Министерство науки и высшего образования Российской Федерации
Тольяттинский государственный университет

Г.А. Тырыгина

ИСТОРИЯ И МЕТОДОЛОГИЯ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Электронное учебное пособие

ISBN 978-5-8259-1361-2

УДК 51(091)+004.056.55(091)
ББК 22.1г(0)+32.81г(0)

Рецензенты:
канд. физ.-мат. наук, доцент, заведующая кафедрой
«Математические и естественно-научные дисциплины»
Поволжского государственного университета сервиса
Т.В. Никитенко;
канд. физ.-мат. наук, доцент кафедры «Прикладная математика
и информатика» Тольяттинского государственного университета
О.В. Лелонд.

Тырыгина, Г.А. История и методология прикладной математики и информатики : электронное учебное пособие / Г.А. Тырыгина. – Тольятти : Изд-во ТГУ, 2023. – 1 оптический диск. – ISBN 978-5-8259-1361-2.

В учебном пособии представлены некоторые темы по дисциплине «История и методология прикладной математики и информатики» с учетом требований ФГОС ВО.

Предназначено для студентов, обучающихся по направлению подготовки 01.04.02 «Прикладная математика и информатика» (направленность (профиль) «Математическое моделирование») очной формы обучения.

Текстовое электронное издание.

Рекомендовано к изданию научно-методическим советом Тольяттинского государственного университета.

Минимальные системные требования: IBM PC-совместимый компьютер: Windows XP/Vista/7/8/10; PIII 500 МГц или эквивалент; 128 Мб ОЗУ; SVGA; CD-ROM; Adobe Acrobat Reader.

Учебное издание

Тырыгина Галина Алексеевна

ИСТОРИЯ И МЕТОДОЛОГИЯ
ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Редактор *Е.А. Держаева*
Технический редактор *Н.П. Крюкова*
Компьютерная верстка: *Л.В. Сызганцева*
Художественное оформление,
компьютерное проектирование: *Г.В. Карасева*

При оформлении пособия использовано изображение
от rawpixel.com на Freepik

Дата подписания к использованию 05.10.2023.
Объем издания 1,9 Мб.
Комплектация издания: компакт-диск, первичная упаковка.
Тираж 50 экз. Заказ № 1-18-22.

Издательство Тольяттинского государственного университета
445020, г. Тольятти, ул. Белорусская, 14,
тел. 8 (8482) 44-91-47, www.tltsu.ru

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Учебное пособие «История и методология прикладной математики и информатики» предназначено для студентов, обучающихся по направлению подготовки высшего образования 01.04.02 «Прикладная математика и информатика» и соответствует содержанию учебного материала ФГОС ВО и рабочей программе дисциплины.

В данном учебном пособии первая и вторая главы посвящены истории развития криптографических методов защиты информации, в третьей главе рассматриваются вопросы, связанные с развитием теории приближения функций. Библиографический список содержит источники только по указанным темам.

Предложенные в пособии варианты описания исторического развития указанных выше тем могут быть использованы студентами при их работе над рефератами по другим темам по истории и методологии прикладной математики и информатики.

ВВЕДЕНИЕ

Математика отвечает потребностям общества. Как правило, различные математические теории связаны с решением практических задач, стоящих перед человечеством. В истории развития математики можно проследить взаимосвязь *теоретического и прикладного направлений,* их единство и взаимообогащение. Для систематизации математического знания, полученного в ходе исторического развития, учеными предлагались различные варианты периодизации. А.Н. Колмогоров предложил рассматривать четыре периода.

1. Зарождение математики. Это период накопления математических знаний, продолжающийся до VI–V вв. до н. э.
2. Период элементарной математики. Он продолжается от VI–V вв. до н. э. до XVI в. н. э. включительно и характеризуется изучением постоянных величин.
3. Период создания математики переменных величин. Характеризуется введением переменных величин в аналитической геометрии Декарта и созданием дифференциального и интегрального исчисления И. Ньютоном и Г.В. Лейбницем.
4. Период современной математики.

На начальном этапе развивалось прикладное направление математики: возникали различные системы счета, геометрические представления, велись астрономические наблюдения. Это характерно для древних цивилизаций Египта и Мексики. В Древней Греции после накопления результатов решения практических задач началось активное развитие теоретической математики. Рост торговых городов в эпоху Возрождения способствовал развитию математики, ее прикладной ветви. В XVI веке ученые-алгебраисты были медиками, архитекторами, географами, купцами. С развитием капитализма в работах Галилея, Кеплера, Ньютона и др. теоретические результаты непосредственно определялись прикладными задачами. К середине XIX столетия математика состояла из большого числа плохо связанных между собой частей, доступ к которым был понятен лишь узким специалистам. Для успешного развития математики потребовалась систематизация накопленного материала. В этот период большее внимание уделялось теоретическому направлению. В работах

Кантора по теории множеств, Вейерштрасса по теории функций и ряда других математиков были выработаны основные понятия, общие термины. В XVIII веке в работах Лагранжа и Лапласа по механике – синтез практической и теоретической сторон математики. В последующих веках в работах математиков также можно проследить синтез практической и теоретической сторон при создании новых математических теорий и их применении. Более подробно вопросы развития математики можно найти в работах [36–54].

Глава 1. ИСТОРИЯ РАЗВИТИЯ КРИПТОГРАФИИ

Наука, занимающаяся вопросами безопасной связи (т. е. посредством зашифрованных сообщений) называется **криптологией** (*kryptos* – тайный, *logos* – наука). Она в свою очередь разделяется на два направления: криптографию и криптоанализ [1].

Криптография – наука о создании безопасных методов связи, о создании стойких (устойчивых к взлому) шифров. Она занимается поиском математических методов преобразования информации [2].

Криптоанализ посвящен исследованию возможности чтения сообщений без знания ключей, т. е. связан непосредственно со взломом шифров. Люди, занимающиеся криптоанализом и исследованием шифров, называются *криптоаналитиками*.

Шифр – совокупность обратимых преобразований множества открытых текстов (т. е. исходного сообщения) во множество зашифрованных текстов, проводимых с целью их защиты. Конкретный вид преобразования определяется с помощью ключа шифрования.

Определим еще несколько понятий, которые необходимо усвоить, чтобы чувствовать себя уверенно. Во-первых, *зашифрование* – процесс применения шифра к открытому тексту. Во-вторых, *расшифрование* – процесс обратного применения шифра к зашифрованному тексту. И в-третьих, **дешифрование** – попытка прочесть зашифрованный текст без знания ключа, т. е. взлом шифротекста или шифра. Здесь следует подчеркнуть разницу между расшифрованием и дешифрованием. Первое действие проводится законным пользователем, знающим ключ, а второе – криптоаналитиком или мощным хакером [24].

Криптографическая система – семейство преобразований шифра и совокупность ключей (т. е. алгоритм + ключи). Само по себе описание алгоритма не является криптосистемой. Только дополненное схемами распределения и управления ключами, оно становится системой. Примеры алгоритмов – описания DES, ГОСТ 28147–89. Дополненные алгоритмами выработки ключей, они превращаются в криптосистемы. Как правило, описание алгоритма шифрования уже включает в себя все необходимые части.

1.1. Криптография древнего периода

Криптография возникла вместе с письменностью. В исторических документах древних цивилизаций Индии, Египта, Месопотамии имеются сведения о системах и способах составления шифрованного письма. Так, в древнеиндийских рукописях содержится изложение 64 способов преобразования текста. Среди них написание знаков не по порядку, а вразброс по некоторому правилу. Многие из приводимых способов следует рассматривать как криптографические, то есть обеспечивающие секретность переписки. Приведена система замены букв. Упоминается, что тайнопись является одним их 64 искусств, которым следует владеть как мужчинам, так и женщинам [11].

Более достоверные сведения о применяемых системах шифров относятся к периоду возникновения государств Древней Греции. В Спарте в VI–V веке до нашей эры существовала хорошо развитая криптография. К этому времени относятся описания двух известных приборов для шифрования – сцитала и таблица Энея, которые осуществляют перестановку букв в тексте и замену букв открытого текста отрезками на прямой. Эней в сочинении «Об обороне укрепленных мест» описывает так называемый книжный шифр, Полибий описывает систему шифра, называемую «квадрат Полибия», представляющую собой замену каждой буквы парой чисел – координатами буквы в квадрате 5×5, в котором написаны буквы алфавита. Юлий Цезарь в книге «Записки о Галльской войне» описывает шифр, в котором буквы заменяются в соответствии с подстановкой, в которой каждая буква сдвинута на три позиции вправо [14].

В математике этого периода накапливается материал, относящийся к началам арифметики и геометрии. В этот период появляются правила вычисления площади треугольника и трапеции, объемы пирамиды с квадратным основанием, правила решения простейших квадратных уравнений, теорема Пифагора и формула для суммы арифметической прогрессии [1].

Потребителями криптографии в этот период являются структуры административной и религиозной власти. Плутарх сообщает, что жрецы хранили тексты прорицателей в зашифрованном виде [33].

Э. Шюре в книге «Великие посвященные» сообщает, что с большим трудом добыл Платон один из манускриптов Пифагора, который записывал свое эзотерическое учение только тайными знаками и под различными символами. Там же отмечается, что Аристотель получил от Платона шифрованный текст Пифагора. Платону принадлежит метод доказательства от противного, а Аристотель заложил основы теории логического вывода и теории доказательств. Аристотелю приписывается метод дешифрования шифра сцитала.

1.2. Криптография Арабского мира

В период расцвета арабских государств (VIII век н. э.) криптография получила новое развитие. Слово «шифр» – арабского происхождения, так же как и слово «цифра». В 855 году появляется «Книга о большом стремлении человека разгадать загадки древней письменности», в которой приводятся описания систем шифров, в том числе и с применением нескольких шифралфавитов. В 1412 году издается 14-томная энциклопедия, содержащая обзор всех научных сведений, – «Шауба аль-Аша» (составитель – Шехаб аль-Калкашанди). В данной энциклопедии содержится раздел о криптографии, в котором приводятся описания всех известных способов шифрования. В этом разделе есть упоминание о криптоанализе системы шифра, который основан на частотных характеристиках открытого и шифрованного текста. Приводится частота встречаемости букв арабского языка на основе изучения текста Корана.

Что касается математики Арабского мира, то следует упомянуть следующие выдающиеся достижения. Сочинение Мухаммеда бен Мусы аль-Хорезми (IX век) по правилам арифметики в позиционной системе счисления, от названия которого появились два термина: «алгебра» и «алгоритм». Трактат по тригонометрическим функциям аль-Баттани (IX век). Вычисление числа пи с 17 десятичными знаками (около 1427 г.) аль-Каши, сотрудником Улугбека.

1.3. Криптография в эпоху Возрождения (XIV–XVI века)

До эпохи Возрождения имеется мало сведений о применяемых шифрах. Известен ряд значковых шифров, в которых буквы открытого текста заменяются на специальные знаки, например шифр Карла Великого. Известен так называемый еврейский шифр, в котором замена букв осуществляется по подстановке, в которой нижняя строка образуется так: алфавит разбивается на две половины. Буквы второй половины пишутся под буквами первой половины в обратном порядке. Аналогично поступают с остальными буквами [9].

В эпоху Возрождения в итальянских городах-государствах расцветают науки и ремесла. Шифры применяются не только государственной или церковной властью, но и учеными для защиты приоритета научных открытий (Галилей). В XIV веке появляется книга Чикко Симонетти, сотрудника канцелярии папской курии. В этой книге описаны шифры замены, в которых гласным буквам ставятся в соответствие несколько знаков с целью выравнивания частот букв в шифротексте. Дано описание лозунгового шифра, в котором замена букв определяется так: под алфавитом пишутся различные буквы лозунга в порядке появления, а затем буквы, не появившиеся в лозунге. В XV веке появляется книга Габриэля де Лавинда, секретаря папы Климента VII, «Трактат о шифрах», в которой дается описание шифра пропорциональной замены. Шифр обеспечивает замену букв несколькими символами, пропорционально встречаемости букв в открытом тексте. Дается рекомендация заменять имена, должности, географические названия специальными знаками. В этот период в Милане применяется шифр «Миланский ключ», представляющий собой значковый шифр пропорциональной замены [7].

В 1466 году знаменитый архитектор и философ Леон Альберти представил трактат о шифрах в папскую канцелярию. В трактате рассматриваются различные способы шифрования, в том числе маскировка открытого текста в некотором вспомогательном тексте. Работа завершается собственным шифром, который он назвал шифром, достойным королей. Это был многоалфавитный шифр, реализованный в виде шифровального диска.

Суть заключается в том, что в данном шифре используется несколько замен в соответствии с ключом. Позднее Альберти изобрел код с перешифровкой. Данное изобретение значительно опередило свое время, поскольку данный тип шифра стал применяться в странах Европы лишь 400 лет спустя [14].

В 1518 году в развитии криптографии был сделан новый шаг благодаря появлению в Германии первой печатной книги по криптографии. Аббат Иоганнес Тритемий, настоятель монастыря в Вюрцбурге, написал книгу «Полиграфия», в которой дается описание ряда шифров. Один из них развивает идею многоалфавитной замены. Шифрование осуществляется так: заготавливается таблица замены, в которой первая строка есть алфавит, вторая строка есть алфавит, сдвинутый на один шаг, и т. д. При шифровании первая буква открытого текста заменяется на букву, стоящую в первой строке, вторая буква – на букву, стоящую во второй строке, и т. д. В 1553 году в Италии вышла небольшая книга «Шифр синьора Белазо». Об авторе Джованни Белазо известно мало. Его вклад заключается в следующем. Он предложил использовать слово или группу слов, назвав это «паролем», выписывая его над (под) открытым текстом. Буква пароля означает номер применяемой замены к букве открытого текста. В начале XVI в. Маттео Арженти, криптограф папской канцелярии, изобрел код, представляющий собой шифр замены, в котором заменяются буквы, слоги, слова и целые фразы. Необходимым количеством словарных величин в коде считалось 1200. В это же время появляется и числовой код [30].

Следующий шаг в развитии криптографии был сделан Джованни Порта, известным итальянским естествоиспытателем. В 1563 году он написал книгу «О тайной переписке», в которой приводится описание всех известных систем шифров. Дается также описание биграммного шифра, в котором осуществляется замена пар букв. Порта предвосхитил то, что называют методом вероятного слова, и приводит примеры списков вероятных слов из различных областей. Примерно в то же время итальянский математик и философ Джероламо Кардано, автор многочисленных книг по различным вопросам, написал книгу «О тонкости вещей», в которой есть часть,

посвященная криптографии. Он предложил использовать открытый текст в качестве ключа и шифр, называемый решеткой Кардано. Кроме того, Кардано дает «доказательства» стойкости шифров, основанные на подсчете числа ключей.

В том же XVI в. был сделан еще один существенный шаг в развитии криптографии. Блез де Виженер, французский посол в Риме, познакомился там с трудами по криптографии и в 1585 году написал книгу «Трактат о шифрах», в которой он излагает основы криптографии. Ему принадлежит мысль «Все вещи в мире представляют собой шифр. Вся природа является просто шифром и секретным письмом» [15]. Эту мысль повторил позднее Блез Паскаль и в наше время Норберт Винер. Предложение Виженера во многом развивает идею Кардано о применении открытого или шифрованного текста в качестве ключа.

Прогресс в математике в этот период характеризуется трудами Леонардо Фибоначчи, в которых излагается арифметика, алгебра и геометрия. Для вычислений используется сходимость геометрической прогрессии. Н. Орем установил расходимость гармонического ряда, строгое доказательство этого появится только в XVII веке. Кардано при решении уравнений третьей степени вводит отрицательные и мнимые корни и устанавливает известную формулу Кардано. Алгебра получает развитие благодаря Ф. Виету, который установил связь коэффициентов алгебраических уравнений и корней (формула Виета). Он же начал использовать буквенные обозначения для коэффициентов уравнений, до него это использовалось лишь для корней. Ф. Виет привлекался к дешифровальной работе при дворе Генриха IV и успешно дешифровал переписку испанского короля Филиппа II. Отметим, что великий ученый и художник эпохи Возрождения Леонардо да Винчи (1452–1519) владел криптографией и пользовался ею, в частности в своих рукописях.

