# ВВЕДЕНИЕ В КРИПТОГРАФИЮ

Под общей редакцией В.В. Ященко

# Введение в криптографию

Под редакцией В. В. Ященко

Издание четвертое, дополненное

Москва
Издательство МЦНМО
2012

УДК 003.26
ББК 32.973-18.2
В24

Авторский коллектив: В. В. Ященко (редактор, глава 1, приложение В), Н. П. Варновский (главы 2, 3, приложение В), Ю. В. Нестеренко (глава 4), Г. А. Кабатянский (глава 5), П. Н. Девянин, В. Г. Проскурин, А. В. Черемушкин (глава 6), П. А. Гырдымов, А. Ю. Зубов, А. В. Зязин, В. Н. Овчинников (глава 7), М. И. Анохин (приложение Б).

В24 **Введение** в криптографию / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012. — 348 с.

ISBN 978-5-4439-0026-1

В книге впервые на русском языке дается систематическое изложение научных основ криптографии от простейших примеров и основных понятий до современных криптографических конструкций. Понимание принципов криптографии стало для многих потребностью в связи с широким распространением криптографических средств обеспечения информационной безопасности, поэтому книга может быть полезна массовому читателю.

В книгу включены задачи олимпиад по криптографии для школьников.

Книга рассчитана на школьников, студентов-математиков и специалистов по информационной безопасности.

ББК 32.973-18.2

**ISBN 978-5-4439-0026-1**

# Оглавление

## Предисловие к четвертому изданию

Настоящее издание можно считать в некотором смысле юбилейным: минуло более десяти лет со дня выхода книги в свет. За это время она стала настоящим бестселлером. Вышли 3 издания в МЦНМО, книга была напечатана также в издательстве «Питер». Перевод на английский язык издан Американским математическим обществом.

Основная причина популярности книги, безусловно, состоит в том, что она остается единственной в своем жанре. Вместе с тем интерес к проблемам криптографии и, в более широком смысле, к информационной безопасности с каждым годом возрастает.

С момента выхода предыдущих изданий ситуация с математической криптографией в стране немного изменилась. Курс лекций «Теоретическая криптография» теперь читается на факультете управления и прикладной математики МФТИ. Учебные курсы, посвященные этой математической дисциплине, появились на матмехе СПбГУ: Э. А. Гирш «Сложностная криптография» и Ю. Лифшиц «Современные задачи криптографии».

В МГУ проводится ежегодная международная конференция «Математика и безопасность информационных технологий».

В настоящее издание внесены некоторые добавления и исправления. В главе по теории чисел описан недавно открытый полиномиальный алгоритм проверки целых чисел на простоту. Добавлены список литературы для дальнейшего чтения с краткими аннотациями и «Словарь криптографических терминов».

*Март* 2012 *г.* *В. Ященко*

## Предисловие к третьему изданию

В последние годы в жизни общества постоянно возрастает значение информационной составляющей (информационные ресурсы, информационные технологии и т. д.) и, как следствие, информационной безопасности. Специалисты в области информационной безопасности необходимы и в государственных структурах, и в научных учреждениях, и в коммерческих фирмах.

Для развития системы подготовки таких специалистов в 1999–2000 гг. приняты дополнительные меры: в перечень специальностей высшего образования включено 6 специальностей блока 070000 (информационная

безопасность), в перечень диссертационных специальностей — междисциплинарная специальность 051319. В Московском государственном университете им. М. В. Ломоносова с сентября 2000 г. начато обучение по специализациям «Математические методы защиты информации» и «Программное обеспечение защиты информации». Научный фундамент этих специализаций — криптография — наука о шифрах.

Систематических учебников по криптографии на русском языке пока нет, они будут появляться по мере становления системы гражданского криптографического образования. В этих условиях предлагаемая книга «Введение в криптографию», которая уже выдержала два издания, может быть рекомендована в качестве первого учебного пособия для студентов-математиков, специализирующихся в области информационной безопасности. Книга написана специалистами-криптографами с целью популяризации научных основ криптографии и поэтому доступна и может быть полезна массовому читателю.

