А. А. Молдовян, Н. А. Молдовян, Н. Д. Гуц, Б. В. Изотов

Криптография
Скоростные шифры

НАУЧНОЕ ИЗДАНИЕ

bhv®

А. А. Молдовян
Н. А. Молдовян
Н. Д. Гуц
Б. В. Изотов

Криптография
Скоростные шифры

Санкт-Петербург
«БХВ-Петербург»
2002

УДК 681.3
ББК 32.81
М75

Рецензенты:
доктор технических наук, профессор В. И. Воробьев
доктор технических наук, профессор А. М. Чуднов

Молдовян А. А. и др.

М75 Криптография: скоростные шифры. — СПб.: БХВ-Петербург, 2002. — 496 с.: ил.

ISBN 5-94157-214-X

В книге рассматривается широкий круг вопросов, связанных с использованием криптографических методов защиты информации в компьютерных системах. Впервые излагается разработанная авторами концепция управляемых преобразований, являющаяся новым направлением прикладной криптографии. Представлены варианты построения управляемых операций и анализ их основных криптографических свойств. Дается описание ряда новых криптографических примитивов и скоростных криптосистем с оценкой их стойкости к дифференциальному, линейному и другим методам криптоанализа. Показана возможность построения операционных блоков, реализующих уникальные модификации операций для каждого значения управляющего кода. Отражены вопросы построения управляемых перестановок и управляемых подстановочных операций, в частности, управляемых сумматоров специального типа, а также представлены методы конструирования скоростных итеративных шифров на их основе.

Для специалистов в области безопасности информации, криптографии, прикладной математики, информатики и электроники, а также для преподавателей, студентов и аспирантов инженерно-технических вузов

УДК 681.3
ББК 32.81

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Анна Кузьмина*
Редактор	*Григорий Добин*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн обложки	*Игоря Цырульникова*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 19.09.02.
Формат 70×100$^{1}/_{16}$. Печать офсетная. Усл. печ. л. 39,99.
Тираж 3000 экз. Заказ №
"БХВ-Петербург", 198005, Санкт-Петербург, Измайловский пр., 29.

Гигиеническое заключение на продукцию, товар № 77.99.02.953.Д.001537.03.02
от 13.03.2002 г. выдано Департаментом ГСЭН Минздрава России.

Отпечатано с готовых диапозитивов
в Академической типографии "Наука" РАН
199034, Санкт-Петербург, 9 линия, 12.

ISBN 5-94157-214-X

Содержание

Введение

В настоящее время криптографические методы нашли широкое применение не только для защиты информации от несанкционированного доступа, но и в качестве основы многих новых электронных информационных технологий — электронного документооборота, электронных денег, тайного электронного голосования и др. Современная криптография решает следующие три основные проблемы:

- обеспечение конфиденциальности (секретности);
- обеспечение аутентификации информации и источника сообщений;
- обеспечение анонимности (например, сокрытие перемещения электронных денег от одного субъекта к другому).

Первая проблема известна тысячи лет, последние же две являются относительно новыми, и с их решением связан ряд перспективных направлений теоретической и практической криптографии. Тем не менее, традиционная криптографическая задача обеспечения секретности информации не утратила своей остроты и в настоящее время. Это связано, главным образом, с тем, что в эпоху массового применения компьютерных технологий задача защиты электронной информации приобрела характер широкомасштабной проблемы. При этом к алгоритмам шифрования предъявляются жесткие технологические требования, которые продиктованы их использованием в различных электронных устройствах (телекоммуникационных системах, ЭВМ, компьютерных сетях, интеллектуальных электронных карточках и др.). Характерным для технологических применений криптографических средств является возрастание требований к шифрам одновременно по стойкости, скорости и по простоте реализации. Ужесточение требований по стойкости обусловлено тем, что разностороннее использование криптографии связано с более широкими возможностями для атакующего следовать особенностям конкретных условий, в которых функционирует криптосистема (например, имеются возможности: первая — осуществить внешнее воздействие на устройство шифрования с целью вызвать случайные аппаратные сбои, вторая — выпол-

нить замер потребляемой мощности, третья — определить время вычислений и т. п.). Возросшие требования по скорости связаны с необходимостью сохранения высокой производительности автоматизированных систем после встраивания в них механизмов защиты. Простота аппаратной реализации необходима для снижения стоимости средств шифрования, что будет способствовать их массовому применению и более широким возможностям встраивания в портативную аппаратуру. В силу специфики представления информации в цифровых устройствах наибольший интерес представляют блочные шифры, которые могут, например, обеспечить произвольный доступ к данным на зашифрованных магнитных носителях.

Таким образом, разработка скоростных блочных шифров является важной задачей прикладной криптографии. В этом направлении сделано большое число предложений со стороны российских и зарубежных криптографов. Характерным для большинства новых скоростных шифров является использование предвычислений, осуществляющих расширение секретного ключа. При создании программных шифров применение сложных алгоритмов предвычислений с целью упрощения шифрующих преобразований во многих приложениях является оправданным. При разработке шифров двойной (программной и аппаратной) ориентации, например нового американского стандарта AES, криптографы также в первую очередь учитывают возможности современных массовых процессоров, полагая, что существующая микроэлектронная технология легко может обеспечить аппаратную реализацию весьма сложных алгоритмов преобразования. Однако при массовом использовании устройств шифрования в компьютерных и телекоммуникационных системах, интеллектуальных электронных карточках экономия аппаратных ресурсов является крайне важной. Наиболее экономичные решения позволяют изготовить более дешевые и более надежные устройства, а также снизить потребляемую мощность.

