Основные понятия криптографии

- 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 таких методов «запрятывания» защищаемой информации внутри больших объемов информации, хранящейся в компьютере. Наглядный

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.

ленных 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 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).

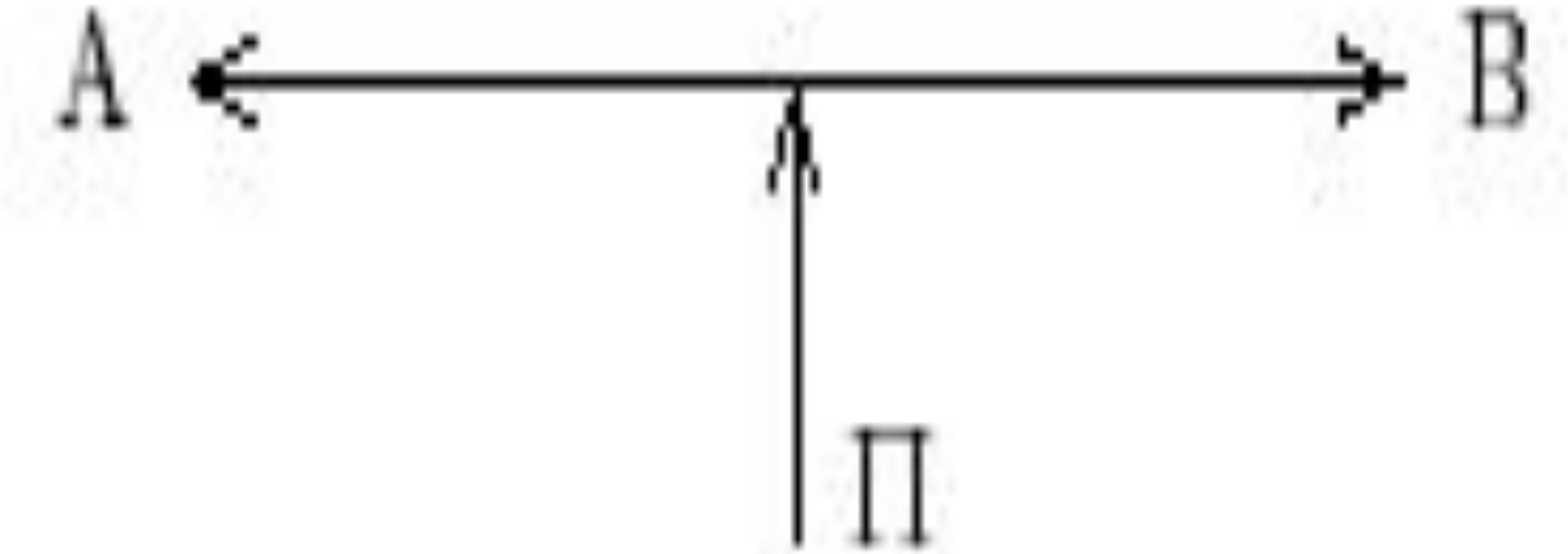

Рис. 1.

- Здесь А и В 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 (военноморские 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 skодирование разновидность шифрованияї 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 (sпринцип равнопрочности защитыї).

- 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 уче ного 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 году1). Имеется перевод этой книги на русский язык (Кан Д. Взломщики кодов. М., Центрполиграф, 2000). Книга Т.А. Соболевой2) 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 sСциталаї). Цезарь использовал в переписке шифр, который вошел в историю как sшифр Цезаряї. В древней Греции был изобретен вид шифра, который в дальнейшем стал называться sквадрат Политияї. 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 (sрешетка Карданої).

- 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 sцифирная азбукаї 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 из вестных рассказах: sЗолотой жукї Э.По и sПляшущие человечкиї А.Конан Дойла.

- Рассмотрим более подробно два примера.
- Шифр sСциталаї. 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 (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 sСциталаї, 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 sяї следует буква saї. 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.

Рис. 2.

- Вернемся к формальному описанию основного объекта криптографии (рис. 1, стр. 11). Теперь в него необходимо внести существенное изменение 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.
- 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.
- 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 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 кибернетикиї 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. . . ї

- Автор шифра PGP Ф. Зиммерманн (sКомпьютерраї, №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. . . ї

- 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.