Ректор МГУ,
академик РАН *В. А. Садовничий*

*Сентябрь* 2000 *г.*

## Предисловие ко второму изданию

В настоящем втором издании исправлены опечатки и неточности, замеченные в первом издании.

*Сентябрь* 1999 *г.* *В. Ященко*

## Предисловие к первому изданию

Криптография — наука о шифрах — долгое время была засекречена, так как применялась в основном для защиты государственных и военных секретов. В настоящее время методы и средства криптографии используются для обеспечения информационной безопасности не только государства, но и частных лиц, и организаций. Дело здесь совсем не обязательно в секретах. Слишком много различных сведений «гуляет» по всему свету в цифровом виде. И над этими сведениями «висят» угрозы недружественного ознакомления, накопления, подмены, фальсификации и т. п. Наиболее надежные методы защиты от таких угроз дает именно криптография.

Пока криптографические алгоритмы для рядового потребителя — тайна за семью печатями, хотя многим уже приходилось пользоваться некоторыми криптографическими средствами: шифрование электронной почты, интеллектуальные банковские карточки и др. Естественно, что при этом основной вопрос для пользователя — обеспечивает ли данное криптографическое средство надежную защиту. Но даже правильно сформулировать этот элементарный вопрос непросто. От какого противника защищаемся? Какие возможности у этого противника? Какие цели он может преследовать? Как измерять надежность защиты? Список таких вопросов можно продолжить. Для ответа на них пользователю необходимы знания основных понятий криптографии.

Популярное изложение научных основ криптографии (речь идет только о «негосударственной» криптографии; разделы криптографии, связанные с государственной безопасностью, должны оставаться секретными) — цель настоящей книги. Ее можно использовать и в качестве учебного пособия. На русском языке аналогичных книг пока нет. Материалы ряда глав публиковались авторами ранее в других изданиях (глава 1 — в книге С. А. Дориченко, В. В. Ященко, «25 этюдов о шифрах», М.: ТЭИС, 1994; главы 1, 2, 4, 5 — в журнале «Математическое просвещение», третья серия, выпуск 2, М.: МЦНМО, 1998; глава 7 — в газете «Информатика» (еженедельное

приложение к газете «Первое сентября»), № 4, январь 1998). При подготовке настоящего издания эти материалы были переработаны и дополнены.

Изложение материала рассчитано на читателя с математическим складом ума. В основном главы не зависят друг от друга (это достигнуто за счет некоторых повторов) и их можно читать в произвольном порядке. Главу 1 — вводную — рекомендуется прочитать всем, поскольку в ней на популярном уровне разъясняются все основные понятия современной криптографии: шифр, ключ, стойкость, электронная цифровая подпись, криптографический протокол и др. В других главах часть материала повторяется, но уже более углубленно. В главах 2, 3, 4, 5 используются некоторые сведения из высшей математики, известные ученикам математических классов и студентам. Глава 6 ориентирована на знатоков компьютерных технологий. Глава 7 содержит материалы олимпиад по криптографии для школьников, и поэтому для ее чтения никаких знаний, выходящих за пределы школьной программы, не требуется.

Предупреждение: криптографические средства и программные продукты, упоминаемые в книге, используются только для иллюстрации общих криптографических идей; авторы не ставили своей целью давать оценки или сравнивать имеющиеся на рынке криптографические средства.

Криптография была поставлена на научную основу во многом благодаря работам выдающегося американского ученого Клода Шеннона. Его доклад «Математическая теория криптографии» был подготовлен в секретном варианте в 1945 г., рассекречен и опубликован в 1948 г., переведен на русский язык в 1963 г. Поскольку «Работы по теории информации и кибернетике» (1963 г.) К. Шеннона стали библиографической редкостью, мы включили в приложение основную часть статьи К. Шеннона «Теория связи в секретных системах». Эту основополагающую работу рекомендуется прочитать всем интересующимся криптографией.