В ряде сетевых приложений требуется обеспечить высокую скорость шифрования при частой смене ключей, что ограничивает применение шифров с предвычислениями, поскольку последние вносят существенные ограничения по быстродействию. В связи с этим весьма важным становится уменьшение сложности предвычислений при сохранении высокой криптостойкости преобразования. В этом плане удачным решением представляется полный отказ от предварительного преобразования секретного ключа путем замены этой процедуры операциями преобразования подключей в зависимости от преобразуемых данных, которые выполняются одновременно с операциями преобразования данных. Таким образом, актуальной является разработка скоростных шифров нового поколения, допускающих экономичную аппаратную реализацию и сохраняющих высокую скорость шифрования при частой смене ключей. При этом криптосистемы должны обладать высокой стойкостью к классическим вариантам атак на основе известных и специально подобранных текстов, а также к новым атакам, например, на основе генерации случайных аппаратных ошибок.

Одним из перспективных направлений построения скоростных шифров является использование гибких операций и/или процедур преобразования. В случае программной реализации, например, легко реализуются криптосистемы, в которых на этапе предвычислений формируется алгоритм шифрования в зависимости от секретного ключа, что может быть сделано путем настройки операций преобразования в зарезервированных местах алгоритма или путем комбинирования процедур преобразования из некоторого специфицированного подмножества шифрующих функций (библиотеки процедур преобразования). Такие шифры можно назвать *гибкими*. В действительности, гибкие блочные алгоритмы с размером входа, равным b битов, формально описываются так же, как и любой другой шифр, — одноалфавитной подстановкой на множестве возможных входных текстов длиной b. Однако, с учетом ориентации на стандартные операции микропроцессора, оправданным и удобным является описание таких шифров в терминах настройки алгоритма. Данный подход к построению гибких аппаратных шифров может быть применен при использовании микропроцессорных устройств шифрования. Недостаток такого подхода выражается в том, что требуется выполнение достаточно сложных процедур предвычислений, существенно замедляющих скорость шифрования в случае частой смены ключей.

Одним из интересных способов синтеза блочных шифров является построение аппаратно ориентированных шифров на основе управляемых операций. Под гибкой (управляемой) операцией преобразования понимается операция, управляемая некоторым двоичным вектором. При фиксированном значении управляющего вектора реализуются преобразования, относящиеся к одному из вариантов (модификаций) гибкой операции. Таким образом, управляемую операцию можно охарактеризовать как множество различных модификаций, каждая из которых соответствует конкретному значению управляющего вектора. В общем случае, различным значениям управляющего вектора может соответствовать одна и та же модификация. Однако при проектировании управляемых операций разумно ориентироваться на следующие конструктивные критерии:

- ❒ уникальность всех модификаций;
- ❒ большое число модификаций;
- ❒ существенные различия модификаций.

Управляемые операции преобразования, по сути, являются новым криптографическим примитивом, задающим для данного секретного ключа фиксированные процедуры зашифрования и расшифрования, в которых управляющий вектор формируется по секретному ключу и/или по преобразуемому блоку данных. Построенные на основе управляемых операций криптоалгоритмы являются гибкими в том смысле, что их описание на основе простых, традиционно используемых операций, приводит к необходимости учитывать зависимость выбора конкретных модификаций таких операций от переменных параметров криптосистемы (ключа, шифруемого текста).

Если управляющий вектор формируется в зависимости только от преобразуемого блока данных, то гибкую операцию будем называть *операцией, зависящей от преобразуемых данных* (ОЗПД). Если управляющий вектор формируется по ключу и по данным, то в подобной гибкой операции в зависимости от ключа задается тот или иной набор модификаций, из которого в зависимости от значения текущего управляющего подблока данных осуществляется выбор конкретной текущей модификации. Таким образом, в этом случае имеем некоторую ОЗПД, зависящую от ключа. Такие примитивы расширяют возможности разработчиков при проектировании гибких шифров.

ОЗПД обычно задают нелинейные преобразования, даже если все соответствующие ей модификации являются линейными. В общем плане эффективность ОЗПД связана с увеличением размера преобразуемого подблока данных, над которым они задают некоторую подстановку. Если модификации данной ОЗПД задают преобразование n-битовых двоичных векторов и число этих модификаций M, то сама ОЗПД определяет преобразование над N-битовыми векторами, где $N = n + \log_2 M$. Из последнего соотношения видно, что для повышения эффективности ОЗПД необходимо существенно увеличить число модификаций. Другим способом является разработка ОЗПД, включающих модификации специального типа. Использование ОЗПД на настоящий момент прошло достаточную практическую апробацию на примере блочных шифров RC5, RC6 и MARS, которые детально исследовались в последние годы. Было показано, что операции циклического сдвига, зависящие от преобразуемых данных и включающие всего лишь 32 модификации, являются эффективным средством противодействия самым мощным современным криптоатакам — дифференциальному и линейному криптоанализу.

Более эффективными способами шифрования на базе ОЗПД являются запатентованные в России технические решения, базирующиеся на управляемых перестановках (патенты РФ № 2127024, 2140710, 2140713, 2140715) и управляемых двухместных операциях (патент № 2140716). Число модификаций, соответствующих некоторой операции управляемой перестановки, может иметь значение до $n!$ ($\approx 2^{n(\log 2n-1)}$). Для управляемых двухместных операций могут быть разработаны быстродействующие операционные блоки, задающие значение M от 2^n до 2^{kn}, где $k \geq 2$ — натуральное число.