1.4. Криптография в XVII–XVIII веках

XVII век называют эрой «черных кабинетов», поскольку в этот период создаются дешифровальные службы. Так, в Англии Оливер Кромвель создает «Интеллиженс сервис» – разведывательную службу, в которой появится дешифровальное отделение. В середине XVII века к дешифровальной работе привлекается известный математик Джон Валлис (1616–1703). Он является автором фундаментального труда «Арифметика бесконечного» (1655). Хорошо известна формула Валлиса, дающая представление числа пи в виде бесконечного произведения. Во Франции по предложению кардинала Ришелье создается дешифровальное отделение, которое возглавил Антуан Россиньоль. Россиньолю принадлежит доктрина: стойкость военного шифра должна быть такой, чтобы обеспечить секретность донесения в течение срока, необходимого для выполнения приказа. Стойкость дипломатического шифра должна обеспечивать секретность в течение нескольких десятков лет. Сам Ришелье оставил след в криптографии благодаря известному шифру Ришелье, который представляет собой шифр перестановки: открытый текст разбивается на отрезки, а внутри каждого отрезка буквы переставляются в соответствии с фиксированной перестановкой [10].

Россиньоль разработал дипломатический шифр, представляющий собой слогово-словарный код на 600 величин [10].

В Германии в это время также создается дешифровальное отделение, которое возглавляет граф Гронсфельд. Ему принадлежит усовершенствование шифра Виженера, заключающееся в том, что вместо буквенного лозунга применяется цифровой, а значение цифры в лозунге означает число шагов, на которое надо сдвинуть букву открытого текста вправо по алфавиту в стандартной записи. Данный шифр получил широкое распространение благодаря простоте применения. Таким образом, дешифровальные подразделения становятся обычным делом. Что касается шифров, то в этот период применяются в основном коды различной степени сложности. Из других шифров следует упомянуть масонский шифр, представляющий собой оригинальный значковый шифр, в котором из написания алфавита на двух крестах – прямом и косом – извлекались

знаки для замены букв. Наполеон во время своих походов использовал шифры, являющиеся вариантами шифра Россиньоля и представляющие собой код на 200 шифровеличин.

Криптография в России развивалась по пути христианских стран. Датой появления криптографической службы следует считать 1549 год (царствование Ивана IV), с момента образования Посольского приказа, в котором имелось цифирное отделение. Используемые шифры – такие же, как в западных странах, – значковые, замены, перестановки. Петр I полностью реорганизовал криптографическую службу, создав Посольскую канцелярию. В знаменитом деле царевича Алексея в обвинительных материалах фигурировали и цифирные азбуки [28].

Математика XVII–XVIII веков получает существенное и качественно новое развитие. Н. Бурбаки называют этот период «героической эпохой». Назовем только некоторых авторов открытий. Изобретатель логарифмов – Джон Непер, шотландский математик, его «Описание удивительной таблицы логарифмов» было издано в 1614 году. Декарт Рене, французский математик, заложил основы аналитической геометрии. Его фундаментальный труд «Геометрия» вышел в 1637 году [19].

Блез Паскаль (1623–1662), французский физик и математик. Получил ряд результатов по комбинаторике (треугольник Паскаля и геометрии (теорема Паскаля). Открыл метод доказательства по индукции.

Английский физик и математик Исаак Ньютон (1643–1727) и немецкий философ и математик Готфрид Лейбниц (1646–1716) разработали дифференциальное и интегральное исчисление. Нет данных о привлечении этих математиков к шифровальной работе, но известно, что некоторые из них владели криптографией (Паскаль, Ньютон, Лейбниц). Увлекался криптографией и знаменитый английский философ Ф. Бэкон (1561–1626), которому принадлежит идея двоичного кодирования.

Якоб Бернулли (1655–1705), швейцарский математик, заложил основы теории вероятностей, ему принадлежит известная теорема Бернулли, являющаяся важным частным случаем закона больших чисел. Его книга «Искусство предположений» вышла в 1713 году.

В развитии математики в России большую роль сыграла «Арифметика» Л.Ф. Магницкого (издана в 1703 году), которую М.В. Ломоносов назвал «вратами учености». Книга представляла собой свод математических сведений на тот период.

К дешифровальной работе в России был привлечен известный математик Христиан Гольбах (1690–1764), приехавший в Россию в 1725 году. В 1727 в Россию приезжает Леонард Эйлер (1707–1783), который принимал участие в разработке шифров. Ему принадлежат исследования по перечислению и построению латинских квадратов, то есть шифров многоалфавитной замены. В области математики Эйлер существенно обогатил все разделы математического анализа и заложил основы новых математических дисциплин (теория чисел, вариационное исчисление, уравнения с частными производными, теория функций комплексного переменного). Дешифровальной работой занимался Франц Эпинус (1724–1802), живший в России с 1757 года, известный математик и физик, изучавший с помощью математических методов электромагнитные явления.

Таким образом, в XVII–XVIII веках в математике закладываются основы аппарата, применяемого в криптографии для анализа шифров и дешифрования [10].

Основным средством для шифрования становятся коды.

1.5. Криптография в XIX веке

В 1819 году во Франции выходит энциклопедия, в которой приведены известные к тому времени системы шифров и методы дешифрования простейших шифров. В 1844 году С. Морзе изобрел телеграф. В России телеграф был изобретен П.Л. Шиллингом в 1832 году. Шиллингу также принадлежит изобретение биграммного шифра. В Англии изобретение биграммного шифра приписывается министру почт при королеве Виктории Леону Плейферу. Изобретение телеграфа оказало существенное влияние на криптографию. Сразу же был опубликован коммерческий код под названием «Словарь для тайной корреспонденции; приспособлен для применения на электромагнитном телеграфе Морзе». Развитие коммерческих кодов повлияло и на развитие дипломатических

кодов. Специалисты пришли к пониманию, что необходима иерархия в шифрованной связи. Для каждого уровня иерархии требуется своя система шифра. Возрастание скорости передачи потребовало возрастания скорости шифрования. Появляются различные механические устройства для зашифрования. Среди них шифратор Т. Джефферсона и шифратор Ч. Уитстона. Устройство Уитстона демонстрировалось на парижской выставке 1876 года [20].

Отметим, что в викторианской Англии к дешифровальной работе был привлечен математик Ч. Беббидж, известный изобретением вычислительной машины.

В 1863 году офицер прусской армии майор Фридрих Казисский опубликовал книгу под названием «Искусство тайнописи и дешифрования», в которой был изложен метод вскрытия многоалфавитного шифра с повторяющимся лозунгом на примере шифра Виженера, который ранее считался недешифруемым. Казисский предложил метод статистического определения числа букв в лозунге, который основан на следующей идее: повторяемость букв в лозунге вместе с повторяемостью букв в открытом тексте дает повторяемость букв в шифрованном тексте. Автор пришел к выводу, что расстояние между повторениями в шифротексте будут равны или кратны периоду лозунга, то есть его длине. После определения длины лозунга шифротекст разбивается на отрезки, равные длине лозунга, и исходная задача сводится к дешифрованию простой замены. Данный метод дешифрования стал называться методом Казисского.

В 1883 году появился крупный научный труд под названием «Военная криптография», его автор Огюст Керкгоффс, преподаватель иностранных языков и математики во Франции.

В данной книге проводится сравнительный анализ шифров. Задача автора – сформулировать требования к шифрам применительно к использованию новых средств связи. Он делает вывод, что практический интерес представляют те шифры, которые остаются стойкими при интенсивной переписке [29].

Другой его вывод: только криптоаналитики могут судить о качестве шифра. Керкгоффс впервые делает различие между секретностью шифросистемы и секретностью ключа. Он вводит требование

секретности по ключу и не требует секретности системы. Это требование сохраняет свое значение и в современной криптографии [20].

Важное событие в криптографии было связано с именем французского офицера Э. Базери, который отрицательно относился к официальным шифрам и предложил несколько собственных систем. Одна из них – это по сути шифратор Джефферсона [4].

Военное руководство отказалось его использовать, сославшись на то, что нет гарантий стойкости этого шифра. В 1901 году Э. Базери издал книгу «Раскрытые секретные шифры», в которой показана возможность дешифрования «Великого шифра Россиньоля».

С 80-х годов XIX века криптография во всех ведущих государствах считается наукой, ее изучают в военных академиях. Для шифрования применяются коды с перешифровкой. Созданы и используются механические устройства для шифрования. Нет свидетельств, относящихся к данному периоду, о привлечении крупных математиков для криптографической работы [15].

Математика XIX века характеризуется революционными открытиями, ломающими привычные представления. В первую очередь следует назвать открытие Н.И. Лобачевским неевклидовой геометрии. Его труд «О началах геометрии» был напечатан в журнале «Казанский вестник» в 1829 году. Сходные результаты были получены Я. Больяи в 1832 году. Б. Больцано и позднее К. Вейерштрасс строят пример непрерывной функции, не имеющей конечной производной ни в одной точке. Но это является только началом открытий патологических явлений в математике.

Г. Кантор разработал теорию бесконечных множеств и открыл первые парадоксы теории множеств. Затем аналогичные парадоксы были открыты Бурали-Форти, Ришаром, Расселом. Сложившуюся ситуацию называют кризисом математики. Знаменитый математик А. Пуанкаре в одном из мемуаров спрашивает, как интуиция может обмануть нас до такой степени. Такое положение дел подтолкнуло к изучению оснований математики, развитию формальных языков и аксиоматического метода. Началась арифметизация математики, то есть применялся метод, при котором рассуждение о математических объектах сводится к рассуждению о натуральных числах.

На математическом конгрессе 1900 года в Париже известный немецкий математик Д. Гильберт, формулируя актуальные проблемы математики, на второе место в списке проблем ставит вопрос о непротиворечивости арифметики, а на первое место – задачу Кантора о мощности континуума [13].

Заметим, что под восьмым номером в списке проблем Д. Гильберта стоит проблема простых чисел, в которой, в частности, цитируется гипотеза Римана о распределении нулей дзета-функции Римана. Данная проблема, как показали современные исследования, имеет большое значение для криптографии в связи с построением алгоритмов факторизации чисел.

1.6. Криптография в XX веке

XX век – век двух мировых войн, научно-технического прогресса, социальных потрясений и передела государственных границ.

В этом веке криптография стала электромеханической, затем электронной. Это означает, что основными средствами передачи информации стали электромеханические и электронные устройства. Это преобразило всю криптографию, поскольку расширились возможности доступа к шифрованному тексту и появились возможности влияния на открытый текст.

Поскольку главным шифросредством во время Первой мировой войны были коды, которые не удавалось сохранить от компрометации, то участники военных действий взаимно читали переписку друг друга. В полевых условиях применялись: решетка Кардано (Германия и Австро-Венгрия), шифр Плейфера (Англия), шифр двойной перестановки (Франция), шифр гаммирования цифровой гаммой (Россия). С применением шифров связан ряд трагических событий, из которых упомянем лишь разгром двух русских армий – Ренненкампфа и Самсонова в Восточной Пруссии в августе 1914 года, который произошел из-за плохой организации шифросвязи и вынужденной связи между этими армиями по радио без всякого шифра.

Война преобразила криптографию. В связи с применением радио для управления войсками расширились возможности добычи шифротекста. В этот период получили развитие методы дешиф-

рования, основанные на парах открытых и шифрованных текстов, на шифротекстах, полученных на одном ключе, на использовании вероятных ключей. Находкой для криптографов было использование в качестве лозунгов пословиц, поговорок, патриотических призывов. В математическом плане получили развитие вероятностно-статистические методы, использующие частоту знаков, биграмм, триграмм и т. д. [13].

Другое новшество этого периода – специализация в криптографической деятельности. Появляются группы по дешифрованию кодов и по дешифрованию полевых шифров, по добыче перехвата, обработке информации, полученной из открытых и агентурных источников, и т. д. [13].

Между мировыми войнами во всех ведущих странах появляются электромеханические шифраторы. Они были двух типов – на коммутационных дисках, или роторах, и на цевочных дисках. Примером первого типа является известная шифромашина «Энигма», которой были оснащены германские сухопутные войска. Пример второго типа – американская шифромашина М-209. Коммутационный диск представляет собой полый диск с нанесенными с двух сторон контактами, соответствующими алфавитам открытого и шифрованного текста, причем они соединены между собой по некоторой подстановке, называемой коммутацией диска. Эта коммутация определяет замену букв в начальном угловом положении. При изменении углового положения диска изменяется соответствующая замена на сопряженную подстановку. Шифратор представляет собой устройство из коммутационных дисков и механизма изменения их угловых положений. Шифратор «Энигма» состоял из 4 коммутационных дисков, которые изменяли свои угловые положения по принципу счетчика. Она имела несколько модификаций. Одну идею в криптографическом отношении можно считать революционной – каждый диск дважды участвовал в шифровании, что усложняло анализ шифра.

Шифромашина М-209 состояла из 6 колес размером 26, 25, 23, 21, 19, 17, каждое из которых имело выступы и по окружности. Эта шестимерная комбинация выступов (их число – 64) с помощью механического устройства превращалась в число, на которое сдви-

гается буква открытого текста. Изменение угловых положений дисков осуществлялось равномерным их вращением. Ясно, что шифратор реализует шифр гаммирования.

Советский Союз производил шифромашины обоих названных типов.

Таким образом, перед Второй мировой войной все ведущие страны имели на вооружении электромеханические шифросистемы, обладающие высокой скоростью обработки информации и высокой стойкостью. Считалось, что применяемые системы недешифруемы и наступил конец криптографии. Впоследствии в ходе войны это мнение было опровергнуто, и все участники военных действий имели криптографические успехи. Поучительная история дешифрования «Энигмы» описана у Д. Кана и других авторов.

Ограничимся упоминанием теоретического открытия, оказавшего существенное влияние на развитие криптографии. Речь идет о работе американского инженера К. Шеннона «Теория связи в секретных системах», выполненной в 1945 году (опубликованной в 1949 году), и работе советского ученого-радиотехника В.А. Котельникова «Основные положения автоматической шифровки», датированной 19 июня 1941 года. В них были сформулированы и доказаны математическими средствами необходимые и достаточные условия недешифруемости системы шифра. Они заключаются в том, что получение противником шифротекста не изменяет вероятностей используемых ключей. При этом было установлено, что единственным таким шифром является так называемая лента одноразового использования, когда открытый текст шифруется с помощью случайного ключа такой же длины. Это обстоятельство делает абсолютно стойкий шифр очень дорогим в эксплуатации.

Упомянем также об участии математиков в криптографической работе в этот период. В Англии во время войны к криптографической работе был привлечен А. Тьюринг, известный работами по формализации концепции вычислимости и разрешимости, автор машины Тьюринга. В США – С. Кульбак, крупный специалист по математической статистике, в Советском Союзе – математики А.А. Марков и А.О. Гельфонд. А.А. Марков известен работами по

теории алгоритмов, автор теории нормальных алгоритмов, которые сейчас называются алгоритмами Маркова. А.О. Гельфонд – специалист по теории чисел, известный решением седьмой проблемы Гильберта о трансцендентности степеней алгебраических чисел.

Начиная с 50-х годов криптография становится «электронной». Это означает широкое применение средств электронной техники для построения систем шифров и их исследования. Возможности применения электронной памяти позволили осуществлять обработку открытых текстов целыми отрезками (блоками), и это вызвало применение так называемых блочных шифров. С 70-х годов сфера применения криптографии начинает расширяться, криптография становится гражданской отраслью. Это означает, что криптографические средства начинают применяться для защиты коммерческой информации. Для этих целей в США в 1978 году был принят стандарт шифрования данных DES, который является блочным шифром с длиной блока 64 бит. В настоящее время все развитые страны имеют свои стандарты шифрования. Разработан криптографический алгоритм IDEA, который рассматривается в качестве кандидата для международного стандарта шифрования.