Для профессионального понимания криптографических алгоритмов и умения оценивать их сильные и слабые стороны необходима уже серьезная математическая подготовка (на уровне математических факультетов университетов). Это объясняется тем, что современная криптография основана на глубоких результатах таких разделов математики, как теория сложности вычислений, теория чисел, алгебра, теория информации и др. Желающим серьезно изучать криптографию можно порекомендовать обзорную монографию «Криптография в банковском деле» Анохина М. И., Варновского Н. П., Сидельникова В. М., Ященко В. В., М.: МИФИ, 1997.

*Октябрь* 1998 *г.* *В. Ященко*

## Глава 1

# Основные понятия криптографии

## § 1. Введение

*Как передать нужную информацию нужному адресату в тайне от других*? Каждый из читателей в разное время и с разными целями наверняка пытался решить для себя эту практическую задачу (для удобства дальнейших ссылок назовем ее «задача ТП», т. е. задача *Тайной Передачи*). Выбрав подходящее решение, он, скорее всего, повторил изобретение одного из способов скрытой передачи информации, которым уже не одна тысяча лет.

Размышляя над задачей ТП, нетрудно прийти к выводу, что есть три возможности.

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами.

2. Использовать общедоступный канал связи, но скрыть сам факт передачи информации.

3. Использовать общедоступный канал связи, но передавать по нему нужную информацию в так преобразованном виде, чтобы восстановить ее мог только адресат.

Прокомментируем эти три возможности.

1. При современном уровне развития науки и техники сделать такой канал связи между удаленными абонентами для неоднократной передачи больших объемов информации практически нереально.

2. Разработкой средств и методов скрытия факта передачи сообщения занимается *стеганография*.

Первые следы стеганографических методов теряются в глубокой древности. Например, известен такой способ скрытия письменного сообщения: голову раба брили, на коже головы писали сообщение и после отрастания волос раба отправляли к адресату.

Из детективных произведений хорошо известны различные способы тайнописи между строк обычного, незащищаемого текста: от молока до сложных химических реактивов с последующей обработкой.

Также из детективов известен метод «*микроточки*»: сообщение записывается с помощью современной техники на очень маленький носитель (микроточку), который пересылается с обычным письмом, например, под маркой или где-нибудь в другом, заранее обусловленном месте.

В настоящее время в связи с широким распространением компьютеров известно много тонких методов «запрятывания» защищаемой информации внутри больших объемов информации, хранящейся в компьютере. Наглядный пример запрятывания текстового файла в графический можно найти в Интернете[1]; он же приведен в журнале «Компьютерра», № 48 (225) от 1 декабря 1997 г., на стр. 62. (Следует отметить, что авторы статьи в журнале ошибочно относят стеганографию к криптографии. Конечно, с помощью стеганографии можно прятать и предварительно зашифрованные тексты, но, вообще говоря, стеганография и криптография — принципиально различные направления в теории и практике защиты информации.)

3. Разработкой методов преобразования (*шифрования*) информации с целью ее защиты от незаконных пользователей занимается *криптография*. Такие методы и способы преобразования информации называются *шифрами*.

*Шифрование* (*зашифрование*) — процесс применения шифра к защищаемой информации, т. е. преобразование защищаемой информации (*открытого текста*) в шифрованное сообщение (*шифртекст*, *криптограмму*) с помощью определенных правил, содержащихся в шифре.

*Дешифрование* — процесс, обратный шифрованию, т. е. преобразование шифрованного сообщения в открытый текст с помощью определенных правил, содержащихся в шифре.

Криптография — прикладная наука, она использует самые последние — прикладная наука, она использует самые последние достижения другой стороны, все конкретные задачи криптографии существенно зависят от уровня развития техники и технологии, от применяемых средств связи и способов передачи информации.

## § 2. Предмет криптографии

*Что же является предметом криптографии*? Для ответа на этот вопрос вернемся к задаче ТП, чтобы уточнить ситуацию и используемые понятия.

