Основные понятия криптографии*

В. В. Ященко

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 *ТайноПиси*). 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.

*Настоящая статья является сокращенным переработанным вариантом книги С. А. Дориченко и В. В. Ященко «25 этюдов о шифрах», М.: Теис, 1994.

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 защищаемую информацию с помощью определенных правил, содержащихся в шифре.

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

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, конфиденциальной, секретной*. Для наиболее типичных, часто встречаю-

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

щихся 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).

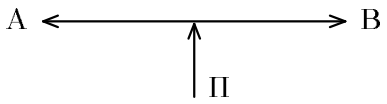

Рис. 1.

Здесь A и B — удаленные 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 зашишаемая информация, а результат ее преобразования с помошью шифра, и для противника возникает сложная задача *вскрытия шифра*.

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

Однако помимо перехвата и вскрытия шифра противник может пытаться получить зашишаемую 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 помошью этого агента получает доступ к зашищаемой информации. В такой ситуации криптография бессильна.

Противник может пытаться не получить, а уничтожить или модифицировать зашишаемую информацию в процессе ее передачи. Это — совсем другой тип угроз для информации, отличный от перехвата и вскрытия шифра. Для зашиты 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 зашишает 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 зашиты: бессмысленно делать какое-то звено очень прочным, если есть заведомо более слабые звенья («принцип равнопрочности зашиты»).

Не следует забывать и ещё об одной важной проблеме: проблеме соотношения цены информации, затрат на ее зашиту и затрат на ее добывание. При современном уровне развития техники сами средства связи, а также разработка средств перехвата информации из них и средств зашиты информации требуют очень больших затрат. Прежде чем зашишать 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 зашиты.

Именно перечисленные соображения и являются решающими при выборе подходящих средств зашиты: 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 учёные, 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 учёного 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 в 1967 году и на русский язык не переведена[2)]. На русском языке недавно вышел в свет фундаментальный труд по истории криптографии в России[3)].

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 «Сциталь»). Цезарь использовал в переписке шифр, который вошёл 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 («решётка 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 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-Дойля.

Рассмотрим более подробно два примера.

Шифр «Сциталь». Этот шифр известен со времен войны Спарты против Афин в V веке до н.э. Для его реализации использовался сциталь — жезл, имеющий форму цилиндра. На сциталь виток к витку наматывалась узкая папирусная лента (без пробелов и нахлестов), а затем на этой ленте вдоль оси сциталя записывался открытый текст. Лента разматывалась и получалось (для

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

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

непосвященных), что поперек ленты в беспорядке написаны какие-то буквы. Затем лента отправлялась адресату. Адресат брал такой же сциталь, таким же образом наматывал на него полученную ленту и читал сообщение вдоль оси сциталя.

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 «Сциталь», 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 зашишаемую информацию. Если же в шифре есть сменный ключ, то, заменив ключ, можно сделать так, что разработанные противником методы уже не дают эффекта.

Под *ключом* в криптографии понимают сменный элемент шифра, который применяется для шифрования конкретного сообщения. Например, в шифре «Сциталь» ключом является диаметр сциталя, 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. 55). Теперь в него необходимо внести существенное изменение — добавить недоступный для противника секретный канал связи для

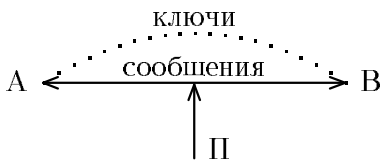

Рис. 2.

обмена ключами (см. рис. 2). Создать такой канал связи вполне реально, поскольку нагрузка на него, вообще говоря, небольшая.

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 подчеркнём 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

помощью 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 ещё 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 счёт.

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 ведёт к распространению исключительно плохого криптообеспечения...»

В заключение данного раздела сделаем ещё 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.

Криптология — наука, состоящая из двух ветвей: криптографии и криптоанализа.

Криптография — наука о способах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей.

Криптоанализ — наука (и практика ее применения) о методах и способах вскрытия шифров.

Соотношение криптографии и криптоанализа очевидно: криптография — защита, т. е. 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.

