матюшков, Л.П. Перспективы информационных технологий в развитии дистанционных рабочих мест и коммерческих операций «Вучоныя запіскі БрДУ» Брест: БрДУ, 2006. – Т. 2. – Ч. 1. – С. 107-115.

15. Банкаускі веснік. Інфармацыйны выпуск. – Мінск: 2004. – № 18/275.

Содержание

Учебное издание

Составители:
Матюшков Леонид Петрович
Головко Владимир Адамович

Традиционные и интеллектуальные информационные технологии

Методические указания к выполнению практических занятий и лабораторных работ для студентов специальности 1-40 03 01 «Искусственный интеллект»

Ответственный за выпуск: Матюшков Л.П.
Редактор: Боровикова Е.А.
Компьютерная верстка: Соколюк А.П.
Корректор: Никитчик Е.В.

Подписано к печати 13.03.2014 г. Формат 60x84 $^{1}/_{16}$. Гарнитура Times New Roman. Бумага «Снегурочка». Усл. п. л. 1,86. Уч. изд. 2,0. Заказ № 213. Тираж 60 экз. Отпечатано на ризографе учреждения образования «Брестский государственный технический университет». 224017, г. Брест, ул. Московская, 267.