Прежде всего заметим, что эта задача возникает только для информации, которая нуждается в защите. Обычно в таких случаях говорят, что информация содержит тайну или является *защищаемой*, *приватной*,

[1] `http://www.geocities.com/SiliconValley/Vista/6001/`

*конфиденциальной*, *секретной*. Для наиболее типичных, часто встречающихся ситуаций такого типа введены даже специальные понятия:

— государственная тайна;

— военная тайна;

— коммерческая тайна;

— юридическая тайна;

— врачебная тайна и т. д.

Далее мы будем говорить о защищаемой информации, имея в виду следующие признаки такой информации:

— имеется какой-то определенный круг *законных пользователей*, которые имеют право владеть этой информацией;

— имеются *незаконные пользователи*, которые стремятся овладеть этой информацией с тем, чтобы обратить ее себе во благо, а законным пользователям во вред.

Для простоты мы вначале ограничимся рассмотрением только одной *угрозы* — угрозы разглашения информации. Существуют и другие угрозы для защищаемой информации со стороны незаконных пользователей: подмена, имитация и др. О них мы поговорим ниже.

Теперь мы можем изобразить ситуацию, в которой возникает задача ТП, следующей схемой (см. рис. 1).

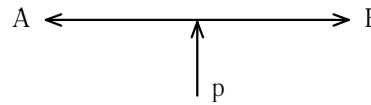


Рис. 1

Здесь A и B — законные пользователи защищаемой информации; они хотят обмениваться информацией по общедоступному каналу связи. П — незаконный пользователь (*противник*), который может перехватывать передаваемые по каналу связи сообщения и пытаться извлечь из них интересующую его информацию. Эту формальную схему можно считать моделью типичной ситуации, в которой применяются криптографические методы защиты информации.

Отметим, что исторически в криптографии закрепились некоторые военные слова (противник, атака на шифр и др.) Они наиболее точно отражают смысл соответствующих криптографических понятий. Вместе с тем широко известная военная терминология, основанная на понятии кода (военно-морские коды, коды Генерального штаба, кодовые книги, кодобозначения и т. п.), уже не применяется в теоретической криптографии. Дело в том, что за последние десятилетия сформировалась *теория кодирования* — большое научное направление, которое

разрабатывает и изучает методы защиты информации от случайных искажений в каналах связи. И если ранее термины кодирование и шифрование употреблялись как синонимы, то теперь это недопустимо. Так, например, очень распространенное выражение «кодирование — разновидность шифрования» становится просто неправильным.

Криптография занимается методами преобразования информации, которые бы не позволили противнику извлечь ее из перехватываемых сообщений. При этом по каналу связи передается уже не сама защищаемая информация, а результат ее преобразования с помощью шифра, и для противника возникает сложная задача *вскрытия шифра*.

*Вскрытие* (*взламывание*) *шифра* — процесс получения открытого текста из шифрованного сообщения без знания примененного шифра.

Однако помимо перехвата сообщений и вскрытия шифра противник может пытаться получить защищаемую информацию многими другими способами. Наиболее известным из таких способов является агентурный, когда противник каким-либо путем склоняет к сотрудничеству одного из законных пользователей и с помощью этого агента получает доступ к защищаемой информации. В такой ситуации криптография бессильна.

Противник может пытаться не получить, а уничтожить или модифицировать защищаемую информацию в процессе ее передачи. Это — совсем другой тип угроз для информации, отличный от перехвата сообщений и вскрытия шифра. Для защиты от таких угроз разрабатываются свои специфические методы.

Следовательно, на пути от одного законного пользователя к другому информация должна защищаться различными способами, противостоящими различным угрозам. Возникает ситуация цепи из разнотипных звеньев, которая защищает информацию. Естественно, противник будет стремиться найти самое слабое звено, чтобы с наименьшими затратами добраться до информации. А значит, и законные пользователи должны учитывать это обстоятельство в своей стратегии защиты: бессмысленно делать какое-то звено очень прочным, если есть заведомо более слабые звенья («принцип равнопрочности защиты»).

Не следует забывать и еще об одной важной проблеме: проблеме соотношения цены информации, затрат на ее защиту и затрат на ее добывание. При современном уровне развития техники сами средства связи, а также разработка средств перехвата информации из них и средств защиты информации требуют очень больших затрат. Прежде чем защищать информацию, задайте себе два вопроса:

1) является ли она для противника более ценной, чем стоимость атаки;

2) является ли она для вас более ценной, чем стоимость защиты.

Именно перечисленные соображения и являются решающими при выборе подходящих средств защиты: физических, стеганографических, криптографических и др.

Некоторые понятия криптографии удобно иллюстрировать историческими примерами, поэтому сделаем небольшое историческое отступление.

Долгое время занятие криптографией было уделом чудаков-одиночек. Среди них были одаренные ученые, дипломаты, священнослужители. Известны случаи, когда криптография считалась даже черной магией. Этот период развития криптографии как искусства длился с незапамятных времен до начала XX века, когда появились первые шифровальные машины. Понимание математического характера решаемых криптографией задач пришло только в середине XX века — после работ выдающегося американского ученого К. Шеннона.

История криптографии связана с большим количеством дипломатических и военных тайн и поэтому окутана туманом легенд. Наиболее полная книга по истории криптографии содержит более тысячи страниц. Она опубликована[1] в 1967 году. Имеется перевод этой книги на русский язык (*Кан Д.* Взломщики кодов. М., Центрполиграф, 2000). Книга Т. А. Соболевой[2] представляет собой фундаментальный труд по истории криптографии в России.

Свой след в истории криптографии оставили многие хорошо известные исторические личности. Приведем несколько наиболее ярких примеров. Первые сведения об использовании шифров в военном деле связаны с именем спартанского полководца Лисандра (шифр «Сцитала»). Цезарь использовал в переписке шифр, который вошел в историю как «шифр Цезаря». В древней Греции был изобретен вид шифра, который в дальнейшем стал называться «квадрат Полития». Одну из первых книг по криптографии написал аббат И. Трителий (1462–1516), живший в Германии. В 1566 году известный математик Д. Кардано опубликовал работу с описанием изобретенной им системы шифрования («решетка Кардано»). Франция XVI века оставила в истории криптографии шифры короля Генриха IV и Ришелье. В упомянутой книге Т. А. Соболевой подробно описано много российских шифров, в том числе и «цифирная азбука» 1700 года, автором которой был Петр Великий. (Некоторые примеры из книги приведены на форзаце.)

Некоторые сведения о свойствах шифров и их применении можно найти и в художественной литературе, особенно в приключенческой, детективной и военной. Хорошее подробное объяснение особенностей одного из простейших шифров — *шифра замены* и методов его вскрытия содержится в двух известных рассказах: «Золотой жук» Э. По и «Пляшущие человечки» А. Конан Дойла.

Рассмотрим более подробно два примера.

Шифр «Сцитала». Этот шифр известен со времен войны Спарты против Афин в V веке до н. э. Для его реализации использовалась сцитала — жезл, имеющий форму цилиндра. На сциталу виток к витку наматывалась узкая папирусная лента

[1] *Kahn David*. Codebreakers. The story of Secret Writing. New York: Macmillan, 1967.

[2] *Соболева Т. А.* Тайнопись в истории России (История криптографической службы России XVIII–начала XX в.). М., 1994.

(без просветов и нахлестов), а затем на этой ленте вдоль оси сциталы записывался открытый текст. Лента разматывалась и получалось (для непосвященных), что на ленте в беспорядке написаны какие-то буквы (каждая из букв поперек ленты). Затем лента отправлялась адресату. Адресат брал такую же сциталу, таким же образом наматывал на нее полученную ленту и читал сообщение вдоль оси сциталы.

Отметим, что в этом шифре преобразование открытого текста в шифрованный заключается в определенной перестановке букв открытого текста. Поэтому класс шифров, к которым относится и шифр «Сцитала», называется *шифрами перестановки*.

Шифр Цезаря. Этот шифр реализует следующее преобразование открытого текста: каждая буква открытого текста заменяется третьей после нее буквой в алфавите, который считается написанным по кругу, т. е. после буквы «я» следует буква «а». Отметим, что Цезарь заменял букву третьей после нее буквой, но можно заменять и какой-нибудь другой. Главное, чтобы тот, кому посылается шифрованное сообщение, знал эту величину сдвига. Класс шифров, к которым относится и шифр Цезаря, называется *шифрами замены*.

Из предыдущего изложения понятно, что придумывание хорошего шифра — дело трудоемкое. Поэтому желательно увеличить «время жизни» хорошего шифра и использовать его для шифрования как можно большего количества сообщений. Но при этом возникает опасность, что противник уже разгадал (вскрыл) шифр и читает защищаемую информацию. Если же в шифре есть сменный ключ, то, заменив ключ, можно надеяться, что разработанные противником методы уже не дают эффекта.

Под *ключом* в криптографии понимают сменный элемент шифра, который применяется для шифрования сообщений. Например, в шифре «Сцитала» ключом является диаметр сциталы, а в шифрах типа шифра Цезаря ключом является величина сдвига букв шифртекста относительно букв открытого текста.

Описанные соображения привели к тому, что безопасность защищаемой информации стала определяться в первую очередь ключом. Сам шифр, шифрмашина или принцип шифрования стали считать известными противнику и доступными для предварительного изучения, но в них появился неизвестный для противника ключ, от которого существенно зависят применяемые преобразования информации. Теперь законные пользователи, прежде чем обмениваться шифрованными сообщениями, должны тайно от противника обменяться ключами или установить одинаковый ключ на обоих концах канала связи. А для противника появилась новая задача — определить ключ, после чего можно легко прочитать зашифрованные на этом ключе сообщения.

Вернемся к формальному описанию основного объекта криптографии (рис. 1, стр. 199). Теперь в него необходимо внести существенное измене-

ние — добавить недоступный для противника секретный канал связи для обмена ключами (см. рис. 2). Создать такой канал связи вполне реально, поскольку нагрузка на него, вообще говоря, небольшая.

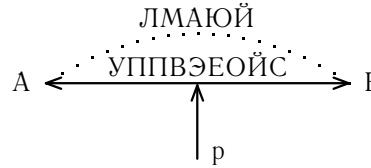


Рис. 2

Отметим теперь, что не существует единого шифра, подходящего для всех случаев. Выбор способа шифрования зависит от особенностей информации, ее ценности и возможностей владельцев по защите своей информации. Прежде всего подчеркнем большое разнообразие видов защищаемой информации: документальная, телефонная, телевизионная, компьютерная и т. д. Каждый вид информации имеет свои специфические особенности, и эти особенности сильно влияют на выбор методов шифрования информации. Большое значение имеют объемы и требуемая скорость передачи шифрованной информации. Выбор вида шифра и его параметров существенно зависит от характера защищаемых секретов или тайны. Некоторые тайны (например, государственные, военные и др.) должны сохраняться десятилетиями, а некоторые (например, биржевые) — уже через несколько часов можно разгласить. Необходимо учитывать также и возможности того противника, от которого защищается данная информация. Одно дело — противостоять одиночке или даже банде уголовников, а другое дело — мощной государственной структуре.

Способность шифра противостоять всевозможным атакам на него называют *стойкостью шифра*.

Под *атакой на шифр* понимают попытку вскрытия этого шифра.

Понятие стойкости шифра является центральным для криптографии. Хотя качественно понять его довольно легко, но получение строгих доказуемых оценок стойкости для каждого конкретного шифра — проблема нерешенная. Это объясняется тем, что до сих пор нет необходимых для решения такой проблемы математических результатов. (Мы вернемся к обсуждению этого вопроса ниже.) Поэтому стойкость конкретного шифра оценивается только путем всевозможных попыток его вскрытия и зависит от квалификации *криптоаналитиков*, атакующих шифр. Такую процедуру иногда называют *проверкой стойкости*.

Важным подготовительным этапом для проверки стойкости шифра является продумывание различных предполагаемых возможностей, с помо-

щью которых противник может атаковать шифр. Появление таких возможностей у противника обычно не зависит от криптографии, это является некоторой внешней подсказкой и существенно влияет на стойкость шифра. Поэтому оценки стойкости шифра всегда содержат те предположения о целях и возможностях противника, в условиях которых эти оценки получены.

Прежде всего, как это уже отмечалось выше, обычно считается, что противник знает сам шифр и имеет возможности для его предварительного изучения. Противник также знает некоторые характеристики открытых текстов, например общую тематику сообщений, их стиль, некоторые стандарты, форматы и т. д.

Из более специфических приведем еще три примера возможностей противника:

— противник может перехватывать все шифрованные сообщения, но не имеет соответствующих им открытых текстов;

— противник может перехватывать все шифрованные сообщения и добывать соответствующие им открытые тексты;

— противник имеет доступ к шифру (но не к ключам!) и поэтому может зашифровывать и дешифровывать любую информацию.

На протяжении многих веков среди специалистов не утихали споры о стойкости шифров и о возможности построения абсолютно стойкого шифра. Приведем три характерных высказывания на этот счет.

Английский математик Чарльз Беббидж (XIX в.):

«Всякий человек, даже если он не знаком с техникой вскрытия шифров, твердо считает, что сможет изобрести абсолютно стойкий шифр, и чем более умен и образован этот человек, тем более твердо это убеждение. Я сам разделял эту уверенность в течение многих лет».

«Отец кибернетики» Норберт Винер:

«Любой шифр может быть вскрыт, если только в этом есть настоятельная необходимость и информация, которую предполагается получить, стоит затраченных средств, усилий и времени...»

Автор шифра PGP Ф. Зиммерманн («Компьютерра», №48 от 1.12.1997, стр. 45–46):

«Каждый, кто думает, что изобрел непробиваемую схему шифрования, — или невероятно редкий гений, или просто наивен и неопытен...»

«Каждый программист воображает себя криптографом, что ведет к распространению исключительно плохого криптообеспечения...»

В заключение данного раздела сделаем еще одно замечание — о терминологии. В последнее время наряду со словом «криптография» часто встречается и слово «криптология», но соотношение между ними не всегда понимается правильно. Сейчас происходит окончательное формирование этих научных дисциплин, уточняются их предмет и задачи.

*Криптография* — инженерно-техническая дисциплина, которая занимается математическими методами защиты информации. Включает в себя криптосинтез и криптоанализ.

*Криптосинтез* — та часть криптографии, которая занимается разработкой криптографических средств защиты информации.

*Криптоанализ* — совокупность методов и способов вскрытия криптографических схем.

*Криптология*, или, что то же самое, *теоретическая* (или *математическая*) *криптография* — отрасль дискретной математики, предметом которой является исследование математических моделей криптографических схем.

Соотношение криптосинтеза и криптоанализа очевидно: криптосинтез — защита, например разработка шифров, а криптоанализ — нападение, т. е. атака на шифры. Однако эти две дисциплины связаны друг с другом, и не бывает хороших криптографов, не владеющих методами криптоанализа.

## § 3. Математические основы

Большое влияние на развитие криптографии оказали появившиеся в середине XX века работы американского математика Клода Шеннона. В этих работах были заложены основы теории информации, а также был разработан математический аппарат для исследований во многих областях науки, связанных с информацией. Более того, принято считать, что теория информации как наука родилась в 1948 году после публикации работы К. Шеннона «Математическая теория связи»[1].

В своей работе[2] «Теория связи в секретных системах» Клод Шеннон обобщил накопленный до него опыт разработки шифров. Оказалось, что даже в очень сложных шифрах в качестве типичных компонентов можно выделить, по крайней мере теоретически, такие простые шифры, как *шифры замены*, *шифры перестановки* или их сочетания.

Шифр замены является простейшим, наиболее популярным шифром. Типичными примерами являются шифр Цезаря, «цифирная азбука» Петра Великого и «пляшущие человечки» А. Конан Дойла. Как видно из самого названия, шифр замены осуществляет преобразование замены букв или других «частей» открытого текста на аналогичные «части» шифрованного текста. Легко дать математическое описание шифра замены. Пусть $X$

[1] *Shannon C. E.* A mathematical theory of communication // Bell System Techn. J. V. 27, № 3, 1948. P. 379–423; V. 27, № 4, 1948. P. 623–656.

[2] См. Приложение.

и $Y$ — два алфавита (открытого и шифрованного текстов соответственно), состоящие из одинакового числа символов. Пусть также $g\colon X \to Y$ — взаимно однозначное отображение $X$ в $Y$. Тогда шифр замены действует так: открытый текст $x_1x_2 \ldots x_n$ преобразуется в шифрованный текст $g(x_1)g(x_2) \ldots g(x_n)$.

Шифр перестановки, как видно из названия, осуществляет преобразование перестановки букв в открытом тексте. Типичным примером шифра перестановки является шифр «Сцитала». Обычно открытый текст разбивается на блоки равной длины и каждый блок шифруется независимо. Пусть, например, длина блоков равна $n$ и $\sigma$ — взаимнооднозначное отображение множества $\{1, 2, \ldots, n\}$ в себя. Тогда шифр перестановки действует так: блок открытого текста $x_1 \ldots x_n$ преобразуется в блок шифрованного текста $x_{\sigma(1)} \ldots x_{\sigma(n)}$.

Важнейшим для развития криптографии был результат К. Шеннона о существовании абсолютно стойкого шифра. Любой такой шифр подобен так называемой ленте одноразового использования в том смысле, что секретный ключ должен быть полностью случайным, одноразовым, и его длина должна быть не меньше длины открытого текста.

Этот результат был доказан К. Шенноном с помощью разработанного им теоретико-информационного метода исследования шифров. Мы не будем здесь останавливаться на этом подробно, заинтересованному читателю рекомендуем изучить работу К. Шеннона [1].

Обсудим особенности строения абсолютно стойкого шифра и возможности его практического использования. Типичным и наиболее простым примером реализации абсолютно стойкого шифра является шифр Вернама, который осуществляет побитовое сложение $n$-битового открытого текста и $n$-битового ключа:

$$y_i = x_i \oplus k_i, \qquad i = 1, \ldots, n.$$

Здесь $x_1 \ldots x_n$ — открытый текст, $k_1, \ldots, k_n$ — ключ, $y_1 \ldots y_n$ — шифрованный текст.

Подчеркнем, что для абсолютной стойкости существенным является каждое из следующих требований к ленте однократного использования:

1) полная случайность (равновероятность) ключа (это, в частности, означает, что ключ нельзя вырабатывать с помощью какого-либо детерминированного устройства);

2) равенство длины ключа и длины открытого текста;

3) однократность использования ключа.

[1] См. Приложение.

ВВЕДЕНИЕ В КРИПТОГРАФИЮ

Под редакцией В. В. Ященко

Подписано в печать 04.09.2012 г. Формат $60 \times 90\ 1/16$. Бумага офсетная.
Печать офсетная. Печ. л. 22. Тираж 2000 экз. Заказ №

Издательство Московского центра непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241–74–83.

Отпечатано по технологии CtP в ИПК ООО «Ленинградское издательство»
194044, Санкт-Петербург, ул. Менделеевская, д. 9. Тел./факс: (812) 495–56–10

Книги издательства МЦНМО можно приобрести в магазине «Математическая книга»,
Большой Власьевский пер., д. 11. Тел. (499) 241–72–85. E-mail: biblio@mccme.ru
http:// biblio.mccme.ru