В данной книге рассматривается применение управляемых операций для построения скоростных шифров, сочетающих в себе высокую стойкость, высокую скорость преобразования данных и низкую сложность схемотехнической реализации. Показана возможность построения операционных блоков, реализующих уникальные модификации операций для каждого значения управляющего кода. Формирование управляющего кода в зависимости от преобразуемых данных и от секретного ключа дает возможность эффективной реализации нового технического решения (патент № 2124814), связанного с построением скоростных шифров, в которых алгоритм шифрования формируется в зависимости от секретного ключа путем настройки ОЗПД. Замечательной особенностью таких шифров яв-

ляется тот факт, что в них не используются предвычисления. Благодаря этому упрощается схемная реализация и легко обеспечивается скорость шифрования 1 Гбит/с и более при произвольной частоте смены секретных ключей. Отражены вопросы построения управляемых перестановок и управляемых подстановочных операций, в частности, управляемых сумматоров специального типа, а также представлены методы конструирования скоростных итеративных шифров на их основе.

Шифры на базе управляемых операций обладают следующими свойствами, обеспечивающими высокую стойкость к линейному и дифференциальному криптоанализу:

1. Нелинейные преобразования выполняются над подблоками большого размера (32, 64, 128, 256 бит).
2. ОЗПД зависят от секретного ключа.
3. Раундовые ключи преобразуются в зависимости от преобразуемых данных.

При расширении элементарных команд микропроцессоров инструкциями, реализующими операцию управляемой перестановки, легко могут быть разработаны программные шифры, обладающие скоростью более 1 Гбит/с при использовании массовых микропроцессоров типа Pentium. Такое расширение команд практически не изменит стоимость процессоров ввиду малой схемотехнической сложности операционных блоков, реализующих управляемую перестановку. При этом подобная новая команда может выполнить операцию циклического сдвига над двоичными векторами произвольной длины (например, над 32-битовыми словами, одновременно над двумя 16-битовыми словами и одновременно над четырьмя байтами).

Особый интерес представляет использование гибких шифров без предвычислений для построения стойких скоростных хэш-функций. Такие хэш-функции характеризуются зависимостью процедур преобразования (трактуемых в стандартных операциях) от хэшируемых данных, что позволяет назвать их гибкими хэш-функциями. Следует, однако, отметить, что термин "гибкая операция", также как и термин "ОЗПД", является условным. Он только подчеркивает способ описания некоторой более сложной операции над двоичными векторами большей длины с использованием более простых стандартных операций. Такой способ является достаточно признанным. Он дает более простое описание новых примитивов, которые при формальном описании теряли бы свою наглядность и простоту восприятия.

При написании данной книги авторы имели намерение дать общую картину современной криптографии в таком изложении, которое было бы легко доступно широкому кругу читателей, а также рассмотреть специальные вопросы, связанные с разработкой скоростных блочных шифров, ориентированных на программную и/или аппаратную реализацию. К вопросам общего характера относится материал, посвященный значению криптографии в информационном обществе,

двухключевой криптографии, криптографическим протоколам, электронной цифровой подписи и ряду хорошо известных одноключевых шифров. Подробное рассмотрение проблемы и подходов к построению скоростных блочных шифров также представляет достаточно широкий интерес ввиду их большого значения в современных технологиях защиты информации и широкого применения. Если не вдаваться в детальные математические выкладки и доказательства, то и эта часть материала является доступной широким слоям читателей, поскольку излагаемые варианты построения скоростных шифров проиллюстрированы наглядными рисунками и схемами. Приведенная в книге библиография отражает уровень современных достижений теоретической и прикладной криптографии в области блочных шифров. Читатели, заинтересованные в глубоком освоении концепции управляемых преобразований как подхода к построению скоростных блочных шифров, найдут ее математическое обоснование.

ГЛАВА 1

Криптография в информационном обществе

1.1. Проблемы защиты информации в компьютерных системах

Криптография исторически зародилась из потребности передачи секретной информации. Длительное время она была связана только с разработкой специальных методов преобразования информации с целью ее представления в форме, недоступной для потенциального злоумышленника. С началом применения электронных способов передачи и обработки информации задачи криптографии начали расширяться. В настоящее время, когда компьютерные информационные технологии нашли массовое применение, проблематика криптографии включает многочисленные задачи, которые не связаны непосредственно с засекречиванием информации. Современные проблемы криптографии включают разработку систем электронной цифровой подписи и тайного электронного голосования, протоколов электронной жеребьевки и аутентификации удаленных пользователей, методов защиты от навязывания ложных сообщений и т. п.

Многие задачи практической информатики эффективно решаются с использованием криптографических методов. В криптографии рассматривается некоторый *злоумышленник* (оппонент, криптоаналитик противника, нарушитель, нелегальный пользователь), который осведомлен об используемых криптографических алгоритмах, протоколах, методах и пытается вскрыть их. Вскрытие криптосистемы может заключаться, например, в несанкционированном чтении информации, формировании чужой подписи, изменении результатов голосования, нарушении тайны голосования, модифицировании данных, которое не будет обнаружено законным получателем. Разнообразные действия оппонента в общем случае называются *криптографической атакой* (нападением). Специфика криптографии состоит в том, что она направлена на разработку методов, обеспечивающих стойкость к любым действиям злоумышленника, хотя на момент разработки криптосистемы нереально предусмотреть все возможные способы атаки, которые могут

быть изобретены в будущем на основе новых достижений теории и технологического прогресса. Центральным является вопрос, насколько надежно решается та или иная криптографическая проблема. Ответ на этот вопрос непосредственно связан с оценкой трудоемкости каждой конкретной атаки на криптосистему. Решение такой задачи, как правило, чрезвычайно сложно и составляет самостоятельный предмет исследований, называемый *криптоанализом*. *Криптография и криптоанализ* образуют единую область науки — *криптологию*, которая в настоящее время является новым разделом математики, имеющим важные приложения в современных информационных технологиях.