Математические основы

Большое влияние на развитие криптографии оказали появившиеся в середине нашего 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. (Отметим, кстати, что нынешний 1998 год — юбилейный для теории информации. Принято считать, что теория информации как наука родилась в 1948 году после публикации работы К. Шеннона «Математическая теория связи»[4].)

В своей работе «Теория связи в секретных системах» Клод Шеннон обобщил накопленный до него опыт разработки шифров. Оказалось, что даже в сложных шифрах в качестве типичных компонентов можно выделить *шифры замены, шифры перестановки* или их сочетания.

Шифр замены является простейшим, наиболее популярным шифром. Типичными примерами являются шифр Цезаря, «шифрная азбука» Петра Великого и «пляшущие человечки» А. Конан-Дойля. 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 и Y — два алфавита (открытого и шифрованного текстов соответственно), состоящие из одинакового числа символов. Пусть также $g\colon X \to Y$ — взаимнооднозначное отображение X в Y. Тогда шифр замены действует так: открытый текст $x_1x_2\ldots x_n$ преобразуется в шифрованный текст $g(x_1)g(x_2)\ldots g(x_n)$.

[4] *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.

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

Важнейшим для развития криптографии был результат К. Шеннона о существовании и единственности абсолютно стойкого шифра. Единственным таким шифром является какая-нибудь форма так называемой *ленты однократного использования*, в которой открытый текст «объединяется» с полностью случайным ключом такой же длины.

Этот результат был доказан К. Шенноном с помошью разработанного им теоретико-информационного метода исследования шифров. Мы не будем здесь останавливаться на этом подробно, заинтересованному читателю рекомендуем изучить работу К. Шеннона[5)].

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:

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

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

Подчеркнём, 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.

В случае нарушения хотя бы одного из этих условий шифр перестает быть абсолютно стойким и появляются принципиальные возможности для его вскрытия (хотя они могут быть трудно реализуемыми).

[5)] *Shannon C. E.* Communication theory of secrecy systems // Bell System Techn. J. V. 28, №4, 1949. P. 656–715.
Русск. пер. в: *Шеннон К.* Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 333–403.

Но, оказывается, именно эти условия и делают абсолютно стойкий шифр очень дорогим и непрактичным. Прежде чем пользоваться таким шифром, мы должны обеспечить всех абонентов достаточным запасом случайных ключей и исключить возможность их повторного применения. А это сделать необычайно трудно и дорого.

Как отмечал Д. Кан: «Проблема создания, регистрации, распространения и отмены ключей может показаться не слишком сложной тому, кто не имеет опыта передачи сообщений по каналам военной связи, но в военное время объем передаваемых сообщений ставит в тупик даже профессиональных связистов. За сутки могут быть зашифрованы сотни тысяч слов. Создание миллионов ключевых знаков потребовало бы огромных финансовых издержек и было бы сопряжено с большими затратами времени. Так как каждый текст должен иметь свой собственный, единственный и неповторимый ключ, применение идеальной системы потребовало бы передачи по крайней мере такого количества знаков, которое эквивалентно всему объему передаваемой военной информации.»

В силу указанных причин абсолютно стойкие шифры применяются только в сетях связи с небольшим объемом передаваемой информации, обычно это сети для передачи особо важной государственной информации.

Теперь уже понятно, что чаще всего для защиты своей информации законные пользователи вынуждены применять неабсолютно стойкие шифры. Такие шифры, по крайней мере теоретически, могут быть вскрыты. Вопрос только в том, хватит ли у противника сил, средств и времени для разработки и реализации соответствующих алгоритмов. Обычно эту мысль выражают так: противник с неограниченными ресурсами может вскрыть любой неабсолютно стойкий шифр.

Как же должен действовать в этой ситуации законный пользователь, выбирая для себя шифр? Лучше всего, конечно, было бы доказать, что никакой противник не может вскрыть выбранный шифр, скажем, за 10 лет и тем самым получить теоретическую оценку стойкости. К сожалению, математическая теория ещё не даёт нужных теорем — они относятся к нерешенной *проблеме нижних оценок сложности задач*.

