Краткий исторический очерк развития криптографии

В.А. Носов

Из материалов конференции "Московский университет и развитие криптографии в России" (МГУ, 17-18 октября 2002 г.).

1. Введение

В настоящее время нет недостатка в материалах по истории криптографии - достаточно заглянуть на соответствующие сайты Интернет. В данном очерке делается попытка проследить историю криптографии и присутствия в ней математиков. Основное внимание уделено не именам и датам, а развитию криптографических идей и участию в этом процессе математиков.

2. 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-х способов преобразования текста. Среди них написание знаков не по порядку, а вразброс по некоторому правилу. Многие из приводимых способов следует рассматривать как криптографические, т. е. обеспечивающие секретность переписки. Приведена система замены букв. Упоминается, что тайнопись является одним их 64-х искусств, которым следует владеть как мужчинам, так и женщинам.

Более достоверные сведения о применяемых системах шифров относятся к периоду возникновения государств древней Греции. В Спарте в V-VI 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 5x5, 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.

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.

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

Э. Шюре в книге "Великие посвященные" сообщает, что "с великим трудом и большой ценой добыл Платон один из манускриптов Пифагора, который никогда не записывал свое эзотерическое учение иначе, как 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.

3. 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 ее Шехаб аль Кашканди. В данной энциклопедии содержится раздел о криптографии, в котором приводятся описания всех известных способов шифрования. В этом разделе имеется 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 Муса 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 (ок. 1427) аль Каши, сотрудником Улугбека.

4. Криптография в эпоху Возрождения (XIV-XVI вв.)

До эпохи Возрождения имеется мало сведений о применяемых шифрах. Известен ряд значковых шифров, при котором буквы открытого текста заменяются на специальные знаки. Таким является шифр Карла Великого (780-814 г.). 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.

В эпоху Возрождения в итальянских городах-государствах стали расцветать 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 шифртексте. 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 Клементия XII, "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, названный "Миланский ключ", представляющий собой значковый шифр пропорциональной замены.

В 1466 году Леон Альберти, знаменитый архитектор и философ 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 "шифр, достойный 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.

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 века 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.

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 тонкостях", в которой имеется часть, посвященная криптографии. Его вклад содержит два предложения. Первое - использовать открытый текст в качестве ключа. Второе - он предложил шифр, называемый ныне "Решетка Кардано". Кроме данных предложений Кардано дает "доказательство" стойкости шифров, основанное на подсчете числа ключей.

В том же XVI веке был сделан еще существенный шаг в развитии криптографии. Блез 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". 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 у Ф. Виета, 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.

5. 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 появляется 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 при Людовике XIV по предложению кадинала 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, при котором открытый текст разбивается на отрезки, а внутри каждого отрезка буквы переставляются в соответствии с фиксированной перестановкой.

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

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 шифрвеличин.

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 это время применяются для шифрования коды, как приложения к "цифирным азбукам". В знаменитом "деле царевича Алексея" в обвинительных материалах фигурировали и "цифирные азбуки".

Математика XVII-XVIII века получает существенное и качественно новое развитие. Н. Бурбаки называют этот период "героической эпохой". Назовем только некоторых авторов открытий. Изобретатель логарифмов - Дж. 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.

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

Ньютон Исаак (1643-1727) - английский физик и математик и Готфрид Лейбниц (1646-1716) - немецкий философ и математик разработали дифференциальное и интегральное исчисление. Не имеется данных о привлечении этих математиков к шифровальной работе, но есть данные о том, что некоторые их них владели криптографией (Паскаль, Ньютон, Лейбниц). Увлекался криптографией и знаменитый английский философ Ф. Бекон (1561-1626), которому принадлежит идея двоичного кодирования.

Якоб Бернулли (1654-1705), 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.

Для развития математики в России большую роль сыграла "Арифметика" Магницкого Л. Ф., изданная в 1703 году, которую М. В. Ломоносов назвал "вратами учености". Она 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 году в Россию приезжает Леонард Эйлер (1707-1783), который принимал участие в разработке шифров. Ему принадлежат исследования по перечислению и построению латинских квадратов, т. е. 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), в России с 1757 года, известный математик и физик, изучавший математическими методами электромагнитные явления.

Таким образом, в XVII-XVIII веках в математике закладываются основы аппарата, применяемого в криптографии для анализа шифров и дешифрования. Основным средством для шифрования становятся коды.

6. 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. Ф. 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 в области шифрованной связи 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. 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 новым вкладом в криптографию было изложение метода 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 шифртексте будут равны или кратны периоду лозунга, т. е. его длине. После определения длины лозунга шифртекст 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 Кергоффс, 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.