В 70-х годах американские математики Диффи и Хеллман предложили использовать так называемые системы с открытыми ключами, в которых нет канала для распространения ключей, но есть возможность двустороннего обмена информацией между отправителем и получателем. Фиксированная процедура такого обмена позволяет выработать общий секретный ключ. В этот период были предложены несколько систем с открытыми ключами. Среди них – система RSA, названная так по первым буквам ее авторов – Ривест, Шамир, Адлеман. В RSA открытые сообщения кодируются натуральными числами, а операция шифрования заключается в возведении в степень числа, представляющего открытый текст, и в приведении полученного числа по некоторому модулю. Дешифрование данной системы представляет собой известную математическую задачу «дискретное логарифмирование», для которой к настоящему моменту не найдено эффективных алгоритмов.

Другая система шифра – система Меркля – Хеллмана – основана на известной математической задаче о рюкзаке, заключающейся в представлении натурального числа в виде суммы чисел из множества заданных. Данная проблема относится к классу NP-полных проблем, что соответствует ее труднорешаемости [16].

Данные идеи оказались плодотворными. Во-первых, они расширили область средств, применяемых для обоснования шифров. Во-вторых, способствовали притоку математиков к решению криптографических проблем. В-третьих, привели к возникновению новых направлений криптографии. Например, процедура обмена информацией при выработке общего ключа привела к формированию понятия криптографического протокола. В-четвертых, они привели к появлению новых направлений в дискретной математике. Например, возникло понятие однонаправленной функции, для которой имеется простой алгоритм вычисления значения функции, но сложно вычисляется значение аргумента по значению функции. Для криптографических применений это понятие трансформировано в понятие односторонней функции с секретом. Хотя в настоящее время существование односторонних функций не доказано, имеется ряд кандидатов для этого, которые используются для построения систем шифров.

В заключение два слова о будущем криптографии. Ее роль будет возрастать в связи с расширением ее областей приложения (цифровая подпись, аутентификация и подтверждение подлинности и целостности электронных документов, безопасность электронного бизнеса, защита информации, передаваемой через Интернет, и др.). Знакомство с криптографией потребуется каждому пользователю электронных средств обмена информацией, поэтому криптография в будущем станет «второй грамотностью» наравне с владением компьютером и информационными технологиями.

1.7. Стеганография

Стеганогра́фия (в пер. с греч. «тайнопись») – это наука о скрытой передаче информации путем сохранения в тайне самого факта передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование. Стеганография не заменяет, а дополняет криптографию. Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение к тому же зашифровано, то оно имеет еще один, дополнительный уровень защиты.

Можно выделить три раздела стеганографии:

1) классическая стеганография – включает все «некомпьютерные методы», например запись на боковой стороне колоды карт, расположенных в условленном порядке, акростихи, трафареты, которые, будучи положенными на текст, оставляют видимыми только значащие буквы;

2) компьютерная стеганография – направление классической стеганографии, основанное на особенностях компьютерной платформы и использования специальных свойств компьютерных форматов данных, например использование регистра букв, пробелов, специфики файловых систем;

3) цифровая стеганография – направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты в совокупности с некоторыми искажениями этих объектов.

Используется избыточность аудио- и визуальной информации.

Выводы

В данной главе представлен краткий обзор развития методов защиты информации с древних веков до наших дней. Рассмотрены методы защиты информации в Древнем мире, в эпоху Возрождения. Описаны подходы к изучению криптографических вопросов в XVII–XX веках.

Контрольные вопросы

1. Охарактеризуйте методы криптографии в Древнем мире.
2. Охарактеризуйте методы криптографии в Арабском мире.
3. Охарактеризуйте методы криптографии в эпоху Возрождения (XIV–XVI вв.).
4. Охарактеризуйте методы криптографии в XVII–XVIII веках.
5. Охарактеризуйте методы криптографии в XIX веке.
6. Охарактеризуйте методы криптографии в XX веке.
7. Охарактеризуйте методы стеганографии.

Глава 2. ИСТОРИЯ РАЗВИТИЯ КРИПТОСИСТЕМ

Криптосистемы могут обеспечивать не только секретность передаваемых сообщений, но и их аутентичность (подлинность), а также подтверждение подлинности пользователя. Современные криптосистемы классифицируют следующим образом [1].

Современная криптография включает четыре крупных раздела:

1. *Симметричные криптосистемы.* В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. (Шифрование – преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом, дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.)

2. *Криптосистемы с открытым ключом.* В системах с открытым ключом используются два ключа – открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения. (Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.)

3. *Электронная подпись.* Системой электронной подписи называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

4. *Управление ключами.* Это процесс системы обработки информации, содержанием которого является составление и распределение ключей между пользователями.

Основные направления использования криптографических методов – передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

2.1. Симметричное шифрование

Симметричные криптосистемы (с секретным ключом – secret key systems) построены на основе сохранения в тайне ключа шифрования. Процессы зашифрования и расшифрования используют один и тот же ключ. Секретность ключа является постулатом. Основная проблема при применении симметричных криптосистем для связи заключается в сложности передачи обоим сторонам секретного ключа. Однако данные системы обладают высоким быстродействием. Раскрытие ключа злоумышленником грозит раскрытием только той информации, что была зашифрована на этом ключе. Американский и российский стандарты шифрования DES и ГОСТ 28147–89 – представители симметричных криптосистем [11].

Длина ключа. Количество информации в ключе, как правило, измеряется в битах. Для современных симметричных алгоритмов (AES, CAST5, IDEA, Blowfish, Twofish) основной характеристикой криптостойкости является длина ключа. Шифрование с ключами длиной 128 бит и выше считается сильным, так как для расшифровки информации без ключа требуются годы работы мощных суперкомпьютеров. Для асимметричных алгоритмов, основанных на проблемах теории чисел (проблема факторизации – RSA, проблема дискретного логарифма – Elgamal), в силу их особенностей минимальная надежная длина ключа в настоящее время – 1024 бит. Для асимметричных алгоритмов, основанных на использовании теории эллиптических кривых (ECDSA, ГОСТ Р 34.10–2001, ДСТУ 4145–2002), минимальной надежной длиной ключа считается 163 бит, но рекомендуются длины от 191 бит и выше [9].

В этой методологии и для шифрования, и для расшифровки отправителем и получателем применяется один и тот же ключ, об использовании которого они договорились до начала взаимодействия. Если ключ не был скомпрометирован, то при расшифровке автоматически выполняется аутентификация отправителя, так как только отправитель имеет ключ, с помощью которого можно зашифровать информацию, и только получатель имеет ключ, с помощью которого можно ее расшифровать. Поскольку отправитель и получатель – единственные люди, которые знают этот симметричный

ключ, при компрометации ключа будет скомпрометировано только взаимодействие этих двух пользователей. Проблемой, которая будет актуальна и для других криптосистем, является вопрос о том, как безопасно распространять симметричные (секретные) ключи [9].

Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных.

Порядок использования систем с симметричными ключами:

1. Безопасно создается, распространяется и сохраняется симметричный секретный ключ.

2. Отправитель создает электронную подпись с помощью расчета хеш-функции для текста и присоединения полученной строки к тексту.

3. Отправитель использует быстрый симметричный алгоритм шифрования-расшифровки вместе с секретным симметричным ключом к полученному пакету (тексту вместе с присоединенной электронной подписью) для получения зашифрованного текста. Неявно таким образом производится аутентификация, так как только отправитель знает симметричный секретный ключ и может зашифровать этот пакет. Только получатель знает симметричный секретный ключ и может расшифровать этот пакет.

4. Отправитель передает зашифрованный текст. Симметричный секретный ключ никогда не передается по незащищенным каналам связи.

5. Получатель использует тот же самый симметричный алгоритм шифрования-расшифровки вместе с тем же самым симметричным ключом (который уже есть у получателя) к зашифрованному тексту для восстановления исходного текста и электронной подписи. Его успешное восстановление аутентифицирует кого-то, кто знает секретный ключ.

6. Получатель отделяет электронную подпись от текста.

7. Получатель создает другую электронную подпись с помощью расчета хеш-функции для полученного текста.

8. Получатель сравнивает две этих электронных подписи для проверки целостности сообщения (отсутствия его искажения).

В блочных шифрах обрабатывают информацию блоками определенной длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. Результатом повторения раундов является лавинный эффект – нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.

Особенностью блочного шифра является обработка блока нескольких байтов за одну итерацию (как правило, 8 или 16). Блочные криптосистемы разбивают текст сообщения на отдельные блоки и затем осуществляют преобразование этих блоков с применением ключа [14]. Преобразование должно использовать следующие принципы:

– рассеивание (diffusion) – то есть изменение любого знака открытого текста или ключа влияет на большое число знаков шифротекста, что скрывает статистические свойства открытого текста;
– перемешивание (confusion) – использование преобразований, затрудняющих получение статистических зависимостей между шифротекстом и открытым текстом.

К достоинствам блочных шифров относят похожесть процедур шифрования и расшифрования, которые, как правило, отличаются лишь порядком действий. Это упрощает создание устройств шифрования, так как позволяет использовать одни и те же блоки в цепях шифрования и дешифрования. Названия некоторых из симметричных шифров: AES (Advanced Encryption Standard) – американский стандарт шифрования; ГОСТ 28147–89 – советский и российский стандарт шифрования, также является стандартом СНГ; DES (англ. Data Encryption Standard) – стандарт шифрования данных в США; IDEA (International Data Encryption Algorithm) – международный алгоритм шифрования данных; RC2 (Rivest Cipher или Ron's Cipher) – шифр Ривеста.

В поточных шифрах шифрование проводится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования. Поточный шифр может быть легко создан на основе блочного (например, ГОСТ 28147–89 в режиме гаммирования), запущенного в специальном режиме [17].

Большинство симметричных шифров используют сложную комбинацию большого количества подстановок и перестановок. Многие такие шифры исполняются в несколько (иногда до 80) проходов, с использованием на каждом проходе ключа прохода. Множество ключей прохода для всех проходов называется расписанием ключей (key schedule). Как правило, оно создается из ключа выполнением над ним неких операций, в том числе перестановок и подстановок.

Операция перестановки перемешивает биты сообщения по некоему закону. В аппаратных реализациях она тривиально реализуется как перепутывание проводников. Именно операции перестановки дают возможность достижения эффекта лавины. Операция перестановки линейна – $f(a)$ xor $f(b) == f(a$ xor $b)$ [6].

Операции подстановки выполняются как замена значения некоей части сообщения (часто в 4, 6 или 8 бит) на стандартное, жестко встроенное в алгоритм иное число путем обращения к константному массиву. Операция подстановки привносит в алгоритм нелинейность.

Существует множество (не менее двух десятков) алгоритмов симметричных шифров, существенными параметрами которых являются: стойкость, длина ключа, число раундов, длина обрабатываемого блока, сложность аппаратной/программной реализации, сложность преобразования.

Доступными сегодня средствами, в которых используется симметричная методология, являются:

– Kerberos, который был разработан для аутентификации доступа к ресурсам в сети, а не для верификации данных. Он использует центральную базу данных, в которой хранятся копии секретных ключей всех пользователей;

– сети банкоматов (ATM Banking Networks). Эти системы являются оригинальными разработками владеющих ими банков и не продаются. В них также используются симметричные методологии.

Виды поточных шифров:

1. RC4 (алгоритм шифрования с ключом переменной длины).
2. SEAL (Software Efficient Algorithm, программно-эффективный алгоритм).

3. WAKE (World Auto Key Encryption algorithm, всемирный алгоритм шифрования на автоматическом ключе).

Достоинства:

- скорость (по данным Applied Cryptography – на 3 порядка выше);
- простота реализации (за счет более простых операций);
- меньшая требуемая длина ключа для сопоставимой стойкости;
- изученность (за счет большего возраста).

Недостатки:

- сложность управления ключами в большой сети. Означает квадратичное возрастание числа пар ключей, которые надо генерировать, передавать, хранить и уничтожать в сети. Для сети в 10 абонентов требуется 45 ключей, для 100 уже 4950, для 1000 – 499 500 и т. д.;
- сложность обмена ключами. Для применения необходимо решить проблему надежной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам [18].

2.2. Асимметричное шифрование

Асимметричные криптосистемы (системы открытого шифрования – о. ш., с открытым ключом и т. д. – *public key systems*) – криптосистемы, в которых для зашифрования и расшифрования используются разные преобразования. Одно из них – зашифрование – является абсолютно открытым для всех. Другое же – расшифрование – остается секретным. Таким образом, любой, кто хочет что-либо зашифровать, пользуется открытым преобразованием. Но расшифровать и прочитать это сможет лишь тот, кто владеет секретным преобразованием. В настоящий момент во многих асимметричных криптосистемах вид преобразования определяется ключом. У пользователя есть два ключа – секретный и открытый. Открытый ключ публикуется в общедоступном месте, и каждый, кто захочет послать сообщение этому пользователю, зашифровывает текст открытым ключом. Расшифровать сможет только упомянутый пользователь с секретным ключом. Таким образом, пропадает проблема передачи секретного ключа (как у симметричных систем). Однако, несмотря на все свои преимущества, эти криптосистемы достаточно трудоем-

ки и медлительны. Стойкость асимметричных криптосистем базируется в основном на алгоритмической трудности решить за приемлемое время какую-либо задачу. Если злоумышленнику удастся построить такой алгоритм, то дискредитирована будет вся система и все сообщения, зашифрованные с помощью этой системы. В этом состоит главная опасность асимметричных криптосистем в отличие от симметричных. Примеры – системы о. ш. RSA, система о. ш. Рабина и т. д.

Одно из основных правил криптографии (если рассматривать ее коммерческое применение, так как на государственном уровне все несколько иначе) можно выразить следующим образом: *взлом шифра с целью прочесть закрытую информацию должен обойтись злоумышленнику гораздо дороже, чем эта информация стоит на самом деле.*

Все асимметричные криптосистемы являются объектом атак путем прямого перебора ключей, и поэтому в них должны использоваться гораздо более длинные ключи, чем те, которые используются в симметричных криптосистемах, для обеспечения эквивалентного уровня защиты. Это сразу же сказывается на вычислительных ресурсах, требуемых для шифрования, хотя алгоритмы шифрования на эллиптических кривых могут смягчить эту проблему. Брюс Шнейер в книге «Прикладная криптография: протоколы, алгоритмы и исходный текст на С» приводит следующие данные об эквивалентных длинах ключей [18].

В асимметричных криптосистемах важно, чтобы сеансовые и асимметричные ключи были сопоставимы в отношении уровня безопасности, который они обеспечивают. Если используется короткий сеансовый ключ (например, 40-битовый DES), то не имеет значения, насколько велики асимметричные ключи. Хакеры будут атаковать не их, а сеансовые ключи. Асимметричные открытые ключи уязвимы к атакам прямым перебором отчасти из-за того, что их тяжело заменить. Если атакующий узнает секретный асимметричный ключ, то будет скомпрометировано не только текущее, но и все последующие взаимодействия между отправителем и получателем [21].

Порядок использования систем с асимметричными ключами:

1. Безопасно создаются и распространяются асимметричные открытые и секретные ключи (см. раздел 2.2 ниже). Секретный

асимметричный ключ передается его владельцу. Открытый асимметричный ключ хранится в базе данных X.500 и администрируется центром выдачи сертификатов (по-английски – Certification Authority, или CA). Подразумевается, что пользователи должны верить, что в такой системе производится безопасное создание, распределение и администрирование ключей. Более того, если создатель ключей и лицо или система, администрирующие их, не одно и то же, то конечный пользователь должен верить, что создатель ключей на самом деле уничтожил их копию.

2. Создается электронная подпись текста с помощью вычисления его хеш-функции. Полученное значение шифруется с использованием асимметричного секретного ключа отправителя, а затем полученная строка символов добавляется к передаваемому тексту (только отправитель может создать электронную подпись).

3. Создается секретный симметричный ключ, который будет использоваться для шифрования только этого сообщения или сеанса взаимодействия (сеансовый ключ), затем при помощи симметричного алгоритма шифрования/расшифровки и этого ключа шифруется исходный текст вместе с добавленной к нему электронной подписью – получается зашифрованный текст (шифротекст).