Широкое применение компьютерных технологий в системах обработки данных и управления привело к обострению проблемы защиты информации от несанкционированного доступа. Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жестко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Известно большое число угроз информации, которые могут быть реализованы как со стороны внешних, так и внутренних нарушителей [9].

Радикальное решение проблем защиты информации, циркулирующей в высокопроизводительных автоматизированных системах, может быть получено на базе использования криптографических методов. При этом важным является применение скоростных алгоритмов шифрования, которые не приводят к снижению производительности компьютерных и телекоммуникационных систем. Криптографические преобразования данных являются гибким и эффективным средством обеспечения их конфиденциальности, целостности и подлинности. Использование методов криптографии в совокупности с необходимыми техническими и организационными мероприятиями может обеспечить защиту от широкого спектра потенциальных угроз.

Потребности современной практической информатики привели к возникновению нетрадиционных задач защиты электронных данных, одной из которых является аутентификация электронной информации в условиях, когда обменивающиеся этой информацией стороны не доверяют друг другу. Эта проблема связана с созданием систем электронной цифровой подписи. Теоретической базой для решения этой проблемы стало открытие в середине 1970-х годов американскими исследователями У. Диффи и М. Е. Хеллманом *двухключевой криптографии* [62], которое явилось блестящим достижением многовекового эволюционного развития криптографии. Революционные идеи двухключевой криптографии привели к резкому росту числа открытых исследований в этой области, показали новые пути совершенствования криптографии, ее далеко не исчерпанные возможности и уникальное значение в современных условиях бурного развития электронных информационных технологий.

Технической основой перехода в информационное общество являются современные микроэлектронные технологии, которые обеспечивают непрерывный рост

качества средств вычислительной техники и служат базой для сохранения основных тенденций ее развития:

- ❒ миниатюризации и снижения энергопотребления оборудования;
- ❒ увеличения объема оперативной памяти (ОП) и емкости встроенных и съемных накопителей информации;
- ❒ роста производительности и надежности систем;
- ❒ расширения сфер и масштабов применения ЭВМ.

Данные тенденции развития средств вычислительной техники привели к тому, что на современном этапе защита компьютерных систем от несанкционированного доступа характеризуется применением *программных криптографических методов защиты*.

Как показывает практика последних лет, расширяются масштабы использования и *аппаратных шифров*. Одной из актуальных проблем практической криптографии является построение алгоритмов, обеспечивающих скорость шифрования более 1500 Мбит/с при их реализации в виде недорогих микроэлектронных схем — *крипточипов*. В первую очередь это связано с широким применением шифрования в коммерческом телевидении. Другой массовой областью использования крипточипов является мобильная телефония. В последнее время специалистами по защите информации и пользователями осознана необходимость криптографической защиты и при передаче охранной информации с видеокамер внешнего наблюдения, а также других устройств сигнализации. Эта область применения криптографии требует разработки устройств шифрования низкой схемотехнической сложности.

Одной из важных социально-этических проблем, порожденных все более расширяющимся применением методов криптографической защиты информации, является противоречие между желанием пользователей защитить свою информацию и передачу сообщений и желанием специальных государственных служб иметь возможность доступа к информации организаций и отдельных лиц с целью пресечения незаконной деятельности. В развитых странах наблюдается широкий спектр мнений о подходах к вопросу о регламентации использования алгоритмов шифрования. Высказываются предложения от полного запрета широкого применения криптографических методов до полной свободы их использования. Некоторые предложения относятся к разрешению использования только ослабленных алгоритмов или к установлению порядка обязательной регистрации ключей шифрования.

Чрезвычайно трудно найти оптимальное решение этой проблемы. Как оценить соотношение потерь законопослушных граждан и организаций от незаконного использования их информации, с одной стороны, и убытков государства от невозможности получения доступа к зашифрованной информации отдельных групп, скрывающих свою незаконную деятельность, с другой стороны? Как исключить незаконное использование криптоалгоритмов лицами, которые нару-

шают и другие законы? Кроме того, всегда существуют способы скрытого хранения и передачи информации. Эти вопросы еще предстоит решать социологам, психологам, правоведам и политикам.

Что касается исследовательских работ в области криптографии, которые могут привести к удобным и практически абсолютно стойким алгоритмам, то их ограничение вряд ли представляется разумным. Видимо, надо предоставить законопослушным гражданам и организациям одинаковые возможности для защиты своей информации по сравнению с возможностями злоумышленников, которые так или иначе получают доступ к достижениям криптографии и поэтому могут оказаться в существенно более выгодных условиях.

В дополнение к этому, ограничение исследовательских работ в области криптографии быстрее всего приведет к отставанию в ее развитии, но никак не к предотвращению доступа криминальных структур к современным криптографическим методам, полученным, например, из других стран. В результате наиболее серьезно будут ущемляться интересы именно законопослушных организаций. Во многих странах мира начали понимать сущность данной проблемы, что привело в настоящее время к возрастанию числа развитых стран, в которых снимаются жесткие ограничения на применение шифрования.

Независимо от прогресса в области разработки криптографических методов защиты информации государство всегда имеет возможность законодательно потребовать, чтобы все пользователи шифров регистрировали свои ключи (или необходимую долю ключевых данных) в специально созданных учреждениях. В этом случае контроль информации обеспечивается независимо от уровня стойкости используемых алгоритмов. Эти и другие аспекты показывают, что торможение исследовательских работ в области криптографии не является объективно обоснованным. Еще в начале 1970-х годов в развитых западных странах потребности практики вызвали интерес к криптографии со стороны широких кругов исследователей и дали толчок к началу открытых исследований в этой области, которая прежде считалась элитарной и входила в сферу интересов сугубо секретных служб.