Поэтому у пользователя остается единственный путь — получение практических оценок стойкости. Этот путь состоит из следующих этапов:

– понять и чётко сформулировать, от какого противника мы собираемся защищать информацию; необходимо уяснить, что именно противник знает или сможет узнать о системе шифра, а также какие силы и средства он сможет применить для его вскрытия;

– мысленно стать в положение противника и пытаться с его позиций атаковать шифр, т. е. разрабатывать различные алгоритмы вскрытия

шифра; при этом необходимо в максимальной мере обеспечить моделирование сил, средств и возможностей противника;
– наилучший из разработанных алгоритмов использовать для практической оценки стойкости шифра.

Здесь полезно для иллюстрации упомянуть о двух простейших методах вскрытия шифра: случайное угадывание ключа (он срабатывает с маленькой вероятностью, зато имеет маленькую сложность) и перебор всех подряд ключей вплоть до нахождения истинного (он срабатывает всегда, зато имеет очень большую сложность). Отметим также, что не всегда нужна атака на ключ: для некоторых шифров можно сразу, даже не зная ключа, восстанавливать открытый текст по шифрованному.

Новые направления

В 1983 году в книге «Коды и математика» М. Н. Аршинова и Л. Е. Садовского (библиотечка «Квант») было написано: «Приемов тайнописи — великое множество, и, скорее всего, это та область, где уже нет нужды придумывать что-нибудь существенно новое.» Однако это было очередное большое заблуждение относительно криптографии. Еще в 1976 году была опубликована работа молодых американских математиков У. Диффи и М. Э. Хеллмана «Новые направления в криптографии»[6)], которая не только существенно изменила криптографию, но и привела к появлению и бурному развитию новых направлений в математике. Центральным понятием «новой криптографии» является понятие односторонней функции (подробнее об этом см. статью Н. П. Варновского в настоящем номере журнала, стр. 71–86).

Односторонней называется функция $F\colon X \to Y$, обладающая двумя свойствами:
а) существует полиномиальный алгоритм вычисления значений $F(x)$;
б) не существует полиномиального алгоритма *инвертирования* функции F (т. е. решения уравнения $F(x) = y$ относительно x для непренебрежимо малой доли области значений функции).

Отметим, что односторонняя функция существенно отличается от функций, привычных со школьной скамьи, из-за ограничений на сложность ее вычисления и инвертирования. Вопрос о существовании односторонних функций пока открыт.

Другим понятием, более близким к традиционной криптографии, в которой есть секретный ключ, является понятие *функции с секретом*.

[6)] *Диффи У., Хеллман М. Э.* Защищенность и имитостойкость. Введение в криптографию // ТИИЭР. Т. 67, №3, 1979.

Иногда ещё употребляется термин *функция с ловушкой*. *Функцией с секретом* K называется функция $F_K\colon X \to Y$, зависящая от параметра K и обладающая тремя свойствами:
а) при любом K существует полиномиальный алгоритм вычисления значений $F_K(x)$;
б) при неизвестном K не существует полиномиального алгоритма инвертирования F_K;
в) при известном K существует полиномиальный алгоритм инвертирования F_K.

Про существование функций с секретом можно сказать то же самое, что сказано про односторонние функции. Для практических целей криптографии было построено несколько функций, которые могут оказаться функциями с секретом. Для них свойство б) пока строго не доказано, но известно, что задача инвертирования эквивалентна некоторой давно изучаемой трудной математической задаче. Наиболее известной и популярной из них является теоретико-числовая функция, на которой построен шифр RSA (подробнее об этом см. статью Ю. В. Нестеренко в настоящем номере журнала, стр. 87–114).

Применение функций с секретом в криптографии позволяет:

1) организовать обмен шифрованными сообщениями с использованием только открытых каналов связи, т. е. отказаться от секретных каналов связи для предварительного обмена ключами;

2) включить в задачу вскрытия шифра трудную математическую задачу и тем самым повысить обоснованность стойкости шифра;

3) решать новые криптографические задачи, отличные от шифрования (*цифровая подпись* и др.).