4. Теперь нужно решить проблему с передачей сеансового ключа получателю сообщения.

5. Отправитель должен иметь асимметричный открытый ключ центра выдачи сертификатов (CA). Перехват незашифрованных запросов на получение этого открытого ключа является распространенной формой атаки. Может существовать целая система сертификатов, подтверждающих подлинность открытого ключа CA. Стандарт X.509 описывает ряд методов для получения пользователями открытых ключей CA, но ни один из них не может полностью защитить от подмены открытого ключа CA, что наглядно доказывает, что нет такой системы, в которой можно было бы гарантировать подлинность открытого ключа CA.

6. Отправитель запрашивает у CA асимметричный открытый ключ получателя сообщения. Этот процесс уязвим к атаке, в ходе которой атакующий вмешивается во взаимодействие между отправителем и получателем и может модифицировать трафик, передава-

емый между ними. Поэтому открытый асимметричный ключ получателя «подписывается» CA. Это означает, что CA использовал свой асимметричный секретный ключ для шифрования асимметричного открытого ключа получателя. Только CA знает асимметричный секретный ключ CA, поэтому есть гарантии того, что открытый асимметричный ключ получателя получен именно от CA.

7. После получения асимметричный открытый ключ получателя расшифровывается с помощью асимметричного открытого ключа CA и алгоритма асимметричного шифрования/расшифровки. Естественно, предполагается, что CA не был скомпрометирован. Если же он оказывается скомпрометированным, то это выводит из строя всю сеть его пользователей. Поэтому можно и самому зашифровать открытые ключи других пользователей, но где уверенность в том, что они не скомпрометированы?

8. Теперь шифруется сеансовый ключ с использованием асимметричного алгоритма шифрования-расшифровки и асимметричного ключа получателя (полученного от CA и расшифрованного).

9. Зашифрованный сеансовый ключ присоединяется к зашифрованному тексту (который включает в себя также добавленную ранее электронную подпись).

10. Весь полученный пакет данных (зашифрованный текст, в который входит, помимо исходного текста, его электронная подпись, и зашифрованный сеансовый ключ) передается получателю. Так как зашифрованный сеансовый ключ передается по незащищенной сети, он является очевидным объектом различных атак.

11. Получатель выделяет зашифрованный сеансовый ключ из полученного пакета.

12. Теперь получателю нужно решить проблему с расшифровкой сеансового ключа.

13. Получатель должен иметь асимметричный открытый ключ центра выдачи сертификатов (CA).

14. Используя свой секретный асимметричный ключ и тот же самый асимметричный алгоритм шифрования, получатель расшифровывает сеансовый ключ.

15. Получатель применяет тот же самый симметричный алгоритм шифрования-расшифровки и расшифрованный симметрич-

ный (сеансовый) ключ к зашифрованному тексту и получает исходный текст вместе с электронной подписью.

16. Получатель отделяет электронную подпись от исходного текста.

17. Получатель запрашивает у CA асимметричный открытый ключ отправителя.

18. Как только этот ключ получен, получатель расшифровывает его с помощью открытого ключа CA и соответствующего асимметричного алгоритма шифрования-расшифровки.

19. Затем расшифровывается хеш-функция текста с использованием открытого ключа отправителя и асимметричного алгоритма шифрования-расшифровки.

20. Повторно вычисляется хеш-функция полученного исходного текста.

21. Две эти хеш-функции сравниваются для проверки того, что текст не был изменен.

Виды асимметричных шифров:

1. RSA (Rivest-Shamir-Adleman).
2. DSA (Digital Signature Algorithm).
3. Elgamal (шифросистема Эль-Гамаля).
4. Diffie-Hellman (обмен ключами Диффи – Хелмана).
5. ECDSA (Elliptic Curve Digital Signature Algorithm) – алгоритм с открытым ключом для создания цифровой подписи.
6. ГОСТ Р 34.10–2001.

Преимущества:

- преимущество асимметричных шифров перед симметричными состоит в отсутствии необходимости предварительной передачи секретного ключа по надежному каналу;
- в симметричной криптографии ключ держится в секрете для обеих сторон, а в асимметричной криптосистеме только один секретный;
- при симметричном шифровании необходимо обновлять ключ после каждого факта передачи, тогда как в асимметричных криптосистемах пару (E, D) можно не менять значительное время;
- в больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

Недостатки:

- преимущество алгоритма симметричного шифрования перед несимметричным заключается в том, что в первый относительно легко внести изменения;
- сообщения надежно шифруются, но «засвечиваются» получатель и отправитель самим фактом пересылки шифрованного сообщения;
- несимметричные алгоритмы используют более длинные ключи, чем симметричные;
- процесс шифрования-расшифрования с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом;
- в чистом виде асимметричные криптосистемы требуют существенно больших вычислительных ресурсов, поэтому на практике используются в сочетании с другими алгоритмами.

2.3. Требования к криптосистемам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т. д. Программная реализация более практична, допускает известную гибкость в использовании. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

▪ зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

▪ число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

▪ число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

▪ знание алгоритма шифрования не должно влиять на надежность защиты;

▪ незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

▪ структурные элементы алгоритма шифрования должны быть неизменными;

▪ дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

▪ длина шифрованного текста должна быть равной длине исходного текста;

▪ не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

▪ любой ключ из множества возможных должен обеспечивать надежную защиту информации;

▪ алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования [35].

2.4. Аутентификация на основе паролей

Аутентифика́ция (англ. *authentication*) – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности [4].

Почти каждая компьютерная система требует, чтобы в начале сеанса работы пользователь идентифицировал себя. Обычно пользователю предлагается ввести имя и пароль. Пароль – это секретная информация (или просто секрет), разделенная между пользователем и удаленным сервером. Пользователь помнит этот секрет, а сервер хранит либо копию секрета, либо значение, вычисленное на основе секрета. Во время аутентификации происходит сопоставление пароля, введенного пользователем, и значения, хранимого сервером. Аутентификация при помощи паролей – наиболее распространенный вид. Если злоумышленник знает чужой пароль,

то имеет возможность выдавать себя за другого субъекта, и сервер не может отличить его от настоящего пользователя.

Существует несколько способов получения секретного пароля в сети. Пользователь *C* может использовать программу-анализатор, или сниффер. Программы-анализаторы легко доступны в Интернете, они позволяют перехватывать сетевой трафик между компьютерами одной локальной сети. Для перехвата пароля пользователю *C* можно даже не находиться в одном помещении с пользователем *A* и не иметь доступа к его компьютеру – ему достаточно лишь сетевого подключения к той же самой локальной сети. Эти программы настолько упрощают перехват информации, что хищение пароля часто называют атакой анализатора. После смены пароль остается неизвестен пользователю *C* только до очередного запуска программы-анализатора. Если пользователь *C* постоянно запускает свою программу-анализатор, то получает новый пароль пользователя *A*, как только он выбран.

Некоторые типы локальных сетей более уязвимы для атак анализатора. Особенно это касается тех, которые, как многоканальная сеть Ethernet, используют широковещательную среду. Сети, подобные коммутируемой сети Ethernet, не столь восприимчивы. Концентратор передает трафик только по проводам, соединяющим связывающиеся компьютеры. В этом случае, желая получить ту же самую информацию, пользователь *C* сталкивается с более трудной задачей: инсталлировать программу-анализатор на компьютер пользователя *A* [4].

Атаки анализаторов обнажают две серьезные проблемы аутентификации при помощи паролей. Во-первых, для аутентификации пользователь *A* должен передать свой пароль, разделенный секрет. Выполняя это, пользователь *A* может раскрыть его. Во-вторых, если разделенный секрет пользователя *A* используется долгое время, пользователю *C* достаточно получить пароль один раз, после чего он может выдавать себя за пользователя *A*, пока последний не изменит свой пароль. Эти слабые стороны делают атаки анализаторов успешными [11].

Аутентификация при помощи паролей неэффективна в среде со многими серверами. Предположим, что пользователь *A* регулярно взаимодействует с шестью удаленными серверами. Он может

использовать один и тот же пароль для каждой системы или разные пароли для всех систем. Если пользователь *A* использует один и тот же пароль, то успешная атака анализатора позволяет пользователю *C* получить доступ к учетным записям пользователя *A* сразу на всех серверах и в дальнейшем выдавать себя за него. Если пользователь *A* использует разные пароли для каждого сервера, то успешная атака анализатора позволяет пользователю *C* получить доступ только к одному серверу, но при этом пользователь *A* должен помнить шесть разных паролей. Скорее всего, пользователь *A* запишет свои пароли, в этом случае они могут быть похищены другим способом [15].

Взаимная аутентификация при помощи паролей возможна, только если существует два разделенных между пользователем и сервером секрета, два пароля. В этом случае каждый пользователь должен помнить пароль сервера и свой пароль. Сервер должен обменяться вторым разделенным секретом с каждым пользователем, причем этот секрет должен быть уникальным, чтобы ни один пользователь не мог маскироваться под сервер перед другим пользователем. Если взаимная аутентификация пользователей отсутствует, то пользователь *C* может получить пароль пользователя *A*, создав фальшивый сервер. Когда пользователи попытаются получить доступ к этому серверу, пользователь *C* сможет собрать их имена и пароли.

Эволюция механизмов аутентификации началась в ответ на атаки анализаторов. Очевидно, что должна была появиться защита от этих атак в виде шифрования. Шифрование предотвращает раскрытие пароля при передаче. Но если все пользователи используют один и тот же ключ шифрования, то любой из них может использовать анализатор, получить чужой пароль и расшифровать его тем же способом, что и сервер. Если каждый пользователь имеет свой ключ, то управление этими ключами обеспечивает более сильную аутентификацию, чем пароли. Следует отметить, что пользователь *A* защищен и в том случае, если его пароль используется однократно. Удачная атака анализатора позволяет пользователю *C* получить устаревший пароль *A*. Ясно, что пользователю *A* в этом случае необходим новый пароль для каждой попытки аутентификации.

Эти механизмы позволяют проверить подлинность личности участника взаимодействия безопасным и надежным способом.

Сервер генерирует случайный запрос и отправляет его пользователю *A*. Вместо того чтобы в ответ отправить серверу пароль, пользователь *A* шифрует запрос при помощи ключа, известного только ему самому и серверу. Сервер выполняет такое же шифрование и сравнивает результат с шифротекстом, полученным от пользователя *A*. Если они совпадают, то аутентификация прошла успешно, в противном случае – неудачно.

Этот простой механизм имеет несколько преимуществ по сравнению с простой аутентификацией при помощи паролей. Поскольку запрос генерируется случайным образом, пользователь *C* не может повторно использовать шифротекст, сгенерированный пользователем *A*, чтобы выдавать себя за него. Значение, которое отправляет пользователь *A*, аутентифицирует его идентичность только один раз. Имя пользователя *A* передается открыто, и нет причин его скрывать. Перехват информации больше не является угрозой, и пользователь *A* может выполнять аутентификацию на удаленном сервере в открытой сети [6].

Механизм усложняется, если пользователю *A* необходимо пройти аутентификацию на многих серверах, в этом случае, как и при использовании паролей, пользователь *A* должен иметь для каждого сервера свой ключ шифрования запроса и защищенно хранить все эти ключи.

Чтобы этот механизм был пригоден для взаимной аутентификации, необходимы еще один запрос и ответ. Пользователь *A* может направить второй запрос вместе с зашифрованным первым запросом, а сервер – вернуть зашифрованный ответ вместе с уведомлением о корректной проверке запроса пользователя *A*. Таким образом, этот механизм может быть использован для взаимной аутентификации без второго разделяемого ключа шифрования запроса [8].

В некоторых случаях аутентификация типа «запрос – ответ» невозможна, потому что сервер не имеет средств формирования запроса к пользователю, это характерно для систем, первоначально спроектированных для применения простых паролей. Тогда необходим неявный запрос, который обычно базируется на значении текущего времени.

2.5. Электронная цифровая подпись

Электронная цифровая подпись (**ЭЦП**) – реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП. Значение реквизита получается в результате криптографического преобразования информации с использованием *закрытого ключа* ЭЦП.

Электронная подпись позволяет проверять целостность данных, но не обеспечивает их конфиденциальности. Электронная подпись добавляется к сообщению и может шифроваться вместе с ним при необходимости сохранения данных в тайне. Добавление временных меток к электронной подписи позволяет обеспечить ограниченную форму контроля участников взаимодействия [19].

Электронная цифровая подпись – по сути шифрование сообщения алгоритмом с открытым ключом. Текст, зашифрованный секретным ключом, объединяется с исходным сообщением. Тогда проверка подписи – расшифрование открытым ключом, если получившийся текст аналогичен исходному тексту – подпись верна [10].

Популярные алгоритмы ЭЦП:

1. FDH (Full Domain Hash), вероятностная схема RSA-PSS (Probabilistic Signature Scheme), схемы стандарта PKCS#1 и другие схемы, основанные на алгоритме RSA.
2. Схема Эль-Гамаля.
3. Американские стандарты электронной цифровой подписи: DSA, ECDSA (DSA на основе аппарата эллиптических кривых).
4. Российские стандарты электронной цифровой подписи: ГОСТ Р 34.10–94 (в настоящее время не действует), ГОСТ Р 34.10–2001 (не рекомендован к использованию после 31 декабря 2017 года), ГОСТ Р 34.10–2012.
5. Евразийский союз: ГОСТ 34.310–2004 полностью идентичен российскому стандарту ГОСТ Р 34.10–2001.
6. Украинский стандарт электронной цифровой подписи ДСТУ 4145–2002.

7. Белорусский стандарт электронной цифровой подписи СТБ 1176.2–99 (в настоящее время не действует), СТБ 34.101.45–2013.
8. Схема Шнорра.

Использование хеш-функции позволяет оптимизировать данный алгоритм. Производится шифрование не самого сообщения, а значение хеш-функции, взятой от сообщения. Данный метод обеспечивает следующие преимущества:

- понижение вычислительной сложности. Как правило, документ значительно больше его хеша;
- повышение криптостойкости. Криптоаналитик не может, используя открытый ключ, подобрать подпись под сообщение, а только под его хеш;
- обеспечение совместимости. Большинство алгоритмов оперирует со строками данных, но некоторые используют другие представления. Хеш-функцию можно использовать для преобразования произвольного входного текста в подходящий формат.

Хеширование (иногда хэширование, англ. *hashing*) – преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются **хеш-функциями** или **функциями свёртки**, а их результаты называют **хешем**, **хеш-кодом** или **дайджестом сообщения** (англ. *message digest*).

Хеширование применяется для сравнения данных: если у двух массивов хеш-коды разные, массивы гарантированно различаются; если одинаковые – массивы, скорее всего, одинаковы. В общем случае однозначного соответствия между исходными данными и хеш-кодом нет в силу того, что количество значений хеш-функций меньше, чем вариантов входного массива; существует множество массивов, дающих одинаковые хеш-коды – так называемые коллизии. Вероятность возникновения коллизий играет немаловажную роль в оценке качества хеш-функций.

Существует множество алгоритмов хеширования с различными характеристиками (разрядность, вычислительная сложность, криптостойкость и т. п.). Выбор той или иной хеш-функции определяется спецификой решаемой задачи. Простейшими примерами хеш-функций могут служить контрольная сумма или CRC.

Криптографической хеш-функцией называется всякая хеш-функция, являющаяся криптостойкой, то есть удовлетворяющая ряду требований, специфичных для криптографических приложений. Примеры современных хеш-функций: MD4, MD5, MD6, SHA-1, SHA-2, ГОСТ Р 34.11–94.

Среди множества существующих хеш-функций принято выделять криптографически стойкие, применяемые в криптографии. Для того чтобы хеш-функция H считалась криптографически стойкой, она должна удовлетворять трем основным требованиям, на которых основано большинство применений хеш-функций в криптографии:

- *необратимость*: для заданного значения хеш-функции m должно быть вычислительно неосуществимо найти блок данных X, для которого $H(X) = m$;
- *стойкость к коллизиям первого рода*: для заданного сообщения M должно быть вычислительно неосуществимо подобрать другое сообщение N, для которого $H(N) = H(M)$;
- *стойкость к коллизиям второго рода*: должно быть вычислительно неосуществимо подобрать пару сообщений, имеющих одинаковый хеш.