Известен ряд примеров, когда секретность в области криптографии приводила к существенным провалам при изготовлении засекречивающей аппаратуры и даже к отставанию от научно-технического прогресса. Широкая деятельность в столь животрепещущей сфере науки создали условия для повышения и самого качества исследований в криптологии, что позволило У. Диффи и М. Е. Хеллману открыть двухключевую криптографию, идеи которой привели к возникновению новых нетрадиционных разделов криптографии и превратили ее в одно из бурно развивающихся направлений современной математики. Открытие двухключевой криптографии является ярким примером взаимодействия теории и практики, а также примером влияния политики на достижения теории.

Сдерживание открытых исследований в области криптографии упрощает некоторые проблемы спецслужб, однако для государства, в целом, отрицательный эф-

фект от такого сдерживания крайне велик и связан с отставанием в области разработки современных систем защиты информации, распространенностью компьютерных преступлений и другими проблемами. Примером может служить глобальная компьютерная сеть Internet, являющаяся грандиозным достижением компьютерных технологий, внедрение которой, однако, связано с массой правовых нарушений и преступлений.

В результате опыта работы в Internet были выявлены слабости и недостатки традиционных административных и системных механизмов защиты информации. Криптография предоставляет принципиально новые возможности обеспечения безопасности информации в компьютерных сетях, и сейчас ее методы активно внедряются в глобальные сетевые технологии. Не отказ от прогресса в информатизации, а использование современных достижений криптографии — вот стратегически правильное решение, подтвержденное практикой. Возможность широкого применения криптографии в компьютерных сетях является большим достижением и признаком демократического общества.

Владение основами криптографии в информационном обществе объективно не может быть привилегией отдельных государственных служб, а является насущной необходимостью для самых широких слоев научно-технических работников, применяющих компьютерную обработку данных или разрабатывающих информационные системы, сотрудников служб безопасности и руководящего состава различных организаций и предприятий. Только такой подход может служить базой для повышения эффективности внедрения и эксплуатации высококачественных систем защиты электронной информации.

Одна отдельно взятая организация не может обеспечить достаточно полный контроль над информационными потоками в пределах всего государства и надлежащую защиту пространственно распределенного национального информационного ресурса. Однако определенные государственные организации могут создать условия для формирования рынка качественных средств защиты, подготовки достаточного количества специалистов и овладения массовыми пользователями основами защиты информации и криптографии.

В России и других странах СНГ в начале 1990-х годов отчетливо прослеживалась тенденция опережения расширения масштабов и областей применения информационных технологий над развитием систем защиты данных. Такая ситуация в определенной степени являлась и является типичной и для ряда развитых в промышленном отношении стран. Это закономерно — сначала должны возникнуть практические проблемы, а затем будут найдены их решения. Начало политических изменений в ситуации сильного отставания стран СНГ в области информатизации в конце 1980-х годов создало благодатную почву для резкого преодоления указанной тенденции.

Пример развитых стран, возможность приобретения системного программного обеспечения и компьютерной техники вдохновили российских пользователей на проведение активной работы по внедрению новых информационных технологий.

Включение массового потребителя, заинтересованного в оперативной обработке данных и других достоинствах современных информационно-вычислительных систем, в решение проблемы компьютеризации привело к очень высоким темпам развития этой области в России и других странах СНГ. Однако естественное совместное совершенствование средств автоматизации обработки информации и средств защиты информации в значительной степени нарушилось, что стало причиной массовых компьютерных преступлений. Ни для кого не секрет, что такие преступления в настоящее время составляют одну из актуальных проблем.

Использование средств защиты информации зарубежного производства не могло исправить данный перекос, поскольку поступавшие на рынок России продукты этого типа не соответствовали современным требованиям из-за существовавших экспортных ограничений, принятых в США — основном производителе средств защиты информации. Другим аспектом, имеющим первостепенное значение, является то, что подобная продукция должна пройти установленную процедуру сертифицирования в уполномоченных на проведение таких работ организациях. Проверка алгоритмов шифрования, программного обеспечения и электронных устройств на предмет различного рода "закладок" представляет собой чрезвычайно трудоемкую задачу. Последние исследования криптографов показали возможность разработки алгоритмов шифрования с "потайными дверями", которые практически невозможно обнаружить за разумное время даже высокопрофессиональным специалистам.

Сертификаты иностранных фирм и организаций никак не могут быть заменой отечественным. Сам факт использования зарубежного системного и прикладного программного обеспечения в критических областях создает потенциальную угрозу информационным ресурсам. Применение иностранных средств защиты без должного анализа соответствия выполняемым функциям и уровню обеспечиваемой защиты может многократно осложнить ситуацию.

Форсирование процесса информатизации требует адекватного обеспечения потребителей средствами защиты. Отсутствие на внутреннем рынке достаточного количества средств защиты информации, циркулирующей в компьютерных системах, значительное время не позволяло в необходимых масштабах осуществлять мероприятия по качественной защите данных. Ситуация усугублялась отсутствием достаточного количества специалистов в области защиты информации, поскольку они, как правило, готовились только для специальных организаций. Реструктурирование последних, связанное с изменениями, протекающими в России, привело к образованию независимых организаций, специализирующихся в области защиты информации, и увеличению потребности в специалистах по защите информации. Как следствие, возникла конкуренция между организациями, приведшая к появлению весьма большого количества сертифицированных отечественных средств защиты электронной информации.