Опишем, например, как можно реализовать п. 1). Пользователь A, который хочет получать шифрованные сообщения, должен выбрать какую-нибудь функцию F_K с секретом K. Он сообщает всем заинтересованным (например, публикует) описание функции F_K в качестве своего алгоритма шифрования. Но при этом значение секрета K он никому не сообщает и держит в секрете. Если теперь пользователь B хочет послать пользователю A зашишаемую информацию $x \in X$, то он вычисляет $y = F_K(x)$ и посылает y по открытому каналу пользователю A. Поскольку A для своего секрета K умеет инвертировать F_K, то он вычисляет x по полученному y. Никто другой не знает K и поэтому в силу свойства б) функции с секретом не сможет за полиномиальное время по известному шифрованному сообщению $F_K(x)$ вычислить зашишаемую информацию x.

Описанную систему называют *криптосистемой с открытым ключом*, поскольку алгоритм шифрования F_K является общедоступным или

открытым. В последнее время такие криптосистемы ещё называют *асимметричными*, поскольку в них есть асимметрия в алгоритмах: алгоритмы шифрования и дешифрования различны. В отличие от таких систем традиционные шифры называют *симметричными*: в них ключ для шифрования и дешифрования один и тот же, и именно поэтому его нужно хранить в секрете. Для асимметричных систем алгоритм шифрования общеизвестен, но восстановить по нему алгоритм дешифрования за полиномиальное время невозможно.

Описанную выше идею Диффи и Хеллман предложили использовать также для цифровой подписи сообщений, которую невозможно подделать за полиномиальное время. Пусть пользователю A необходимо подписать сообщение x. Он, зная секрет K, находит такое y, что $F_K(y) = x$, и посылает y пользователю B в качестве своей цифровой подписи. Пользователь B хранит y в качестве доказательства того, что A подписал сообщение x.

Сообщение, подписанное цифровой подписью, можно представлять себе как пару (x, y), где x — сообщение, y — решение уравнения $F_K(y) = x$, $F_K\colon X \to Y$ — функция с секретом, известная всем взаимодействующим абонентам. Из определения функции F_K очевидны следующие достоинства цифровой подписи:

1) подписать сообщение x, т. е. решить уравнение $F_K(y) = x$, может только абонент — обладатель данного секрета K; другими словами, подделать подпись невозможно;

2) проверить подлинность подписи может любой абонент, знающий открытый ключ, т. е. саму функцию F_K;

3) при возникновении споров отказаться от подписи невозможно в силу ее неподделываемости;

4) подписанные сообщения (x, y) можно, не опасаясь ущерба, пересылать по любым каналам связи.

Кроме принципа построения криптосистемы с открытым ключом, Диффи и Хеллман в той же работе предложили ещё одну новую идею — *открытое распределение ключей*. Они задались вопросом: можно ли организовать такую процедуру взаимодействия абонентов A и B по открытым каналам связи, чтобы решить следующие задачи:

1) вначале у A и B нет никакой общей секретной информации, но в конце процедуры такая общая секретная информация (общий ключ) у A и B появляется, т. е. вырабатывается;

2) противник, который перехватывает все передачи информации и знает, что хотят получить A и B, тем не менее не может восстановить выработанный общий ключ A и B.

Диффи и Хеллман предложили решать эти задачи с помощью функции

$$F(x) = \alpha^x \pmod p,$$

где p — большое простое число, x — произвольное натуральное число, α — некоторый *примитивный элемент* поля $GF(p)$. Общепризнанно, что инвертирование функции $\alpha^x \pmod p$, т.е. дискретное логарифмирование, является трудной математической задачей.

Сама процедура или, как принято говорить, *протокол выработки общего ключа* описывается следующим образом.

Числа p и α считаются общедоступными.

Абоненты A и B независимо друг от друга случайно выбирают по одному натуральному числу — скажем x_A и x_B. Эти элементы они держат в секрете. Далее каждый из них вычисляет новый элемент:

$$y_A = \alpha^{x_A} \pmod p, \quad y_B = \alpha^{x_B} \pmod p.$$

Потом они обмениваются этими элементами по каналу связи. Теперь абонент A, получив y_B и зная свой секретный элемент x_A, вычисляет новый элемент

$$y_B^{x_A} \pmod p = (\alpha^{x_B})^{x_A} \pmod p.$$

Аналогично поступает абонент B:

$$y_A^{x_B} \pmod p = (\alpha^{x_A})^{x_B} \pmod p.$$

Тем самым у A и B появился общий элемент поля, равный $\alpha^{x_A x_B}$. Этот элемент и объявляется общим ключом A и B.

Из описания протокола видно, что противник знает $p, \alpha, \alpha^{x_A}, \alpha^{x_B}$, не знает x_A и x_B и хочет узнать $\alpha^{x_A x_B}$. В настоящее время нет алгоритмов действий противника, более эффективных, чем дискретное логарифмирование, а это — трудная математическая задача.

Успехи, достигнутые в разработке схем цифровой подписи и открытого распределения ключей, позволили применить эти идеи также и к другим задачам взаимодействия удаленных абонентов. Так возникло большое новое направление теоретической криптографии — криптографические протоколы. Под *криптографическим протоколом* понимают такую процедуру взаимодействия абонентов, в результате которой абоненты (не противники!) достигают своей цели, а противник — не достигает.

Объектом изучения теории криптографических протоколов являются удаленные абоненты, взаимодействующие по открытым каналам связи. Целью взаимодействия абонентов является решение какой-то задачи. Имеется также противник, который преследует собственные цели. При этом противник в разных задачах может иметь разные возможности: например, может взаимодействовать с абонентами от имени других абонентов или вмешиваться в обмены информацией между абонентами и т. д.

Противником может даже оказаться один из абонентов или несколько абонентов, вступивших в сговор.

Приведем ещё несколько примеров задач, решаемых удаленными абонентами. (Читателю рекомендуем по своему вкусу самостоятельно придумать ещё какие-нибудь примеры.)

1. Взаимодействуют два не доверяюших друг другу абонента. Они хотят подписать контракт. Это надо сделать так, чтобы не допустить следующую ситуацию: один из абонентов получил подпись другого, а сам не подписался.

Протокол решения этой задачи принято называть *протоколом подписания контракта.*

2. Взаимодействуют два не доверяюших друг другу абонента. Они хотят бросить жребий с помощью монеты. Это надо сделать так, чтобы абонент, подбрасывающий монету, не мог изменить результат подбрасывания после получения догадки от абонента, угадывающего этот результат.

Протокол решения этой задачи принято называть *протоколом подбрасывания монеты.*

Опишем один из простейших протоколов подбрасывания монеты по телефону (так называемая схема Блюма-Микали). Для его реализации у абонентов A и B должна быть односторонняя функция $f\colon X \to Y$, удовлетворяющая следующим условиям:

1) X — конечное множество целых чисел, которое содержит одинаковое количество чётных и нечётных чисел;

2) любые числа $x_1, x_2 \in X$, имеющие один образ $f(x_1) = f(x_2)$, имеют одну чётность;

3) по заданному образу $f(x)$ «трудно» вычислить чётность неизвестного аргумента x.

Роль подбрасывания монеты играет случайный и равновероятный выбор элемента $x \in X$, а роль орла и решки — чётность и нечётность x соответственно. Пусть A — абонент, подбрасывающий монету, а B — абонент, угадывающий результат. Протокол состоит из следуюших шагов:

1) A выбирает x («подбрасывает монету»), зашифровывает x, т. е. вычисляет $y = f(x)$, и посылает y абоненту B;

2) B получает y, пытается угадать чётность x и посылает свою догадку абоненту A;

3) A получает догадку от B и сообщает B, угадал ли он, посылая ему выбранное число x;

4) B проверяет, не обманывает ли A, вычисляя значение $f(x)$ и сравнивая его с полученным на втором шаге значением y.

Рекомендуем читателю самостоятельно проверить, что необходимые требования к протоколу подбрасывания монеты выполнены из-за свойств функции f.

3. Взаимодействуют два абонента A и B (типичный пример: A — клиент банка, B — банк). Абонент A хочет доказать абоненту B, что он именно A, а не противник.

Протокол решения этой задачи принято называть *протоколом идентификации абонента.*

4. Взаимодействуют несколько удаленных абонентов, получивших приказы из одного центра. Часть абонентов, включая центр, могут быть противниками. Необходимо выработать единую стратегию действий, выигрышную для абонентов.

Эту задачу принято называть задачей о византийских генералах, а протокол ее решения — *протоколом византийского соглашения.*

Опишем пример, которому эта задача обязана своим названием. Византия. Ночь перед великой битвой. Византийская армия состоит из n легионов, каждый из которых подчиняется своему генералу. Кроме того, у армии есть главнокомандующий, который руководит генералами. Однако империя находится в упадке и до одной трети генералов, включая главнокомандующего, могут быть предателями. В течение ночи каждый из генералов получает от главнокомандующего приказ о действиях на утро, причем возможны два варианта приказа: «атаковать» или «отступать». Если все честные генералы атакуют, то они побеждают. Если все они отступают, то им удаётся сохранить армию. Но если часть из них атакует, а часть отступает, то они терпят поражение. Если главнокомандующий окажется предателем, то он может дать разным генералам разные приказы, поэтому приказы главнокомандующего не стоит выполнять беспрекословно. Если каждый генерал будет действовать независимо от остальных, результаты могут оказаться плачевными. Очевидно, что генералы нуждаются в обмене информацией друг с другом (относительно полученных приказов) с тем, чтобы прийти к соглашению.

Осмысление различных протоколов и методов их построения привело в 1985–1986 г.г. к появлению двух плодотворных математических моделей — *интерактивной системы доказательства* и *доказательства с нулевым разглашением.* Математические исследования этих новых объектов позволили доказать несколько утверждений, весьма полезных при разработке криптографических протоколов (подробнее об этом см. статью Н. П. Варновского в настоящем номере журнала, стр. 71–86).

Под интерактивной системой доказательства (P, V, S) понимают протокол взаимодействия двух абонентов: P (доказывающий) и V (проверяющий). Абонент P хочет доказать V, что утверждение S истинно. При этом абонент V самостоятельно, без помощи P, не может доказать утверждение S (поэтому V и называется проверяющим). Абонент P может быть и противником, который хочет доказать V, что утверждение S истинно, хотя оно ложно. Протокол может состоять из многих *раундов*

обмена сообщениями между P и V и должен удовлетворять двум условиям:

1) *полнота* — если S действительно истинно, то абонент P убедит абонента V признать это;

2) *корректность* — если S ложно, то абонент P вряд ли убедит абонента V, что S истинно.

Здесь словами «вряд ли» мы для простоты заменили точную математическую формулировку.

Подчеркнём, что в определении системы (P, V, S) не допускалось, что V может быть противником. А если V оказался противником, который хочет «выведать» у P какую-нибудь новую полезную для себя информацию об утверждении S? В этом случае P, естественно, может не хотеть, чтобы это случилось в результате работы протокола (P, V, S). Протокол (P, V, S), решающий такую задачу, называется доказательством с нулевым разглашением и должен удовлетворять, кроме условий 1) и 2), ещё и следующему условию:

3) *нулевое разглашение* — в результате работы протокола (P, V, S) абонент V не увеличит свои знания об утверждении S или, другими словами, не сможет извлечь никакой информации о том, почему S истинно.

Заключение

За последние годы криптография и криптографические методы всё шире входят в нашу жизнь и даже быт. Вот несколько примеров. Отправляя Email, мы в некоторых случаях отвечаем на вопрос меню: «Нужен ли режим зашифрования?» Владелец интеллектуальной банковской карточки, обращаясь через терминал к банку, вначале выполняет криптографический протокол аутентификации карточки. Пользователи сети Интернет наверняка знакомы с дискуссиями вокруг возможного принятия стандарта цифровой подписи для тех страниц, которые содержат «критическую » информацию (юридическую, прайс-листы и др.). С недавних пор пользователи сетей стали указывать после своей фамилии наряду с уже привычным «Email ... » и менее привычное — «Отпечаток открытого ключа ... ».

С каждым днем таких примеров становится всё больше. Именно новые практические приложения криптографии и являются одним из источников ее развития. Криптографии, как и любой другой науке, необходимы новые нетривиальные и неожиданные идеи. Автор настоящей статьи надеется, что кто-то из ее читателей станет автором новых идей, а, быть может, и новейших направлений в криптографии.