Данные требования не являются независимыми:

- обратимая функция нестойка к коллизиям первого и второго рода;
- функция, нестойкая к коллизиям первого рода, нестойка к коллизиям второго рода; обратное неверно.

Следует отметить, что не доказано существование необратимых хеш-функций, для которых вычисление какого-либо прообраза заданного значения хеш-функции теоретически невозможно. Обычно нахождение обратного значения является лишь вычислительно сложной задачей.

Для криптографических хеш-функций также важно, чтобы при малейшем изменении аргумента значение функции сильно изменялось (лавинный эффект). В частности, значение хеша не должно давать утечки информации даже об отдельных битах аргумента. Это требование является залогом криптостойкости алгоритмов

хеширования, хеширующих пользовательский пароль для получения ключа [15].

Проверка парольной фразы. В большинстве случаев парольные фразы не хранятся на целевых объектах, хранятся лишь их хеш-значения. Хранить парольные фразы нецелесообразно, так как в случае несанкционированного доступа к файлу с фразами злоумышленник узнает все парольные фразы и сразу сможет ими воспользоваться, а при хранении хеш-значений он узнает лишь хеш-значения, которые не обратимы в исходные данные, в данном случае в парольную фразу. В ходе процедуры аутентификации вычисляется хеш-значение введенной парольной фразы и сравнивается с сохраненным [22].

Данная система подразумевает передачу сообщения по защищенному каналу, то есть каналу, из которого криптоаналитику невозможно перехватить сообщения или послать свое. Иначе он может перехватить хеш-значение парольной фразы и использовать его для дальнейшей нелегальной аутентификации. Защищаться от подобных атак можно при помощи метода «тройного рукопожатия».

В такой ситуации пароль не хранится открыто на сервере и, даже перехватив все сообщения между клиентом и сервером, криптоаналитик не может восстановить пароль, а передаваемое хеш-значение каждый раз разное [24].

Выводы

В этой главе описано развитие криптосистем. Сначала учеными было предложено симметричное шифрование, а затем перешли к асимметричному. Рассмотрены также вопросы, связанные с аутентификацией на основе паролей и электронной цифровой подписи.

Контрольные вопросы

1. Дайте определение криптографии и криптоанализа.
2. Дайте определение шифрования, расшифрования, дешифрования.
3. Дайте определение стеганографии.
4. Дайте определение симметричных криптосистем.
5. Дайте определение криптосистемы с открытым ключом.
6. Дайте определение электронной подписи.
7. Дайте определение блочного шифра.
8. Дайте определение поточного шифра.
9. Дайте определение асимметричных криптосистем.
10. Дайте определение аутентификации.

Глава 3. ПРИБЛИЖЕНИЕ ФУНКЦИЙ

3.1. Интерполирование

Простейший и исторически самым ранний способ приближения, или аппроксимации, функций – интерполирование [38–55].

Задача интерполирования ставится так.

На отрезке $[a, b]$ в узлах $x_0, x_1, ..., x_n$ известны значения функции $f(x)$: $f(x_0), f(x_1), ..., f(x_n)$. Требуется построить функцию $\varphi(x)$, которая бы в точках x_i совпадала с заданными значениями $f(x)$: $\varphi(x_i) = f(x_i)$, $i = 0 \div n$. Таблица $f(x_i)$ могла быть получена, например, в результате измерений. Возможно, что известно и аналитическое выражение $f(x)$, но оно очень сложно для вычислений, и потому желательно его заменить более простой функцией $\varphi(x)$. В такой постановке, очевидно, задача не имеет единственного решения. Чаще всего $\varphi(x)$ отыскивают в виде многочлена.

Задача отыскания многочлена $L_n(x)$ степени n, совпадающего со значениями $f(x)$ в узлах $x_0, x_1, ..., x_n$, имеет единственное решение, так как для отыскания коэффициентов $a_0, a_1, ..., a_n$ многочлена

$$L_n(x) = a_0 + a_1 x + a_2 x + ... + a_n x^n$$

получаем систему алгебраических уравнений

$$a_0 + a_1 x_i + a_2 x_i^2 + ... + a_n x_i^n = f(x_i), i = 0 \div n,$$

определитель которой (определитель Вандермонда) отличен от нуля, если все x_i различны. Многочлен $L_n(x)$, удовлетворяющий условию

$$L_n(x_i) = f(x_i), \qquad i = 0 \div n,$$

называется интерполяционным многочленом для функции $f(x)$. Решение системы может быть записано различными способами.

Впервые задачу интерполирования сформулировал шотландский математик Джеймс Грегори (1638–1675). Ньютон получил решение этой задачи в 1711 году, уже после смерти Грегори. Интерполяционная формула Ньютона встречается ранее в его фундаментальном труде «Математические начала натуральной философии» (1687). Однако следует заметить, что еще в 1670 году она была получена Грегори. По этой причине формулу Ньютона часто называют формулой Ньютона – Грегори.

Приведем интерполяционную формулу Ньютона для равностоящих узлов. Для равностоящих узлов x_0, $x_1 = x_0 + \Delta x$, $x_2 = x_0 + 2\Delta x$, ..., $x_n = x_0 + n\Delta x$ она имеет вид

$$f(x) = f(x_0 + t\Delta x) = f(x_0) + \frac{t}{1!}\Delta f(x_0) + \frac{t(t-1)}{2!}\Delta^2 f(x_0) + \cdots +$$

$$+ \frac{t(t-1)(t-2)\ldots(t-(n-1))}{n!}\Delta^n f(x_0).$$

Здесь $t = \frac{x-x_0}{\Delta x}$, $\Delta f(x_0)$, $\Delta^2 f(x_0)$, ..., $\Delta^n f(x_0)$ – конечные разности функции $f(x)$ в точке x_0:

$$\Delta f(x_0) = f(x_0 + \Delta x) - f(x_0),$$

$$\Delta^2 f(x_0) = f(x_0 + \Delta x) - \Delta f(x_0),$$

$$\Delta^3 f(x_0) = \Delta^2 f(x_0 + \Delta x) - \Delta^2 f(x_0),$$

… … … … … … … … … … …

… … … … … … … … … … …

… … … … … … … … … … …

Приведенная формула Ньютона использует разности вперед и удобна, если x находится в начале таблицы.

Если использовать разности назад, получим другой вид формулы.

Эта интерполяционная формула Ньютона имеет широкое применение и в наши дни. Она послужила Тейлору как аналог при получении ряда, носящего его имя. Он рассуждает так. Заменим в формуле Ньютона t на n (n – целое) и рассмотрим бесконечно большое число членов так, чтобы при $n \to \infty$ выполнялось $\Delta x \to 0$, но произведение $n\Delta x = h$ оставалось конечным. Тогда

$$f(x_0 + h) = f(x_0) + h\frac{\Delta f(x_0)}{\Delta x} + \frac{h(h-\Delta x)}{2!}\frac{\Delta^2 f(x_0)}{\Delta^2 x} +$$

$$+ \frac{h(h-\Delta x)(h-2\Delta x)}{3!}\frac{\Delta^3 f(x_0)}{\Delta^3 x} + \cdots$$

И при $\Delta x \to 0$ имеем

$$f(x_0 + h) = f(x_0) + h\frac{df(x_0)}{dx} + \frac{h^2}{2!}\frac{d^2 f(x_0)}{d^2 x} + \frac{h^3}{3!}\frac{d^3 f(x_0)}{d^3 x} + \cdots$$

В 1715 году Тейлор опубликовал этот результат, в котором приводится и частный случай формулы Тейлора – ряд Маклорена ($x_0 = 0$), который Маклорен получил другим путем в 1742 году. Регу-

лярное применение рядов Тейлора и Маклорена стало характерной особенностью дифференциального исчисления.

В 1795 году Лагранж предложил другой вид интерполяционной формулы, получившей наибольшее распространение:

$$L_n(x) = \sum_{i=0}^{n} \frac{\prod_{j \neq i}^{n}(x - x_j)}{\prod_{j \neq i}^{n}(x_i - x_j)} f(x_i),$$

$$L_n(x) = \sum_{i=0}^{n} \frac{\omega(x)}{(x - x_i)\omega'(x_i)} f(x_i),$$

где

$$\omega(x) = (x - x_0)(x - x_1) \dots (x - x_n),$$

$$\omega'(x_i) = (x_i - x_0) \dots (x_i - x_{i-1})(x_i - x_{i+1}) \dots (x - x_n).$$

Существует много других интерполяционных формул, однако при использовании одних и тех же узлов x_0, x_1, ..., x_n все они приводят к единому интерполяционному многочлену степени n.

Известны формулы, использующие центральные разности. К ним принадлежат интерполяционные формулы Гаусса, Стирлинга, Бесселя, Эверетта.

Французский математик Шарль Эрмит в 1878 году сформулировал обобщенную задачу интерполирования функции $f(x)$, имеющей на $[a, b]$ необходимое число непрерывных производных. Она заключается в следующем. Пусть на отрезке $[a, b]$ заданы узлы интерполирования x_0, x_1, ..., x_m, в которых известны

$$f(x_i), f'(x_i), \dots, f^{(a_1-1)}(x_i), i = 0 \div m,$$

то есть всего $a_0 + a_1 + \dots + a_m$ величин. Требуется построить алгебраический многочлен $H_n(x)$ степени $a_0 + a_1 + \dots + a_m - 1$, для которого

$$H_n^{(k)} = f^{(k)}(x_i), i = 0 \div m, k = 0 \div a_1 - 1.$$

Многочлен $H_n(x)$ (Hermite) существует и единственен. Он называется многочленом Эрмита.

Если интерполяционная функция $f(x)$ периодическая, то зачастую удобнее пользоваться не алгебраическими, а тригонометрическими многочленами. Такие многочлены были получены, в частности, Гауссом в 1805 году. В каждом конкретном случае удобнее пользоваться той или иной формулой. Был разработан и общий подход получения интерполяционных формул.

Вернемся к классической задаче интерполирования и рассмотрим вопросы точности интерполяционных многочленов. Интерполяционные многочлены совпадают с $f(x)$ в узлах интерполирования. Однако возникает вопрос о величине отклонения $L_n(x)$ от $f(x)$ в произвольной точке отрезка $[a, b]$. Подчеркнем, что интерполяционные многочлены получены без каких-либо требований гладкости $f(x)$. Если предположить, что $f(x)$ имеет непрерывную $(n + 1)$-ю производную, то для остаточного члена

$$R_n(x) = f(x) - L_n(x)$$

можно получить формулу (в форме Коши)

$$R_n(x) = \frac{f^{(n+1)}(\xi)}{(n+1)!}\ \omega(x), \xi \in [a, b],$$

и оценку

$$|R_n(x)| \leq \frac{|\omega(x)|}{(n+1)!}\ M_{n+1},$$

где $|f^{(n+1)}(\xi)| \leq M_{n+1}$ на $[a, b]$.

Если есть свобода в выборе узлов интерполирования $x_0, x_1, \ldots, x_n$, то погрешность можно уменьшить, минимизируя величину

$$\max_{x\in[a,b]} |\omega(x)| = \max_{x\in[a,b]} |(x - x_0)(x - x_1) \ldots (x - x_n)|.$$

3.2. Наилучшее равномерное приближение функций многочленами

Это можно сделать, опираясь на фундаментальные результаты, полученные П.Л. Чебышевым, который в 1859 году в работе «Вопросы о наименьших величинах, связанные с приближенным представлением функций» развил теорию наилучшего равномерного приближения функций многочленами. Первые результаты были им опубликованы в 1854 году в статье «Теория механизмов, известных под названием параллелограммов» в связи с исследованием прикладной задачи по кинематике шарнирных механизмов. Здесь были сформулированы условия наилучшего приближения и получен многочлен, наименее уклоняющийся от нуля на отрезке $[a, b]$ среди всех многочленов данной степени с коэффициентом единица при старшей степени. Такие многочлены называются многочленами

Чебышева и обозначаются $T(x)$ (от французского написания фамилии Чебышева – *Tshebysheff*).

Минимум достигается, если $\omega(x)$ есть многочлен Чебышева

$$\omega(x) = T_{n+1}(x) =$$

$$= \frac{(b-a)^{n+1}}{2^{2n+1}} \cos\left((n+1)\arccos\frac{2x-(a+b)}{b-a}\right),$$

корни которого суть

$$x_i = \frac{a+b}{2} + \frac{b-a}{2}\cos\frac{(2i+1)\pi}{2(n+1)}, i = 0 \div n.$$

Тогда

$$\max_{x\in[a,b]} |\omega(x)| = \frac{(b-a)^{n+1}}{2^{2n+1}},$$

и для остаточного члена справедлива оценка

$$|R_n(x)| \le \frac{M_{n+1}}{(n+1)!}\frac{(b-a)^{n+1}}{2^{2n+1}}.$$

Величину R_n можно пытаться уменьшить, увеличивая число узлов на $[a, b]$.

Сходимость интерполяционного процесса

Возникает вопрос о сходимости: будет ли $R_n(x) \to 0$ при $n \to \infty$? Вообще говоря, нет. Сходимость интерполяционного процесса в точке $x^* \in [a, b]$ означает, что существует $\lim\limits_{n\to\infty} L_n(x^*) = f(x^*)$. Равномерная сходимость на $[a, b]$ означает, что

$$\max_{x\in[a,b]} |f(x) - L_n(x)| \to 0.$$

Большой вклад в теорию приближений функций внес другой русский математик С.Н. Бернштейн. В частности, он показал, что для функции $f(x) = |x|$ на отрезке $[-1, 1]$ последовательность $L_n(x)$, построенная по равностоящим узлам, при $n \to \infty$ не сходится к $|x|$ ни в одной точке $[-1, 1]$, кроме $x = -1, 0, 1$. Более того, интерполяционный многочлен при $n \to \infty$ совершает неограниченные колебания между узлами. Немецкий ученый Фабер доказал, что никакая последовательность узлов не гарантирует сходимости процесса интерполяции для произвольной непрерывной функции. Более точно: какова бы ни была последовательность узлов, найдется непрерывная на $[a, b]$ функция $f(x)$ такая, что последовательность интерполяционных многочленов не сходится к $f(x)$ равномерно на $[a, b]$.

Таким образом, не существует универсальной системы узлов интерполяции, обеспечивающей сходимость для любой непрерывной функции.

Однако для каждой непрерывной на $[a, b]$ функции можно подобрать систему узлов, чтобы интерполяционный процесс сходился равномерно на $[a, b]$ (Марцинкевич). Подчеркнем, что построить такую систему, свою для каждой функции, весьма сложно. Если $f(x)$ – гладкая функция, то есть $f(x)$ и $f'(x)$ непрерывны, то чебышевская система узлов обеспечивает равномерную сходимость интерполяционного процесса.

3.3. Кусочно-полиномиальная интерполяция

Приближать $f(x)$ на всем промежутке $[a, b]$ интерполяционным многочленам высокой степени нецелесообразно из-за возможных больших погрешностей. Это связано с накоплением погрешностей округления и возможной расходимостью интерполяционного процесса. Выгоднее разбивать отрезок $[a, b]$ на частичные отрезки и на каждом из них заменять функцию $f(x)$ многочленом невысокой степени. Это так называемая кусочно-полиномиальная интерполяция.