Другой его вывод: только криптоаналитики могут судить о качестве шифра. Кергоффс впервые делает различие между секретностью шифрсистемы и секретностью ключа. И вводит требование секретности по ключу и не требует секретности системы. Это требование сохраняет свое значение и в современной криптографии.

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

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 и 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.

Математика XIX века характеризуется революционными открытиями, ломающими привычные представления. В первую очередь следует назвать открытие Н. И. Лобачевским неевклидовой геометрии. Его сочинение " О началах геометрии " было напечатано в журнале "Казанский вестник" в 1829 году. Сходные результаты были получены Я. Больяи в 1832 году. Больцано Б. и позднее Вейерштрасс К. 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, т. е. применялся метод, при котором рассуждение о математических объектах сводится к рассуждению о натуральных числах. Начала формироваться новая математическая дисциплина - метаматематика, которая, по Д. Гильберту, исследует математические доказательства финитными методами.

На математическом конгрессе 1900 года в Париже известный немецкий математик Д. Гильберт, формулируя актуальные проблемы математики, на место N 2 в списке проблем ставит вопрос о непротиворечивости арифметики, а на место N 1 проблему Кантора о мощности континуума.

Заметим, что под N 8 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 важное значение для криптографии в связи с построением алгоритмов факторизации чисел.

7. Криптография в XX веке

XX век - век двух мировых войн, век научно-технического прогресса, век 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 шифрсредством 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 Плейфер (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 - Ранненкампа и Самсонова в Восточной Пруссии в августе 1914 года, которое произошло из-за плохой организации шифрсвязи 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 шифртекста. В этот период получили развитие методы дешифрования, основанные на парах открытых и шифрованных текстов, на шифртекстах, 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.

Другое новшество этого периода - появление специализации в криптографической деятельности. Появляются группы по дешифрованию кодов и по дешифрованию полевых шифров, по добыче перехвата, по обработке информации, полученной из открытых и агентурных источников и т. д.

Между мировыми войнами появляются во всех ведущих странах электромеханические шифраторы. Они были двух типов - на коммутационных дисках или роторах и на цевочных дисках. Примером первого типа является известная шифрмашина "Энигма", которой были оснащены германские сухопутные войска. Примером второго типа является американская шифрмашина 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-х 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. Шифрмашина М-209 состояла из 6 колес размера 26, 25, 23, 21, 19, 17, каждое из которых имело выступы и по окружности. Эта 6-мерная комбинация выступов (их число 64) с помощью механического устройства превращалась в число, на которое сдвигается буква открытого текста. Изменение угловых положений дисков осуществлялось равномерным их вращением. Ясно, что шифратор реализует шифр гаммирования. Советский Союз производил шифрмашины обоих названных типов.

Таким образом, перед второй мировой войной все ведущие страны имели на вооружении электромеханические шифрсистемы, 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, а шифровальные службы были непосредственным участником военных действий. 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 данных работах были сформулированы и доказаны математическими средствами необходимые и достаточные условия недешифруемости системы шифра. Они заключаются в том, что получение противником шифртекста 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 этот период в криптографической работе. 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. Куллбак - крупный специалист по математической статистике, в Советском Союзе крупные 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 - крупный специалист по теории чисел, известный решением проблемы Гильберта N 7 о трансцендентности степеней алгебраических чисел.

8. О криптографии нового времени

Начиная с 50-х годов криптография становится "электронной". Это означает, что 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 становиться 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. Этот процесс получил развитие и 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 ученые 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 - Райвест, Шамир, Адлеман, в которой 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 проблеме "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.

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 понятию 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 "третьей грамотностью" наравне со "второй грамотностью" - владением компьютером и информационными технологиями.

Литература

1. Соболева Т. А. Тайнопись в истории России. М.: 1994.
2. Kahn D. Codebreakers. N. Y.: 1967.
3. Жельников В. Криптография от папируса до компьютера. М.: 1996.
4. Brassard G. Modern Cryptology. Springer-Verlag, 1988.
5. Саломаа А. Криптография с открытым ключом. М.: 1996.
6. Schneier B. Applied Cryptography. John Wiley & Sons, 1996.
7. Диффи У., Хеллмэн М. Защищенность и имитостойкость: Введение в криптографию. ТИИЭР, 1979, **67**, N 3.
8. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. М.: 2001.
9. Чмора А. Л. Современная прикладная криптография. М.: 2001.
10. Математическая энциклопедия. Т. 1-5, М.: 1977-1985.