Одной из важных особенностей массового использования информационных технологий является то обстоятельство, что для эффективного решения проблемы

защиты национального информационного ресурса необходимо рассредоточение мероприятий по защите данных среди массовых пользователей. Информация должна быть защищена в первую очередь там, где она создается, собирается, перерабатывается и теми организациями, которые несут непосредственный урон от несанкционированного доступа к своим данным. Указанный принцип рационален и эффективен: защита интересов отдельных организаций — это базовая составляющая защиты интересов государства в целом.

1.2. Проблематика криптографии

1.2.1. Традиционные вопросы криптографии

Слово "криптография" в переводе с греческого языка означает "тайнопись", что вполне отражает ее первоначальное предназначение. Примитивные с позиций сегодняшнего дня криптографические методы известны с древнейших времен и длительное время рассматривались скорее как некоторые ухищрения, чем строгая научная дисциплина. Классической задачей криптографии является обеспечение обратимости преобразования некоторого *исходного текста (открытого текста)* в кажущуюся случайной последовательность знаков, называемую *шифртекстом (закрытым текстом)*, или *криптограммой*. При этом шифртекст может содержать как новые знаки, так и уже имеющиеся в исходном сообщении. Количество знаков в криптограмме и в исходном тексте в общем случае может различаться. Непременным требованием является возможность однозначного и в полном объеме восстановления исходного текста, используя лишь некоторые логические действия с символами шифртекста. В далекие времена надежность сохранения информации в тайне определялась секретностью самого метода преобразования.

Однако секретность алгоритма принципиально не может обеспечить его *безусловную стойкость*, т. е. невозможность чтения криптограммы противником, обладающим бесконечными вычислительными ресурсами. Поскольку секретные алгоритмы не доступны для проведения широкомасштабных криптоаналитических исследований, то по сравнению с открытыми алгоритмами имеется значительно более высокая вероятность того, что впоследствии будут найдены уязвимые места и эффективные способы их взлома. В связи с этими обстоятельствами в настоящее время наиболее широко используются открытые алгоритмы, прошедшие длительное тестирование и обсуждение в открытой криптографической литературе.

Стойкость современных криптосистем основывается не на секретности алгоритма, а на секретности некоторой информации сравнительно малого размера, называемой *секретным ключом*. Ключ используется для управления процессом криптографического преобразования (шифрования) и является легко сменяемым элементом криптосистемы. Ключ может быть заменен пользователями в произ-

вольный момент времени, тогда как сам алгоритм шифрования является долговременным элементом криптосистемы и связан с длительным этапом разработки и тестирования.

При прочих равных условиях отсутствие полных данных об алгоритме шифрования существенно (при адекватной его реализации) затрудняет проведение криптоаналитической атаки. Поэтому были предложены современные шифры, в которых непосредственно действующий алгоритм шифрования является легко сменяемым элементом и выбирается случайно. При этом общая структура криптосистемы открыта для детального обсуждения, что позволяет оценить ее стойкость в целом. Такие шифры реализуются как гибкие криптосистемы, в которых алгоритм, действующий в сеансе шифрования, формируется по специальному *алгоритму инициализации (предвычислений)*. Этот алгоритм является открытым, а сам действующий алгоритм шифрования — неизвестным и зависимым от секретного ключа пользователя.

Прошли многие века, в течение которых криптография была предметом избранных — жрецов, правителей, крупных военачальников и дипломатов. Несмотря на малую распространенность, использование криптографических методов вскрытия шифров противника оказывало существенное воздействие на исход важных исторических событий. Известен не один пример, когда переоценка используемых средств шифрования приводила к военным и дипломатическим поражениям. Несмотря на применение криптографических методов в важных областях, эпизодическое использование криптографии не могло даже близко подвести ее к той роли, которую она имеет в современном обществе. Своим превращением в научную дисциплину криптография обязана потребностям практики и развитию электронных информационных технологий.

Пробуждение значительного интереса к криптографии и ее последующее развитие началось в XIX веке, что связано с зарождением электросвязи. В XX столетии секретные службы большинства развитых стран стали относиться к этой дисциплине как к обязательному инструменту своей деятельности.

Говоря об исторических аспектах научных исследований в области криптографии, необходимо отметить тот факт, что весь период с древних времен до 1949 года можно назвать донаучным периодом, поскольку средства закрытия письменной информации не имели строгого математического обоснования. Поворотным моментом, придавшим криптографии научность и выделившим ее в отдельное направление математики, явилась публикация в 1949 году статьи К. Э. Шеннона "Теория связи в секретных системах" [126]. Указанная работа послужила основой развития *одноключевых симметричных криптосистем*, в которых предполагается обмен секретными ключами между корреспондентами. Впоследствии с учетом особенностей построения симметричные шифры были разделены на две криптосистемы: *поточные* и *блочные шифры*. Отличительная особенность первых состоит в преобразовании каждого символа в потоке исходных данных, тогда как вторые осуществляют последовательное преобразование целых блоков данных.

Фундаментальным выводом из работы Шеннона стало определение зависимости надежности алгоритма от размера и качества секретного ключа, а также от *информационной избыточности* исходного текста. Шеннон ввел формальное определение информации и функции ненадежности ключа как его неопределенности при заданном количестве известных битов закрытого текста. Кроме того, им было введено важное понятие *расстояния единственности* как минимального размера текста, для которого еще возможно однозначное раскрытие исходного текста. Было показано, что расстояние единственности прямо пропорционально длине ключа и обратно пропорционально избыточности исходного текста. Следствием работы К. Э. Шеннона стало доказательство наличия теоретически стойких шифров, как, например, шифр Вернама.