Аппроксимация дифференциальных выражений на равномерной сетке

Важным применением кусочно-полиномиальной интерполяции является аппроксимация дифференциальных выражений на равномерной сетке. Рассмотрим функцию $f(x)$, имеющую $n + 1$ производную на некотором отрезке $[a, b]$ оси x. Введем равномерную сетку x_k с шагом h, покрывающую отрезок $[a, b]$, так что $x_k = x_0 + kx$, $k = 0, \pm1, \pm2, \ldots$ Для каждого отрезка $[x_k, x_{k+1}]$ запишем интерполяционный многочлен $L_{n,k}(x)$, аппроксимирующий функцию $f(x)$ и построенный по точкам

$$x_{k-\nu_1}, x_{k-\nu_1+1}, \ldots, x_k, x_{k+1}, \ldots, x_{k+\nu_2},$$

$$\nu_1 \geq 0, \nu_2 \geq 0, \nu_1 + \nu_2 = n.$$

Погрешность аппроксимации $f(x)$ на отрезке $[x_k, x_{k+1}]$ дается формулой

$$\left|f(x) - L_{n,k}(x)\right| \leq \frac{|\omega(x)|}{(n+1)!} M_{n+1}.$$

Так как при любом l, $-\nu_1 \le l \le \nu_2$,

$$|x - x_{k+l}| \le x_{k+\nu_2} - x_{k-\nu_1} = (\nu_1 + \nu_2)h = nh,$$

то

$$|f(x) - L_{n,k}(x)| \le \frac{n^{n+1}}{(n+1)!} M_{n+1} h^{n+1}.$$

Функция $R(x) = f(x) - L_{n,k}(x)$ обращается в нуль в $n + 1$ точке x_l, $-\nu_1 \le l \le \nu_2$. Отсюда по теореме Ролля следует, что $L'_{n,k}(x)$ является интерполяционным многочленом для $f'(x)$, построенным по n точкам

$$\xi_l \in (x_l, x_{l+1}), l = k - \nu_1, k - \nu_1 + 1, \ldots, k + \nu_2 - 1.$$

Рассматривая последовательно $R^{(s)}(x)$, $s = 1, 2, \ldots, n$, получаем, что для погрешности аппроксимации производных $f^{(s)}(x)$ производными $L^{(s)}_{n,k}$ имеет место оценка

$$|f^{(s)}(x) - L^{(s)}_{n,k}(x)| \le \frac{n^{n+1-s}}{(n+1-s)!} M_{n+1} h^{n+1-s}, \; s = 0, 1, \ldots, n,$$

определяющая уникальное свойство кусочно-полиномиальной интерполяции на равномерной сетке по сравнению с другими способами аппроксимации (полиномиальные приближения в степенных нормах, дробно-рациональные приближения, непрерывные дроби и др.). Можно сказать, что все конечно-разностные методы численного решения дифференциальных уравнений основаны на приведенной оценке близости производных исходной и аппроксимирующей функций.

Рассмотрим теперь кусочную интерполяцию на всем отрезке $[a, b]$ при фиксированном шаге сетки h, так что $x_0 = a$, $x_i = a + ih$, $x_n = b$ и $b - a = nh$. Пусть $f(x)$ аппроксимируется функцией $S(x)$, определенной на каждом частичном отрезке $[x_i, x_{i+1}]$ формулой $S(x) = L_{n_i,i}(x)$, где $L_{n_i,i}(x)$ – многочлен степени n_i, и $S(x_i) = f(x_i)$ для всех i. Производные $L'_{n_i,i}(x_i)$ и $L'_{n_{i-1},i-1}(x_i)$, вообще говоря, не равны, и $S(x)$ не является гладкой функцией. Можно усложнить задачу, потребовав гладкого сопряжения в точках x_i. Такой подход приводит к понятию сплайна.

В течение многих лет для вычерчивания плавных обводов конструкций (кораблей, самолетов и др.) использовались тонкие гибкие рейки, которые устанавливались на больших горизонтальных

плоскостях (плазах) так, чтобы они проходили через определенные точки. Английское название этого устройства – spline, что означает «рейка» или «планка». Рассматривая планку чертежника как тонкую балку, форма которой описывается функцией $y(x)$, можно показать, что между точками свободного закрепления (без защемления) изгибающий момент, а следовательно, и вторая производная $y''(x)$ изменяется линейно, а в точках закрепления она непрерывна.

Использование математической модели сплайна как способа аппроксимации произвольной функции было предложено в 1946 году Шенебергом в его статье «К задаче аппроксимации равноотстоящих данных аналитическими функциями». Начиная с 50-х годов прошлого века теория сплайн-аппроксимаций стала быстро развиваться. Существенный вклад в теорию сплайнов был сделан советскими математиками С.М. Никольским и С.Л. Соболевым. Внедрению сплайнов в практику вычислений в значительной степени способствовало появление электронных вычислительных машин.

Определим так называемый кубический сплайн. Пусть на $[a, b]$ задана непрерывная функция $f(x)$ в узлах

$$a = x_0 < x_1 < x_2 < \ldots < x_n = b.$$

Сплайном называется функция $S(x)$, удовлетворяющая условиям:

а) на каждом сегменте $[x_{i-1}, x_i]$ $i = 1 \div n$, функция $S(x)$ есть многочлен 3-й степени;

б) функции $S(x)$, $S'(x)$, $S''(x)$ непрерывны на $[a, b]$;

в) $S(x_i) = f(x_i)$, $i = 0 \div n$.

Сплайн, удовлетворяющий этим условиям, называется интерполяционным кубическим сплайном. Доказано его существование и единственность, если для $S(x)$ заданы граничные условия, например $S''(a) = S''(b) = 0$. При неограниченном увеличении числа узлов n последовательность сплайнов сходится $f(x)$. Такой сплайн является нелокальным, так как коэффициенты полиномов $L_{n_i,i}(x)(n_i = 3)$ зависят от всех значений $f(x_i)$.

Более просто строится локальный сплайн с непрерывной первой (но не второй) производной. Он конструируется следующим образом. Пусть $Q_i(x)$ – интерполяционный многочлен второй степени, построенный по точкам x_{i-1}, x_i, x_{i+1} так, что

$$Q_i(x_{i+j}) = f(x_{i+j}),\ j = -1, 0, 1.$$

Тогда ($n_i = 2$)

$$L_{n_i,i}(x) = \frac{(x_{i+1} - x)Q_i(x) + (x - x_i)Q_{i+1}(x)}{x_{i+1} - x_i}.$$

Легко проверить, что $L'_{n_{i-1},i-1}(x_i) = L'_{n_i,i}(x_i)$. В ряде случаев локальный сплайн может оказаться более предпочтительным, чем нелокальный, например для иллюстративных целей.

3.4. Задача наилучшего равномерного приближения функций

Теория наилучшего равномерного приближения для случая алгебраических полиномов

В теории приближения функций огромная роль принадлежит П.Л. Чебышеву. Он разработал теорию наилучшего равномерного приближения, создал отечественную школу конструктивной теории функций, которая держит передовые позиции в мире и в настоящее время.

Задача непрерывного приближения непрерывной на отрезке $[a, b]$ функции $f(x)$ с помощью алгебраических многочленов состоит в определении такого многочлена $P_n(x)$, для которого выполняется условие

$$|f(x) - P_n(x)| \le \varepsilon$$

для всех $x \in [a, b]$ при заданном ε. Разрешимость этой задачи следует из теоремы Вейерштрасса: если $f(x)$ непрерывна на $[a, b]$, то для любого $\varepsilon > 0$ существует многочлен $P_n(x)$ степени $n = n(\varepsilon)$ такой, что для всех $x \in [a, b]$

$$|f(x) - P_n(x)| \le \varepsilon.$$

Существенно, что n зависит от ε. Если ε фиксировано и требуется, чтобы степень n многочлена не превышала некоторого заданного числа, то задача о равномерном приближении может не иметь решения.

Пусть H_n – множество всех многочленов степени не больше n. Величину $\Delta(f, P_n) = \max\limits_{x\in[a,b]} |f(x) - P_n(x)|, P_n \in H_n$, называют отклонением $f(x)$ от $P_n(x)$, а величину $E_n(f) = \inf\limits_{P_n\in H_n} \Delta(f, p_n)$ – наименьшим отклонением (наилучшим приближением). Многочлен $Q_n \in H_n$, для которого эта грань достигается, т. е. $E_n(f) = \Delta(f, Q_n)$ называется многочленом наилучшего приближения.

Исследования равномерных приближений функций были начаты Чебышевым в связи с работой в области теории шарнирных механизмов. В 1859 году он получил следующую замечательную теорему: для того чтобы многочлен $P_n(x)$ был многочленом наилучшего приближения для непрерывной функции $f(x)$ на отрезке $[a, b]$, необходимо и достаточно, чтобы разность $f(x) - P_n(x)$ достигала своего наибольшего по модулю значения по меньшей мере в $(n + 2)$-x точках отрезка $[a, b]$, последовательно меняя знак.

Таким образом, имеем $E_n(f) = \Delta(f, P_n)$, если в точках

$$a \le x_1 < x_2 < \ldots < x_{n+1} < x_{n+2} \le b$$

выполняются соотношения

$$f(x_1) - P_n(x_1) = \pm E_n(f),$$
$$f(x_2) - P_n(x_2) = \pm E_n(f),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$f(x_{n+2}) - P_n(x_{n+2}) = \pm(-1)^{n+1} E_n(f).$$

График многочлена $P_n(x)$ касается кривых $f(x) \pm E_n(f)$ попеременно в точках $x_1, x_2, \ldots, x_{n+2}$.

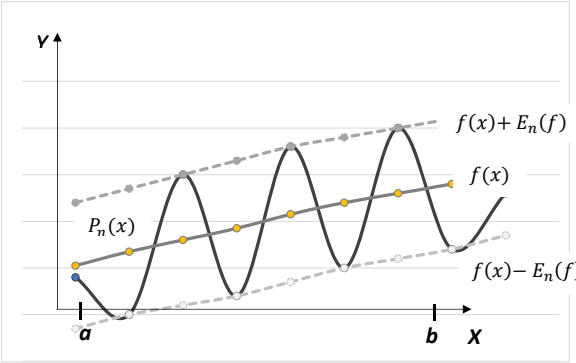

График многочлена $P_n(x)$

Задача о наилучшем равномерном приближении имеет единственное решение. Сформулированная теорема о наилучшем приближении носит имя Чебышева. Она послужила началом интенсивных исследований в области приближения функций. Первоклассные результаты принадлежат отечественным ученым, прежде всего академику С.Н. Бернштейну и его научной школе. Бернштейн внес много нового в доказательство основной теоремы Чебышева.

В развитии конструктивной теории функций заметную роль сыграл И.П. Натансон, которому принадлежит обстоятельная монография «Конструктивная теория функций» (1949). Бернштейном и американским ученым Д. Джексоном доказаны теоремы, устанавливающие связь между величиной наименьшего отклонения $E_n(f)$ и свойствами, в частности дифференциальными, функции $f(x)$.

Условия наилучшего приближения были сформулированы (без доказательства) Чебышевым в 1854 году. Это позволило ему решить задачу о нахождении многочлена, наименее уклоняющегося от нуля. Для отрезка [–1, 1] таким многочленом степени n с коэффициентом единица при старшей степени является многочлен

$$\bar{T}_n(x) = \frac{1}{2^{n-1}} T_n(x),$$

где $T_n(x) = \cos(n \arccos x)$. Он называется многочленом Чебышева. Из тождества $\cos(n+1)\varphi = 2\cos\varphi\cos n\varphi - \cos(n-1)\varphi$ следует рекуррентная формула

$$T_{n+1}(x) = 2x\,T_n(x) - T_{n-1}(x),\ T_0(x) = 1, T_1(x) = x.$$

Нули $T_n(x)$ находятся в точках $x_i = \cos\frac{2i-1}{2n}\pi$, $i = 1 \div n$, а экстремумы – в точках $x_k = \cos\frac{k\pi}{n}$, $k = 1 \div n-1$, и $T_n(x_k) = \cos k\pi = (-1)^k$.

Рассмотрим функцию $f(x) = \sin x$ на отрезке $\left[-\frac{\pi}{4}, \frac{\pi}{4}\right]$ и поставим задачу приблизить ее многочленом с погрешностью, не превышающей заданного числа $\varepsilon = 0{,}5 \cdot 10^{-7}$. Возьмем отрезок ряда Тейлора

$$\sin x \approx P_9(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \frac{x^9}{9!},$$

приближающий функцию $\sin x$ на отрезке $\left[-\frac{\pi}{4}, \frac{\pi}{4}\right]$ с погрешностью $|\sin x - P_9(x)| < \left(\frac{\pi}{4}\right)^{11} \frac{1}{11!} \approx 0{,}18 \cdot 10^{-8} < \varepsilon$. Отбросить член $\frac{x^9}{9!}$ нельзя, так как при этом погрешность возрастает до величины $3{,}2 \cdot 10^{-7} > \varepsilon$.

Использование многочлена Чебышева позволяет снизить степень многочлена до 7 с погрешностью, не превышающей ε. Для этого приблизим x^9 многочленом $Q_7(x)$ наилучшим образом. Для простоты, однако, проделаем это для отрезка $|x| < 1$. Имеем

$$x^9 - Q_7(x) = \bar{T}_9(x) = x^9 - \frac{9}{4}x^7 + \frac{27}{16}x^5 - \frac{15}{32}x^3 + \frac{9}{256}x.$$

Так как $|\bar{T}_9(x)| \le \frac{1}{2^8}$, то, заменив x^9 на $Q_7(x)$, допустим ошибку, не превышающую $\frac{1}{9!}\frac{1}{2^8} \approx 0{,}11 \cdot 10^{-7}$. Получаем многочлен

$$P_7(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \frac{1}{9!}Q_7(x),$$

и для

$$-\frac{\pi}{4} \le x \le \frac{\pi}{4} \quad |P_7(x) - \sin x| \approx 0{,}18 \cdot 10^{-8} + 0{,}11 \cdot 10^{-7} \approx 0{,}13 \cdot 10^{-7} < \varepsilon.$$

Такой прием, называемый иногда сверткой степенного ряда, широко используется при разработке алгоритмов вычисления элементарных функций для стандартных программ для компьютеров.

К. Ланцошем был предложен другой способ использования многочленов Чебышева для целей приближения. Продемонстрируем его на очень простом примере, взятом из книги Р.В. Хемминга «Численные методы» (1962), где способ Ланцоша называется процессом экономизации. Выпишем несколько чебышевских многочленов.

$$T_0(x) = 1, \qquad T_3(x) = 4x^2 - 3x,$$

$$T_1(x) = x, \qquad T_4(x) = 8x^4 - 8x^2 + 1,$$

$$T_2(x) = 2x^2 - 1, \qquad T_5(x) = 16x^5 - 20x^3 + 5x.$$

Выразим x^i через эти многочлены:

$$1 = T_0(x), \qquad x^3 = \frac{1}{4}[3T_1(x) + T_3(x)],$$

$$x = T_1(x), \qquad x^4 = \frac{1}{8}[3T_0(x) + 5T_2(x) + T_4(x)],$$

$$x^2 = \frac{1}{2}[T_0(x) + T_2(x)], \qquad x^5 = \frac{1}{16}[10T_1(x) + 5T_3(x) + T_5(x)].$$

Рассмотрим на отрезке [0, 1] функцию

$$\ln(1+x) \approx x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5}$$

и, используя выражение x^i через многочлены, получим

$$\ln(1+x) \approx -\frac{11}{32}T_0(x) + \frac{11}{8}T_1(x) - \frac{3}{8}T_2(x) + \frac{7}{48}T_3(x) - \frac{1}{32}T_4(x) + \\ + \frac{1}{80}T_5(x).$$

Разложение позволяет получить для вычисления функции $\ln(1 + x)$ многочлен меньшей степени, чем при той же точности. Действительно, отбрасывая последнее слагаемое, получаем многочлен четвертой степени, при этом ошибка оценивается величиной 0,2. В разложении можно отбросить три последних слагаемых, что приводит к многочлену второй степени с ошибкой, не превышающей величину

$$\frac{7}{48} + \frac{1}{32} + \frac{1}{80} = \frac{91}{15 \cdot 32} < \frac{10}{52} < 0{,}2.$$

Воспользовавшись формулами, получаем

$$\ln(1+x) \approx \frac{1}{32} + \frac{11}{8}x + \frac{3}{4}x^2, 0 \le x \le 1.$$

Теория наилучшего равномерного приближения для случая тригонометрических полиномов

Начало использования тригонометрических рядов для целей приближения функций относится ко второй половине XVIII века и связано с задачей о колебании струны. Решение этой задачи получено независимо Даламбером и Эйлером. В 1753 году Д. Бернулли, исходя из физических соображений, получил для уравнения колебаний струны решение в виде ряда:

$$U(x,t)\sum_{k=1}^{\infty} b_k \cos\frac{k\pi a}{l}t \cdot \sin\frac{k\pi}{l}x.$$

Отсюда следует, в частности, что функция $f(x)$, характеризующая начальную форму струны при $t = 0$, представима рядом по синусам

$$f(x) = \sum_{k=1}^{\infty} b_k \sin\frac{k\pi}{l}x.$$

Против этого решения выступили Даламбер и Эйлер. Они считали, что решение Бернулли можно рассматривать лишь как частное. Сам же Бернулли утверждал, что это разложение справедливо для широкого класса функций. После работы Бернулли возрос интерес к тригонометрическому разложению

$$f(x) = a_0 + \sum_{k=1}^{\infty} (a_k \cos kx + b_k \sin kx),$$

которое известно в математике как ряд Фурье. Исследование Фурье относится к 1807 году. Результаты опубликованы в его знаменитом труде «Аналитическая теория тепла» в 1822 году. Фурье, почленно интегрируя ряд, получил формулы коэффициентов для функции $f(x)$, заданной в промежутке $[-\pi, \pi]$:

$$a_0 = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x)\,dx, a_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos kx\,dx, b_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin kx\,dx.$$

Этот метод называется методом Эйлера – Фурье. Дело в том, что Эйлер еще в 1777 году применил его для определения коэффициентов разложения по косинусам функции $f(x)$, заданной в промежутке $[0, \pi]$. Еще ранее, в 1757 году, Клеро решил эту задачу с помощью интерполирования $f(x)$ тригонометрическим многочленом. Вопрос о законности процедуры интегрирования ряда долго не возникал. Справедливость самого разложения Эйлер предполагал. Фурье же пытался дать доказательство, но безуспешно. Однако он был уверен, что это разложение справедливо для произвольных функций. Эта уверенность базировалась на том, что интегралы имеют смысл для широкого класса функций.

Первую теорему о сходимости тригонометрического ряда Фурье доказал в 1829 году немецкий математик Дирихле. Он рассмотрел класс функций, заданных на $[-\pi, \pi]$ и имеющих конечное число точек разрыва первого рода и конечное число точек экстремума. Эти условия носят название условий Дирихле. Как доказал Дирихле, для функции $f(x)$, удовлетворяющей этим условиям, ряд Фурье сходится во всех $[-\pi, \pi]$ к $f(x)$ в точках непрерывности, к $\frac{1}{2}[f(x+0) + f(x-0)]$ в точках разрыва и к $\frac{1}{2}[f(-\pi) + f(\pi)]$ на концах промежутка.

Позднее было установлено, что если при этом $f(x)$ непрерывна и $f(-\pi) = f(\pi)$, то сходимость будет равномерной. Достаточными условиями равномерной сходимости ряда Фурье являются и такие: $f(x)$ непрерывна на $[-\pi, \pi]$, имеет кусочно-непрерывную производную и $f(-\pi) = f(\pi)$. Существуют и другие, более точные, условия равномерной сходимости. Заметим, что только в случае равномерной сходимости ряда Фурье применим метод Эйлера – Фурье для определения коэффициентов тригонометрического разложения.

Следует подчеркнуть, что Дирихле пытался снять дополнительные условия, налагаемые на функцию $f(x)$, кроме условия непрерывности, при доказательстве сходимости ряда Фурье, но это ему сделать не удалось. И это не случайно – в 1876 году французский математик Дю Буа-Раймон построил первый пример непрерывной на $[-\pi, \pi]$ функции, для которой ряд Фурье расходится в любой наперед заданной точке этого отрезка.

Отметим два результата, относящихся к вопросу о сходимости ряда Фурье и полученных в прошлом столетии. В 1966 году шведский математик Л. Карлесон доказал, что если для функции $f(x)$ существует в смысле Лебега интеграл

$$\int_{-\pi}^{\pi} f^2(x)\,dx,$$

то ее тригонометрический ряд Фурье сходится к этой функции почти всюду на $[-\pi, \pi]$. Эта теорема охватывает все функции, интегрируемые на $[-\pi, \pi]$ промежутке в смысле Римана. Интегрируемости в смысле Лебега недостаточно для сходимости ряда Фурье. В 1923 году А.Н. Колмогоров построил пример интегрируемой на $[-\pi, \pi]$ в смысле Лебега функции, для которой тригонометрический ряд Фурье расходится всюду на этом отрезке.

В 1904 году венгерский ученый Л. Фейер разработал метод суммирования тригонометрического ряда Фурье. Фейер показал, что если $S_k(x)$ – частичные суммы ряда Фурье непрерывной на $[-\pi, \pi]$ функции $f(x)$ такой, что $f(-\pi) = f(\pi)$, то

$$\sigma_n(x) = \frac{S_0(x) + S_1(x) + \ldots + S_{n-1}(x)}{n}$$

равномерно сходится к $f(x)$ на отрезке $[-\pi, \pi]$. Подчеркнем, что при этом тригонометрический ряд Фурье функции $f(x)$ может быть и расходящимся. В 1930 году С.Н. Бернштейн предложил другой способ использования частичных сумм для построения полиномов, равномерно сходящихся к $f(x)$.

3.5. Теория наилучшего среднеквадратичного приближения

Ряды Фурье оказались очень удобным математическим аппаратом и нашли широкое применение в самых различных областях науки в теоретических и прикладных исследованиях. В XX веке была развита теория наилучшего среднеквадратичного приближения. Эта теория связана с обобщенными рядами Фурье

$$f(x) = \sum_{k=1}^{\infty} c_k \varphi_k(x),$$

где $\{\varphi_k(x)\}$ – ортонормированная система функций на отрезке $[a, b]$, а $c_k = \int_a^b f(x)\,\varphi_k(x)\,dx$ – коэффициенты Фурье.

Было показано, что среди обобщенных многочленов

$$P_n(x) = \sum_{k=0}^{n} a_k \varphi_k(x)$$

для функции $f(x)$, интегрируемой с квадратом на отрезке $[a, b]$, наилучшим в смысле среднеквадратичного приближения, т. е. многочленом, обращающим в минимум величину

$$\delta_n = \int_a^b |f(x) - P_n(x)|^2\,dx,$$

является тот, коэффициенты которого $a_k = c_k$ являются коэффициентами Фурье и вычисляются по формуле. При этом

$$\delta_n = \int_a^b f^2(x)\,dx - \sum_{k=0}^{n} c_k^2 .$$

При $n \to \infty$ выполняется неравенство Бесселя

$$\sum_{k=0}^{\infty} c_k^2 \le \int_a^b f^2(x)\,dx.$$

Знак равенства для любой функции, интегрируемой с квадратом, означает, что система φ_k – полная. При этом

$$\lim_{n\to\infty} \int_a^b \left| f(x) - \sum_{k=0}^{n} c_k\,\varphi_k(x) \right|^2 dx = 0,$$

и ряд Фурье сходится в среднем. Тригонометрическая система

$$\frac{1}{\sqrt{2\pi}}, \frac{\cos x}{\sqrt{\pi}}, \frac{\sin x}{\sqrt{\pi}}, \frac{\cos 2x}{\sqrt{\pi}}, \frac{\sin 2x}{\sqrt{\pi}}, \ldots$$

является ортонормированной и полной на отрезке $[-\pi, \pi]$, поэтому тригонометрический ряд Фурье любой кусочно-непрерывной функции сходится к ней на $[-\pi, \pi]$ в среднем.

Оценки $E_n(f)$ при конечных n

Величина наилучшего приближения $E_n(f)$, фигурирующая в теореме Чебышева, зависит от того, к какому классу принадлежит функция $f(x)$.

Принципиальным является следующий из теоремы Вейерштрасса факт, что для непрерывной на $[a, b]$ функции $f(x)$ ее наилучшее приближение $E_n(f) \to \infty$ при $n \to \infty$. Однако весьма важны оценки $E_n(f)$ при конечных n. Такие оценки были получены рядом ученых в первой половине XX века.

Приведем некоторые результаты для приближений алгебраическими многочленами функции $f(x)$, заданной на отрезке $[a, b]$. Следующие две оценки принадлежат Джексону:

1. Если $f(x)$ непрерывна на $[a, b]$ и удовлетворяет условию Липшица с постоянной K, то

$$E_n(f) \le \frac{CK}{n}, C = \text{const}.$$

2. Если $f(x)$ на $[a, b]$ имеет непрерывную производную порядка p, то

$$E_n(f) \le \frac{C(p)}{n^p} M, \left|f^{(p)}(x)\right| \le M, C(p) = \text{const}.$$

Бернштейн доказал теорему о том, что для аналитической функции $f(x)$ $E_n(f)$ убывает с ростом n в геометрической прогрессии

$$E_n(f) \le Cq^n, 0 < q < 1, C = \text{const}.$$

Им доказана и обратная теорема о том, что если для функции величина $E_n(f)$ убывает с ростом n как член геометрической прогрессии со знаменателем $0 < q < 1$, то $f(x)$ – аналитическая функция.

Аналогичные оценки были получены для случая приближения функций с помощью тригонометрических многочленов. Существует теорема Вейерштрасса о том, что для функции $f(x)$, имеющей период 2π и непрерывной на отрезке $[-\pi, \pi]$, существует тригонометрический многочлен $P_n(f)$ степени n такой, что

$$|f(x) - P_n(x)| \le \varepsilon, n = n(\varepsilon),$$

для любого ε. Отсюда следует, что величина $E_n(f)$ наилучшего приближения с помощью тригонометрического многочлена стремится к нулю при $n \to \infty$.

Джексоном дана оценка

$$E_n(f) \le \frac{\ln n}{n^k} CM, C = \text{const},$$

если $f(x)$ имеет непрерывные производные $f^{(k)}(x)$, и $\left|f^{(k)}(x)\right| \le M$. Как и для случая алгебраических многочленов справедлива оценка, установленная Бернштейном, для наилучшего приближения аналитической функции

$$E_n(f) \le Cq^n, \qquad 0 < q < 1, \qquad C = \text{const}.$$

3.6. Численное интегрирование

Одновременно с разработкой методов интерполяции осуществлялось использование интерполяционных многочленов для целей численного дифференцирования и интегрирования. Имеем

$$f(x) = L_n(x) + R_n(x),$$

где $L_n(x)$ – многочлен Лагранжа, построенный по узлам $a = x_0, x_1, x_2, \ldots, x_n = b$. Производную $f^{(k)}(x)$ заменяют на $L_n^{(k)}(x)$:

$$f^{(k)}(x) = L_n^{(k)}(x) + R_n^{(k)}(x).$$

В вычислительной практике широко пользуются этими формулами. Следует подчеркнуть, что для больших k могут сильно нарастать погрешности. Говорят, что процесс численного дифференцирования неустойчив или что задача численного дифференцирования некорректна.

Интегрирование дает

$$\int_a^b f(x)\,dx = \int_a^b L_n(x)\,dx + \overline{R_n}.$$

В случае равноотстоящих узлов $x_i = a + ih$, $h = \dfrac{b-a}{n}$, $i = 0 \div n$, отсюда следует квадратурная формула

$$\int_a^b f(x)\,dx = \sum_{i=0}^{n} A_i f(x_i) + \overline{R_n},\ A_i = \int_a^b \frac{\omega(x)}{(x - x_i)\omega'(x_i)}\,dx.$$

Квадратурные формулы такого типа носят название формул Ньютона – Котеса. Наиболее употребительны формулы при $n = 1$ и $n = 2$. При $n = 1$ это формула трапеций. Обычно ее применяют к каждому из отрезков $[x_{i-1}, x_i]$, что дает

$$\int_a^b f(x)\,dx = h\frac{f(a) + f(b)}{2} + h\sum_{i=1}^{n-1} f(x_i) + \overline{R_1},$$

$$\overline{R_1} = -\frac{(b-a)h^2}{12} f''(\xi), a \le \xi \le b.$$

При $n = 2$ это формула Симпсона:

$$\int_a^b f(x)\,dx = \frac{h}{3}\,[f(x_0) + 4f(x_1) + 2f(x_2) + 4f(x_3) + \ldots + 4f(x_{2n-1}) +$$

$$+ f(x_{2n})] + \overline{R_2},$$

$$\overline{R_2} = -\frac{(b-a)h^4}{180} f^{(IV)}(\xi), a \le \xi \le b, h = \frac{b-a}{2n}.$$

Остаточный член формулы Ньютона – Котеса обращается в нуль, если $f(x)$ – произвольный многочлен степени n. Знаменитый немецкий математик Гаусс показал, что степень многочлена, для которого квадратурная формула точна, можно повысить с помощью выбора узлов интерполирования.

Гаусс получил свою квадратурную формулу путем специального выбора узлов интерполирования. Задача формулируется так: определить в квадратурной формуле

$$\int_a^b \rho(x) f(x)\, dx = \sum_{i=0}^{n} C_i f(x_i)$$

коэффициенты C_i и узлы x_i, $i = 0 \div n$, так, чтобы она была точна для многочленов степени $2n - 1$ при фиксированном n и весовой функции $\rho(x)$. Справедлива следующая теорема: формула точна для многочленов степени $2n - 1$ тогда и только тогда, когда выполнены условия:

а) многочлен $\omega(x) = (x - x_0) \ldots (x - x_n)$ ортогонален с весом $\rho(x)$ любому многочлену $q(x)$ степени меньше $n + 1$:

$$\int_a^b \rho(x)\omega(x)q(x)\, dx = 0;$$

б)

$$C_i = \int_a^b \rho(x) \frac{\omega(x)}{(x - x_i)\omega'(x_i)}\, dx, i = 0 \div n.$$

Важными являются два частных случая формулы для отрезка $[-1, 1]$. Один из них – это формула Гаусса – Чебышева или формула Эрмита с весом $\rho(x) = (1 - x^2)^{-1/2}$. Она имеет вид

$$\int_{-1}^{1} \frac{f(x)}{\sqrt{1 - x^2}} dx \approx \sum_{i=1}^{n} C_i f(x_i).$$

В этом случае $\omega(x) = T_n(x) = \frac{1}{2^{n-1}} \cos(n \arccos x)$ – многочлен Чебышева,

$$x_i = \cos \frac{2i - 1}{2n} \pi, \quad C_i = \frac{\pi}{n}.$$

Второй случай – это формула Гаусса – Лежандра с весом $\rho(x) = 1$:

$$\int_{-1}^{1} f(x)\, dx \approx \sum_{i=1}^{n} C_i f(x_i).$$

Здесь $\omega(x) = P_n(x)$ – многочлен Лежандра:

$$\omega(x) = P_n(x) = \frac{1}{2^n n!}\frac{d^n}{dx^n}[(x^2-1)^n],\ P_0(x) = 1.$$

$P_n(x)$ на [−1, 1] имеет n различных корней. Коэффициенты C_i определяются по формуле

$$C_i = \frac{2(1-x_i^2)}{n^2 P_{n-1}^2(x_i)}.$$

Выводы

Рассмотрены вопросы интерполирования и наилучшего равномерного приближения функций в их историческом развитии. Описан вклад П.Л. Чебышева в создание теории наилучшего равномерного приближения функций многочленами. Обсуждены вопросы развития теории наилучшего среднеквадратичного приближения.

Контрольные вопросы

1. Сформулируйте постановку задачи интерполирования.
2. Дайте определение многочлена Лагранжа.
3. Дайте определение многочлена Ньютона.
4. Сформулируйте постановку обобщенной задачи интерполирования.
5. Дайте определение квадратурной формулы.
6. Дайте определение обобщенного ряда Фурье.
7. Дайте определение ряда Фурье.
8. Дайте определение непрерывной функции.
9. Дайте определение ортонормированной системы функций.
10. Что понимается под точностью интерполяционного многочлена?