Другим фундаментальным толчком развития криптографии явилась публикация в 1976 году статьи У. Диффи и М. Е. Хеллмана "Новые направления в криптографии" [62]. В этой работе впервые было показано, что секретность передачи информации может обеспечиваться без обмена секретными ключами. Тем самым была открыта эпоха *двухключевых (асимметричных) криптосистем*, разновидностями которых являются системы электронной цифровой подписи, тайного электронного голосования, защиты от навязывания ложных сообщений, электронной жеребьевки, идентификации и аутентификации удаленных пользователей и ряд других систем.

Последние годы на базе совершенствования электронных технологий появились новые теоретические разработки в области *квантовой криптографии* [41], основанной на принципах неопределенности Гейзенберга.

Наряду с развитием криптографических систем совершенствовались и методы, позволяющие восстанавливать исходное сообщение, исходя из шифртекста и другой известной информации, получившие название *криптоанализа*. Успехи криптоанализа приводили к ужесточению требований к криптографическим алгоритмам. Принципиально важным вопросом криптографии всегда была надежность криптосистем. Эта проблема допускала различное трактование на протяжении всей истории криптографии.

Голландский криптограф Керкхофф (1835—1903) впервые сформулировал *правило стойкости шифра*, в соответствии с которым:

- ❒ весь механизм преобразований считается известным злоумышленнику;
- ❒ надежность алгоритма должна определяться только неизвестным значением секретного ключа.

Второе требование означает, что оппонент не сможет разработать методы, позволяющие снять защиту или определить истинный ключ, за время существенно меньшее, чем время *полного (тотального) перебора* всего множества возможных секретных ключей.

По всей видимости, одной из задач оценки стойкости шифра по Керкхоффу было осознание необходимости испытания криптосхем в условиях, более благоприят-

ных для атаки, по сравнению с условиями, в которых, как правило, может действовать потенциальный нарушитель. Правило Керкхоффа стимулировало появление более качественных шифрующих алгоритмов. Можно сказать, что в нем содержится первый элемент стандартизации в области криптографии, поскольку предполагается разработка открытых способов преобразований. В настоящее время это правило интерпретируется более широко: *все долговременные элементы системы защиты должны предполагаться известными потенциальному злоумышленнику*. В последнюю формулировку криптосистемы входят как частный случай систем защиты. В расширенном понимании правила Керкхоффа предполагается, что все элементы криптосистем защиты подразделяются на две категории — долговременные и легко сменяемые элементы. К *долговременным* относятся те элементы, которые связаны со структурой криптосистем защиты и заменяются только специалистами. К *легко сменяемым* относятся элементы криптосистемы, которые предназначены для частого модифицирования в соответствии с заданным порядком. Легко сменяемыми элементами шифра являются, например, секретный ключ, пароль, идентификатор и т. п. Правило Керкхоффа отражает тот факт, что надлежащий уровень секретности зашифрованной информации должен быть обеспечен только за счет неизвестных легко сменяемых элементов шифра. Действительно, долговременные элементы системы защиты трудно сохранить в тайне, поэтому система должна быть стойкой в случае, когда они являются известными атакующему.

Согласно современным требованиям, криптосистемы с секретным ключом, включая шифры с ключом ограниченного размера (128—256 бит), должны быть стойкими к криптоанализу на основе известного алгоритма, большого объема известного открытого текста и соответствующего ему шифртекста. Несмотря на эти общие требования, шифры, используемые специальными службами, сохраняются, как правило, в секрете. Это обусловлено необходимостью иметь дополнительный запас прочности защиты секретной информации, поскольку в настоящее время создание криптосистем с доказуемой стойкостью является предметом развивающейся теории и представляет собой достаточно сложную проблему. Чтобы избежать возможных слабостей, алгоритм шифрования может быть построен на основе хорошо изученных и проверенных на практике принципов и способов преобразования. Ни один серьезный современный пользователь не будет полагаться только на надежность сохранения в секрете своего алгоритма, поскольку крайне сложно гарантировать отсутствие вероятности того, что информация об алгоритме станет известной злоумышленнику.

Обоснование надежности используемых систем осуществляется как теоретически, так и экспериментально при моделировании криптоаналитических атак с привлечением группы опытных специалистов, которым предоставляются значительно более благоприятные условия по сравнению с условиями, возникающими на практике в предполагаемых областях применения криптоалгоритма. Например, кроме шифртекста и алгоритма преобразований криптоаналитикам предоставляется весь или часть исходного текста, несколько независимых шифртекстов,

полученных с помощью одного и того же ключа, или шифртексты, полученные из данного открытого текста с помощью различных ключей. Оценивается стойкость испытываемой криптосистемы ко всем известным методам криптоанализа, и, по возможности, разрабатываются новые подходы к ее вскрытию. Если в этих условиях криптосистема оказывается стойкой, то она рекомендуется для конкретного применения.

В современном криптоанализе рассматриваются атаки на засекречивающие системы на основе следующих известных данных:

- ❒ шифртекста;
- ❒ открытого текста и соответствующего ему шифртекста;
- ❒ выбранного открытого текста;
- ❒ выбранного шифртекста;
- ❒ адаптированного открытого текста;
- ❒ адаптированного шифртекста.

Кроме того, рассматриваются следующие методы инженерного (технического) криптоанализа с использованием перечисленных выше известных данных:

- ❒ преднамеренно генерируемых аппаратных ошибок;
- ❒ замеров потребляемой мощности;
- ❒ замеров времени вычислений.

Мы детально перечислили типы атак на криптосистемы, предназначенные для шифрования данных с целью защиты от несанкционированного чтения. По отношению к иным видам криптосистем существует ряд других атак, которые будут рассмотрены ниже. А сейчас рассмотрим перечисленные типы атак подробнее.

- ❒ В случае *криптоанализа на основе известного шифртекста* считается, что противник знает механизм шифрования и ему доступен только шифртекст. Это соответствует модели внешнего нарушителя, который имеет физический доступ к линии связи, но не имеет доступ к аппаратуре зашифрования и расшифрования.
- ❒ При *криптоанализе на основе известного открытого текста* предполагается, что криптоаналитику известен шифртекст и некоторая часть исходного текста, а, в частных случаях, и соответствие между шифртекстом и исходным текстом. Возможность проведения такой атаки складывается при зашифровании документов, подготовленных с использованием стандартных форм, в условиях, когда определенные блоки данных известны и повторяются. В ряде современных средств защиты компьютерной информации используется режим глобального шифрования, в котором вся информации на встроенном магнитном носителе записывается в виде шифртекста, включая главную корневую запись, загрузочный сектор, системные программы и пр. При хищении

такого носителя (или компьютера) легко установить, какая часть криптограммы соответствует стандартной системной информации, и получить большой объем известного исходного текста для выполнения криптоанализа.

- В нападениях *на основе выбранного открытого текста* предполагается, что криптоаналитик противника может ввести специально подобранный им текст в шифрующее устройство и получить криптограмму, образованную под управлением секретного ключа. Это соответствует модели внутреннего нарушителя. На практике такая ситуация может возникнуть, когда в атаку на шифр вовлекаются лица, которые не знают секретного ключа, но в соответствии со своими служебными полномочиями имеют возможность использовать шифратор для закрытия передаваемых сообщений. Для осуществления такой атаки могут быть использованы также технические работники, готовящие формы документов, электронные бланки и др.
- *Криптоанализ на основе выбранного шифртекста* предполагает, что противник (оппонент) имеет возможность использовать для расшифрования сформированные им самим шифртексты, которые выбираются специальным образом, чтобы по полученным на выходе дешифратора текстам он мог вычислить секретный ключ шифрования с минимальной трудоемкостью.
- *Атака на основе адаптированных текстов* соответствует случаю, когда атакующий многократно подставляет тексты для зашифрования (или расшифрования), причем каждую новую порцию данных выбирает в зависимости от полученного ранее результата преобразования. Этот вид атаки является наиболее благоприятным для нападающего.

В настоящее время к наиболее мощным типам криптоаналитических атак на основе выбранных или адаптированных текстов относятся *дифференциальный (разностный) криптоанализ* (ДКА) [44] и *линейный криптоанализ* (ЛКА) [86], а также производные от них методы.

При тестировании новых криптосистем особый интерес представляют нападения на основе известного *секретного* ключа или *расширенного (рабочего)* ключа шифрования. Будем делать различие между секретным ключом и расширенным ключом, поскольку секретный ключ не всегда непосредственно используется в преобразованиях шифруемого текста, а часто служит только для выработки расширенного ключа, который и используется в процессе шифрования. Существуют шифры (например, блочный шифр ГОСТ 28147-89), в которых секретный ключ непосредственно используется при шифровании данных, т. е. секретный ключ служит и рабочим ключом шифрования. Очевидно, что расширенный ключ является секретным элементом шифра. При проведении криптоанализа на основе известных элементов ключа (секретного или расширенного) предполагается, что криптоаналитик имеет информацию о некоторой части рабочего ключа. Чем больше известная доля ключа, при которой шифр оказывается стойким, тем меньше опасений будет вызывать шифр в реальных условиях атаки, когда ключ атакующему неизвестен, но осуществляется попытка восстановить его элементы.

При сравнении двух шифров предпочтение можно дать тому шифру, который имеет лучшие показатели по указанному критерию.

Одним из направлений построения скоростных программных шифров является использование зависимости алгоритма шифрования от секретного ключа. В таких криптосистемах конкретная модификация алгоритма шифрования сменяется одновременно с заменой секретного ключа и атакующему неизвестна. Подобные шифры получили названия *недетерминированных*, или *гибких* шифров. При тестировании гибких шифров представляется разумным проводить анализ их стойкости с использованием атаки на основе *выбранной модификации алгоритма* шифрования. В этом варианте криптоаналитику предоставляется возможность анализировать самую слабую, по его мнению, модификацию из числа потенциально реализуемых модификаций криптоалгоритма. Затем для выбранной модификации проводится криптоанализ на основе специально подобранных текстов, в том числе может рассматриваться и вариант *атаки с частично известным ключом* шифрования. Если не удается найти слабую модификацию криптоалгоритма, то анализируемый гибкий шифр можно признать криптографически стойким.

1.2.2. Современные приложения

Значение криптографии выходит далеко за рамки обеспечения секретности данных. По мере все большей автоматизации процессов передачи и обработки информации и интенсификации информационных потоков криптографические методы приобретают уникальное значение. Новые информационные технологии в своей основе имеют двухключевую криптографию, которая позволяет реализовать протоколы, предполагающие, что секретный ключ известен только одному пользователю, т. е. протоколы, ориентированные на взаимное недоверие взаимодействующих сторон. Отметим основные приложения современной криптографии.

- Защита от несанкционированного чтения (или обеспечение конфиденциальности информации).
- Защита от навязывания ложных сообщений (умышленных и непреднамеренных).
- Аутентификация законных пользователей.
- Контроль целостности информации.
- Аутентификация информации.
- Электронная цифровая подпись.
- Системы тайного электронного голосования.
- Электронные деньги.
- Электронная жеребьевка.
- Защита от отказа факта приема сообщения.