ЗАКЛЮЧЕНИЕ

Русский математик П.Л. Чебышев о связи математической теории и практики писал: «Сближение теории с практикой дает самые благотворные результаты, и не одна только практика от этого выигрывает; сами науки развиваются под влиянием ее: она открывает им новые предметы для исследования или новые стороны в предметах давно известных» [Цит. по: 53].

В XX веке новые проблемы, появившиеся в физике, биологии, экономике и других областях знания, стимулировали развитие математики. Развитие информационных технологий способствовало появлению новых возможностей применения математики. Появилась возможность проводить фундаментальные исследования не только в теоретической, но и прикладной области. Решение сложных задач стало возможным при использовании формальных и неформальных подходов, при применении вычислительных экспериментов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 года № 373-ст : взамен ГОСТ Р 50922–96 : дата введения 2008-02-01 / Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю. – Москва : Стандартинформ, 2008. – IV, 8 с.
2. ГОСТ Р 51188–98. Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство : государственный стандарт Российской Федерации : издание официальное : принят и введен в действие Постановлением Госстандарта России от 14 июля 1998 года № 295 : введен впервые : дата введения 1999-07-01 / Центральный научно-исследовательский институт Министерства обороны Российской Федерации, Научно-консультационный центр по созданию и применению информационных технологий. – Переизд. – Москва : Госстандарт России, 2003. – III, 6 с.
3. Жиров, А. О. Безопасные облачные вычисления с помощью гомоморфной криптографии / А. О. Жиров, О. В. Жирова, С. Ф. Кренделев // Безопасность информационных технологий. – 2013. – Т. 20, № 1. – С. 6–12.
4. Бауэр, Ф. Расшифрованные секреты : Методы и принципы криптологии / Ф. Бауэр ; пер. с 3-го англ. изд. В. И. Ахмолина, В. И. Петрова ; под ред. А. В. Чашкина. – Москва : Мир, 2007. – 550, [15] с. – ISBN 5-03-003551-6.
5. Блинов, А. М. Информационная безопасность. Учебное пособие. Часть 1 / А. М. Блинов. – Санкт-Петербург : Изд-во Санкт-Петербургского государственного университета экономики и финансов, 2010. – 98 с. – URL: www.studfiles.ru/preview/2880351/ (дата обращения: 25.12.2021).

6. Буртыка, Ф. Б. Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов // Труды Института системного программирования РАН. – 2014. – Т. 26, № 5. – С. 99–116.
7. Варновский, Н. П. Математическая криптография. Несколько этюдов // Московский университет и развитие криптографии в России : Материалы конференции в МГУ, 17–18 октября 2002 года / ред. В. В. Ященко. – Москва, 2003. – С. 98–121.
8. Варновский Н. П. Гомоморфное шифрование / Н. П. Варновский, А. В. Шокуров // Труды Института системного программирования РАН. – 2007. – Т. 12. – С. 27–36.
9. Венбо, М. Современная криптография: теория и практика / М. Венбо ; пер. с англ. и ред. Д. А. Клюшина. – Москва : Вильямс, 2005. – 768 с. – URL: www.booksshare.net/index.php?id1=4&category=cryptography&author=venbo-mao&book=2005&page=1 (дата обращения: 15.06.2021). – ISBN 5-8459-0847-7.
10. Галатенко, В. А. Идентификация и аутентификация, управление доступом // Основы информационной безопасности : учеб. пособие / В. А. Галатенко. – 3-е изд. (электрон.). – Москва [и др.], 2020. – С. 154–178. – URL: www.iprbookshop.ru/97562.html (дата обращения: 15.06.2021). – Режим доступа: по подписке.
11. Горбатов, В. С. Основы технологии PKI / В. С. Горбатов, О. Ю. Полянская. – Москва : Горячая линия-Телеком, 2011. – 247, [1] с. – ISBN 978-5-9912-0213-8.
12. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации / Ю. Н. Загинайлов. – Москва [и др.] : Директ-Медиа, 2015. – 255 с. – ISBN 978-5-4475-3946-7.
13. Касперски, К. Записка исследователя компьютерных вирусов / К. Касперски. – Санкт-Петербург [и др.] : Питер, 2006. – 316 с. – ISBN 5-469-00331-0.
14. Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц. – Москва : Научное издательство ТВП, 2001. – X, 254 с.
15. Сингх, С. Книга шифров : Тайная история шифров и их расшифровки / С. Сингх ; пер. с англ. А. Галыгина. – Москва : АСТ [и др.], [2009]. – 447 с. – URL: www.vixri.ru/d/Singx%20Sajmon%20_Kniga%20shifrov.pdf (дата обращения: 15.06.2021). – ISBN 978-5-17-038477-8.

16. Скрипник, Д. А. Общие вопросы технической защиты информации : учеб. пособие / Д. А. Скрипник. – 3-е изд. (электрон.). – Москва [и др.] : Интернет-Университет Информационных технологий [и др.], 2020. – 424 с. – URL: www.iprbookshop.ru/89451.html (дата обращения: 20.06.2021). – Режим доступа: по подписке. – ISBN 978-5-4497-0336-1.
17. Фостер, Дж. К. Разработка средств безопасности и эксплойтов / Дж. К. Фостер, В. Лю. – Москва [и др.] : Русская Редакция [и др.], 2007. – 418 стр. – ISBN 978-5-7502-0301-7.
18. Цирлов, В. Л. Основы информационной безопасности автоматизированных систем : краткий курс / В. Л. Цирлов. – Ростов-на-Дону : Феникс, 2008. – 173 с. – ISBN 978-5-222-13164-0.
19. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин. – Москва : ДМК Пресс, 2012. – 592 с. – ISBN 978-5-94074-833-5.
20. Введение в криптографию / В. В. Ященко, Н. П. Варновский, Ю. В. Нестеренко [и др.] ; под ред. В. В. Ященко – 4-е изд., доп. – Москва : МЦНМО, 2012. – 342 с. – URL: klex.ru/ptt (дата обращения: 20.06.2021). – ISBN 978-5-4439-0026-1.
21. Frolova, E. Самые популярные социальные сети в России // Про СММ : пишем просто о сложном : [блог]. – URL: www.pro-smm.com/populyarnye-socialnye-seti-v-rossii/ (дата обращения: 19.06.2021). – Дата публикации: 31.10.2014.
22. Shamir, A. The Search for Provably Secure Identification Schemes // Proceedings of the International Congress of Mathematicians / Ed. by A. M. Gleason. – Berkeley, 1986. – Vol. 2. – P. 1488–1495.
23. Menezes, A. J. The ElGamal signature scheme / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone // Handbook of applied cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. – Boca Raton [et al.], 1997. – P. 454–459.
24. On the (Im)possibility of obfuscating programs / B. Barak, O. Goldreich, R. Impagliazzo [et al.] // Advances in Cryptology – CRYPTO 2001 : 21st Annual International Cryptology Conference : Proceedings / Ed. J. Kilian. – Berlin [et al.], 2001. – P. 1–18. – (Lecture Notes in Computer Science ; vol. 2139).

25. Brakerski, Z. (Leveled) Fully Homomorphic Encryption without Bootstrapping / Z. Brakerski, C. Gentry, V. Vaikuntanathan // ITCS '12: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. – New York, 2012. – P. 309–325.
26. Социальные сети в России, весна 2015. Цифры, тренды, прогнозы // Brand Analytics : [сайт]. – URL: br-analytics.ru/blog/socialnye-seti-v-rossii-vesna-2015-cifry-trendy-prognozy/ (дата обращения: 21.12.2021).
27. Boyd, D. Social Network Sites: Definition, History, and Scholarship / D. Boyd, N. Ellison // Journal of Computer-Mediated Communication. – 2007. – Vol. 13, № 1. – P. 210–230.
28. Maimut, D. S. Homomorphic encryption schemes and applications for secure digital world / D. S. Maimut, A. Patrascu, E. Simion // Journal of Mobile, Embedded and Distributed Systems. – 2012. – Vol. 4, № 4.
29. Boneh, D. Evaluating 2-DNF Formulas on Ciphertexts / D. Boneh, E.-J. Goh, K. Nissim // Theory of Cryptography : Second Theory of Cryptography Conference : Proceedings / Ed. J. Kilian. – Berlin [et al.], 2005. – P. 325–341. – (Lecture Notes in Computer Science ; vol. 3378).
30. Ellis, J. The Internet Security Guidebook : From Planning to Deployment / J. Ellis, T. Speed ; Ed. E. Carrasco. – San Diego [et al.] : Academic Press, 2001. – 243 p. – ISBN 978-0122374715.
31. ISO/IEC 10118-3:2018. Information technology – Security techniques – Hash-functions. Part 3: Dedicated hash-functions : international standard : cancels and replaces ISO/IEC 10118-3:2004 / prepared by Joint Technical Committee ISO/IEC JTC 1. – Geneva : ISO [et al.], 2018. – VII, 399 p.
32. Kitsos, P. Efficient architecture and hardware implementation of the Whirlpool hash function / P. Kitsos, O. Koufopavlou // IEEE Transactions on Consumer Electronics. – 2004. – Vol. 50, № 1. – P. 208–213.
33. Fully Homomorphic Encryption over the Integers / M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan // Advances in Cryptology – EUROCRYPT 2010 : 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques : Proceedings / Ed. H. Gilbert. – Berlin [et al.], 2010. – P. 24–43. – (Lecture Notes in Computer Science ; vol. 6110).

34. Paillier, P. Public-Key Cryptosystem Based on Composite Degree Residuosity Classes // Advances in Cryptology – EUROCRYPT '99 : International Conference on the Theory and Application of Cryptographic Techniques : Proceedings / Ed. J. Stern. – Berlin, 1999. – P. 223–238. – (Lecture Notes in Computer Science ; vol. 1592).
35. Poulsen, K. Kingpin : How One Hacker Took Over the Billion Dollar Cyber Crime Underground / K. Poulsen. – New York : Crown Publishers, 2011. – 432 p.
36. Березин, И. С. Методы вычислений : [в 2 томах] / И. С. Березин, Н. П. Жидков. – Москва : Физматгиз, 1959. – 2 т.
37. Бурбаки, Н. Очерки по истории математики / Н. Бурбаки ; пер. с фр. И. Г. Башмаковой ; под ред. К. А. Рыбникова. – Москва : Изд-во иностранной литературы, 1963. – 291, [1] с.
38. Болгарский, Б. В. Очерки по истории математики / Б. В. Болгарский. – 2-е изд., испр. и доп. – Минск : Вышэйшая школа, 1979. – 368 с.
39. Вилейтнер, Г. История математики от Декарта до середины XIX столетия / Г. Вилейтнер ; под ред. А. П. Юшкевича. – 2-е изд. – Москва : Наука, 1966. – 507 с.
40. История математики с древнейших времен до начала XIX столетия. В 3 томах. Том 1. С древнейших времен до начала нового времени / [И. Г. Башмакова, Э. И. Березкина, А. И. Володарский и др.] ; под ред. А. П. Юшкевича. – Москва : Наука, 1970. – 351 с.
41. История математики с древнейших времен до начала XIX столетия. В 3 томах. Том 2. Математика XVII столетия / [И. Г. Башмакова, Л. Е. Майстров, Б. А. Розенфельд и др.] ; под ред. А. П. Юшкевича. – Москва : Наука, 1970. – 300 с.
42. История отечественной математики. В 4 томах. Том 1. С древнейших времен до конца XVIII в. / [И. З. Штокало, А. Н. Боголюбов, М. Ю. Брайчевский и др.] ; отв. ред. И. З. Штокало. – Киев : Наукова думка, 1966. – 491, [1] с.
43. История отечественной математики. В 4 томах. Том 2. 1801–1917 / [С. Н. Киро, И. Я. Депман, Н. А. Чайковский и др.] ; отв. ред. И. З. Штокало. – Киев : Наукова думка, 1967. – 615, [1] с.
44. История отечественной математики. В 4 томах. Том 3. 1917–1967 / [А. Н. Боголюбов, Б. Б. Венков, Ю. В. Линник и др.] ; отв. ред. И. З. Штокало. – Киев : Наукова думка, 1968. – 725, [1] с.

45. История отечественной математики. В 4 томах. Том 4. Книга 1. 1917–1967 / [А. А. Гольдберг, А. А. Гончар, Б. Я. Левин и др.] ; отв. ред. И. З. Штокало. – Киев : Наукова думка, 1970. – 883 с.
46. История отечественной математики. В 4 томах. Том 4. Книга 2. 1917–1967 / [Б. В. Гнеденко, И. И. Гихман, А. В. Скороход и др.] ; отв. ред. И. З. Штокало. – Киев : Наукова думка, 1970. – 666, [2] с.
47. Клейн, Ф. Лекции о развитии математики в XIX столетии. Том 1 / Ф. Клейн ; сост. Р. Курантом, О. Нейгебауер ; пер. с нем. Н. М. Нагорного ; под ред. М. М. Постникова. – Москва : Наука, 1989. – 453, [1] с. – ISBN 5-02-013920-3.
48. Колмогоров, А. Н. Математика в ее историческом развитии / А. Н. Колмогоров ; под ред. В. А. Успенского. – Москва : Наука, 1991. – 221, [2] с. – ISBN 5-02-014453-3.
49. Рыбников, К. А. История математики : [учеб. пособие] / К. А. Рыбников. – 2-е изд. – Москва : Изд-во Московского университета, 1974. – 455 с.
50. Стройк, Д. Я. Краткий очерк истории математики / Д. Я. Стройк ; пер. с нем. И. Б. Погребысского. – 5-е изд., испр. – Москва : Наука, 1990. – 251, [2] с. – ISBN 5-02-014329-4.
51. Хрестоматия по истории математики : Математический анализ. Теория вероятностей : учеб. пособие для вузов / [сост. И. Г. Башмакова, Ю. А. Белый, С. С. Демидов и др.] ; под ред. А. П. Юшкевича. – Москва : Просвещение, 1977. – 224 с.
52. Юшкевич, А. П. История математики в России до 1917 года / А. П. Юшкевич. – Москва : Наука, 1968. – 591 с.
53. Петров, Ю. П. История и философия науки : Математика, вычислительная техника, информатика : [учеб. пособие] / Ю. П. Петров. – Санкт-Петербург : БХВ-Петербург, 2005. – 441 с.
54. Русанов, В. В. История и методология прикладной математики / В. В. Русанов, Г. С. Росляков. – Москва : Факультет вычислительной математики и кибернетики МГУ им. М. В. Ломоносова, 2004. – 240, [1] с. – ISBN 5-89407-208-5.
55. Фрейман, Л. С. Творцы высшей математики / Л. С. Фрейман. – Москва : Наука, 1968. – 216 с.

ГЛОССАРИЙ

Асимметричные криптосистемы (системы открытого шифрования) – криптосистемы, в которых для зашифрования и расшифрования используются разные преобразования.

Аутентифика́ция – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Криптоанализ – посвящен исследованию возможности чтения сообщений без знания ключей и связан непосредственно со взломом шифров. Люди, занимающиеся криптоанализом и исследованием шифров, называются криптоаналитиками.

Криптографическая система – семейство преобразований шифра и совокупность ключей (т. е. алгоритм + ключи).

Криптография – наука о создании безопасных методов связи, стойких (устойчивых к взлому) шифров. Она занимается поиском математических методов преобразования информации.

Симметричные криптосистемы (с секретным ключом – *secret key systems*) – криптосистемы, которые построены на основе сохранения в тайне ключа шифрования. Процессы зашифрования и расшифрования используют один и тот же ключ.

Стеганогра́фия (пер. с греч. «тайнопись») – это наука о скрытой передаче информации путем сохранения в тайне самого факта передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование. Стеганография не заменяет, а дополняет криптографию.

Хеширование (иногда хэширование, англ. *hashing*) – преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются хеш-функциями или функциями свёртки, а их результаты называют хешем, хеш-кодом или дайджестом сообщения (англ. *message digest*).

Шифр – совокупность обратимых преобразований множества открытых текстов (т. е. исходного сообщения) во множество зашифрованных текстов, проводимых с целью их защиты. Конкретный вид преобразования определяется с помощью ключа шифрования.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП. Значение реквизита получается в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП.