1. **Роль криптографических протоколов в системах защиты информации**

*Криптографический протокол. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей.*

*Классификация криптографических протоколов. Моделирование криптографических протоколов. Уязвимости и атаки на криптографический протокол. Атаки по сторонним каналам.*

*Аппаратное и программное шифрование.*

*Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Основные подходы к автоматизации анализа протоколов.*

Криптография как наука изучает методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность.

Под конфиденциальностью понимают невозможность получения информации из преобразованного массива без знания дополнительной информации (ключа).

Аутентичность информации состоит в подлинности авторства и целостности.

В XIX в. Керкоффом было сформулировано главное требование к криптографическим системам, актуальное и поныне: *секретность шифров должна быть основана на секретности ключа, а не алгоритма*.

*Протокол* ‑ распределенный алгоритм, в процессе выполнения которого два (или более) участника последовательно выполняют определенные действия и обмениваются сообщениями. Криптографический протокол - протокол, предназначенный для выполнения функций криптографической системы; в процессе его выполнения участники используют криптографические алгоритмы. В данном случае под *криптографической системой* понимают систему обеспечения безопасности информации (как правило конфиденциальности, целостности и авторства) криптографическими методами. В основе выбора и построения криптографических систем лежит условие обеспечения криптографической стойкости. *Криптографическая стойкость* (или криптостойкость) — способность криптографического алгоритма противостоять криптоанализу. Стойким считается алгоритм, атака на который требует от атакующего наличием недостижимым на практике вычислительных ресурсов или перехваченных открытых и зашифрованных сообщений либо огромных затрат времени на расшифровку, что к его моменту защищённая информация потеряет свою актуальность.

Наиболее важные требования к протоколу при передаче сообщений следующие: аутентификация источника данных - получение подтверждения того, что рассматриваемый документ был создан именно указанным источником информации (без установления времени создания и единственности документа); обеспечение целостности данных, т.е. невозможности их модификации после создания. Можно рассматривать как часть задачи аутентификации источника данных. Для реализации современных протоколов с заявленными требованиями успешно применяется схема цифровой подписи сообщения.

*Аутентификация* ‑ установление (проверка и подтверждение) подлинности различных аспектов информационного взаимодействия: сеанса связи, сторон (*идентификация*), содержания (*имитозащита*) и источника (*установление авторства*) передаваемых сообщений, времени взаимодействия и т.д. Является важной составной частью проблемы обеспечения достоверности получаемой информации. Особенно остро эта проблема стоит в случае не доверяющих друг другу сторон, когда источником угроз может служить не только третья сторона (противник), но и сторона, с которой осуществляется информационное взаимодействие.

Виды криптосистем. Криптосистема представляет собой неинтерактивный протокол конфиденциальной передачи сообщений. Имеются два основных типа криптосистем ‑ с секретным и с открытым ключом. Существуют также бесключевые криптосистемы, называемые иногда криптосистемами типа 3.

~~Центральный принцип любой криптосистемы, независимо от используемой методологии ее конструирования, - использование асимметрии. Асимметрия выражается в том, что законный участник криптосистемы обладает некоторой информацией, которая позволяет совершать ему определенные действия; противник же этой информацией не обладает, и для него, таким образом, создаются вычислительные препятствия.~~

~~В криптографии известны три принципиально различных способа реализации асимметрии:~~

1. ~~использование криптографических ключей;~~
2. ~~канал, более надежный для законного пользователя, чем для противника (теоретико-информационные модели);~~
3. ~~вычислительные ресурсы, более мощные, чем у противника.~~

В 1949 г. в работе К. Шеннона «Теория связи в секретных системах» были сформулированы теоретические принципы криптографической защиты информации, обоснована возможность создания сколь угодно стойких криптосистем. Он ввел понятия диффузии и конфузии для описания стойкости алгоритма шифрования.

*Диффузия* – это рассеяние статистических особенностей незашифрованного текста в широком диапазоне статистических особенностей зашифрованного текста. Диффузия достигается тем, что значение каждого элемента незашифрованного текста влияет на значения многих элементов зашифрованного текста или, что то же самое, любой элемент зашифрованного текста зависит от многих элементов незашифрованного текста.

*Конфузия* – это уничтожение статистической взаимосвязи между зашифрованным текстом и ключом.

К. Шеннон обосновал абсолютную стойкость предложенного в 1917 г. Г. Вернамом шифра, в котором размер абсолютно случайного ключа равен или более, чем размер сообщения. Такой шифр также называется *одноразовым шифровальным блокнотом* или *абсолютно стойким шифром*.

Предмет изучения криптографии можно представить в виде многоуровневой схемы (рис. 1.1). Распределение криптографических конструкций по уровням и блокам довольно условно, но тем не менее позволяет выделить несколько основных понятий. Кроме того, следует отметить, что многие направления современной криптографии появились совсем недавно, переживают бурный рост, поэтому в них еще нет устоявшейся терминологии. В каждой области исследований используются свои термины, часто не совпадающие с терминологией из других отраслей науки.

Криптографические примитивы - это отображения самого нижнего уровня, которые могут быть двух типов:

1. перемешивающие, или «инженерные» (в англоязычной терминологии также confusion/dijfusion primitives), например петля Фейстеля, линейный регистр сдвига с обратной связью, SP-сети;
2. алгебраические и комбинаторные примитивы, например функция дискретного логарифма, функция RSA и др.

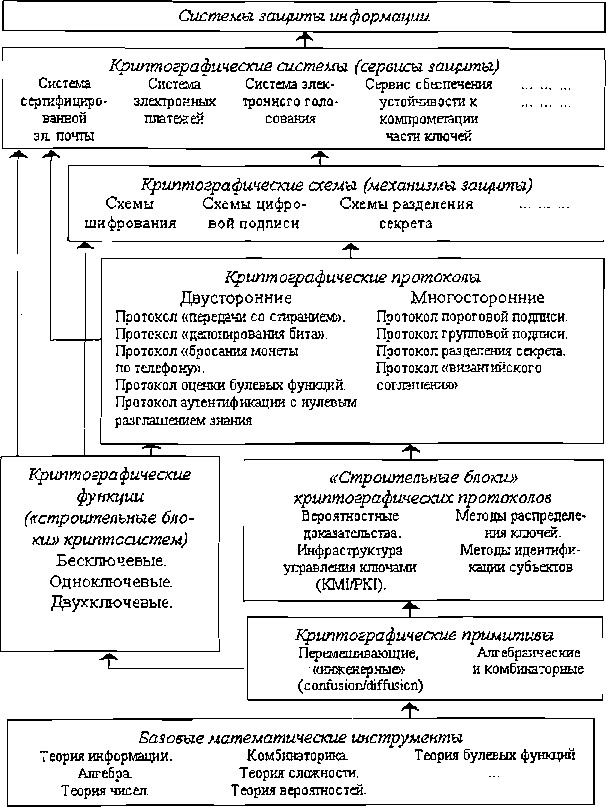
**

Рис. 1.1. Многоуровневая структура криптосистем

Криптографические функции («строительные блоки» криптосистем) ‑ это локальные алгоритмы, которые могут давать результаты, имеющие интерес для криптографии.

«Строительные блоки» криптографических протоколов — это вспомогательные конструкции, которые носят обслуживающий характер по отношению к протоколам, применяемым непосредственно для защиты информации.

Криптографические схемы (механизмы защиты) - это совокупность однородных в функциональном отношении криптографических алгоритмов и(или) протоколов, которые преследуют общие цели защиты. Примерами криптографических схем могут являться:

* схемы шифрования, включающие алгоритм шифрования, алгоритм дешифрования, метод генерации ключей криптосхемы, протокол распределения этих ключей;
* схемы цифровой подписи, включающие алгоритм или протокол генерации цифровой подписи, алгоритм проверки цифровой подписи, способ генерации ключей и протокол распределения ключей;
* схемы разделения секрета, включающие протокол разделения секрета, протокол восстановления секрета, протокол распределения ключей.

Криптографические системы - еще более высокоуровневые конструкции, которые предоставляют готовое решение какой-либо использованы при организации системы защиты информации. Например, услуги могут быть оформлены в виде подсистем, которые вызываются прикладными программами, или же они могут быть встроены в прикладные программы.

Криптографические средства защиты используются для обеспечения следующих свойств: конфиденциальность, целостность, аутентичность, невозможность отказа.

Участники криптографического протокола в общем случае подразделяются на две группы:

1. непосредственно решающие задачу протокола (как правило, обозначаются буквами латинского алфавита А, В, С, D... либо символическими именами Алиса, Боб, Ева и т. п.);
2. обслуживающие участников первой группы: арбитр, третейский судья, дилер, центр доверия, центр распределения ключей и др.

В зависимости от количества участников, принадлежащих к первой группе, протоколы делятся на *двусторонние* и *многосторонние*. Таких участников, в свою очередь, можно подразделить на честных (honest) и нечестных (dishonest). В числе последних отмечают умышленно мешающих честным решать задачу протокола, т.е. противников, или злоумышленников, и неумышленно нечестных, допускающих непреднамеренные ошибки. Вместе с тем на практике бывает весьма трудно достоверно определить, преднамеренным или случайным является отклонение того или иного лица от предписанных протоколом действий. В связи с этим обычной практикой является принятие более сильного предположения о том, что в протоколе действует злоумышленник, и конструирование протокола в расчете именно на реализацию этой угрозы. Противник в разных задачах может иметь различные возможности: взаимодействовать с абонентами от имени других, вмешиваться в обмен информацией, противником может быть один из абонентов или несколько, вступивших в сговор.

По способу вторжения в протокол противник может быть пассивным (eavesdropper) или активным (active adversary). Пассивный обычно обозначается буквой Е (Eva). Он может только прослушивать каналы связи и выборочно или полностью сохранять информацию, передаваемую по этим каналам. Активный, который чаще всего обозначается буквой М (Mallory), может вставлять, модифицировать, удалять сообщения из каналов связи и даже (иногда рассматривают и такую модель) овладевать частью секретных ключей участников протокола.

*Рассмотрим* основные виды атак на криптографические протоколы.

1. Атака по известным ключам (known key attack) - в этой атаке противник обладает некоторыми ключами, использованными в предыдущих сеансах протокола, и затем применяет эту информацию для определения новых ключей в последующих сеансах, например выявляет закон изменения ключей.
2. Атака методом повтора сеанса (replay attack) - в этой атаке противник полностью или фрагментарно записывает сеанс протокола и повторно применяет эти сообщения в следующем сеансе, т. е. «повторно играет» (отсюда название «replay») сеанс или его часть в некоторый более поздний момент времени.
3. Атака методом деперсонификации (impersonation) - противник принимает на себя идентичность одного из законных участников протокола.
4. Словарная атака (dictionary attack) - атака путем перебора наиболее вероятных значений каких-либо величин или сообщений, используемых в протоколе (например, путем перебора паролей, в качестве которых довольно часто берутся легко угадываемые данные: фамилия, имя, отчество, номер телефона, адрес и т. п.).
5. Атака методом опережающего поиска (fonvard search attack) - по принципу осуществления похожа на словарную, но реализуется путем полного перебора всех возможных значений какой- либо величины и используется, как правило, для расшифрования сообщений. Например, банком выполняется транзакция, в которой величина транзакции, зашифрованная схемой открытого шифрования, указана в 32-битовом поле. Противник, используя природу схемы открытого шифрования, может взять 232 возможных открытых текстов и зашифровать их. Каждый из 232 шифртекстов сравнивается с наблюдаемой противником величиной транзакции, и определяется соответствующий ей открытый текст.
6. Атака методом включения в канал (interleaving attack) - противник М «врезается» в канал связи между законными участниками А и В таким образом, что для А создается иллюзия того, что он взаимодействует с В, и наоборот, а на самом деле каждый из взаимодействует с М, который «пропускает через себя» все проходящие сообщения и может их модифицировать, задерживать, менять местами и т. п. Очевидно, что в этой атаке противник должен быть активным.

Компрометация протокола ~ это ситуация, когда протокол не способен достичь тех целей, для которых он был предназначен, причем противник получает преимущество без непосредственного «вскрытия» нижележащих примитивов или алгоритмов, а только путем манипуляции протоколом.

В отдельный вид атак можно выделить *атаки по сторонним каналам (side channel attacks)*, когда для достижения целей используются уязвимости в реализации криптографических методов защиты. Например, атака по энергопотреблению на RSA. Известные типы атак по сторонним каналам:

‑ атака зондированием (probing attack);

‑ атака по времени (timing attack);

‑ атака по ошибкам вычислений (fault-induction attack);

‑ атаки по энергопотреблению (power analysis attack);

‑ атаки по электромагнитному излучению (electromagnetic analysis attacks);

‑ акустическая атака (acoustic attack);

‑ атака по видимому излучению (visible light attack).

Для предотвращения таких атак используются аппаратные способы защиты: экранирование, зашумление, уравнивание времени выполнения операций, балансировка энергопотребления, устранение условных переходов, независимость вычислений от данных.

Криптографические алгоритмы могут реализоваться как аппаратно, так и программно.

Аппаратное шифрование. Существует специальное оборудование для реализации аппаратного шифрования. Оно преобладает над программным, что обусловлено такими его достоинствами, как высокая скорость шифрования, лучшая защищенность аппаратуры от проникновения извне по сравнению с программное обеспечением на компьютере и простота установки шифровальной аппаратуры.

Шифровальная аппаратура представлена самодостаточными модулями, самостоятельно выполняющими все операции с ключами и блоками шифрования для каналов связи, и шифровальными платами для установки в компьютере.

Программное шифрование. Программное обеспечение для такого шифрования легко копируется и модифицируется, просто в использовании. Во всех операционных системах имеются встроенные средства шифрования файлов. Однако работа с ключами полностью выполняется пользователем. Эффективность шифрования повышается, если использовать сжатие перед шифрованием.

Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации.

Алгоритмы шифрования в зависимости от симметричности процессов шифрования и дешифрования делят на симметричные (иногда называют алгоритмами с секретным ключом) и асимметричные (часто называют алгоритмами с открытым ключом).

Алгоритмы шифрования, в которых для шифрования и дешифрования используется один и тот же ключ, а процесс дешифрования обратен процессу шифрования, называются *симметричными*. Они бывают *поточными* (получают сложением открытого потока информации с некоторой псевдослучайной последовательностью) и *блочными* (текст сначала разбивается на блоки длиной m (64, 128, 256 битов и т.д.), над которыми выполняются операции шифрования).

Одни из первых симметричных блочных алгоритмов, реализуемых на мощных и компактных вычислительных средствах, были построены на основе сетей Фейстела[[1]](#footnote-1) (DES, TripleDES, AES, Blowfish, RC6, IDEA, ГОСТ 28147‑89 и др.), все они имеют плоское пространство ключей, с возможным исключением нескольких слабых ключей. Первым в 1978 г. официально был принят американский стандарт шифрования DES (Data Encryption Standard).

В большинстве распространенных алгоритмов симметричного шифрования размер зашифрованного текста всегда равен размеру открытого текста.

Однако серьезной проблемой для симметричных алгоритмаовшифрования осталась передача секретного ключа для шифрования. Также к недостаткам симметричных алгоритмов относится рост пространства ключей с увеличением количества участников обмена. Достоинствами симметричных алгоритмов по сравнению с асимметричными являются: легкость аппаратной реализации, скорость шифрования.

Поточные алгоритмы хорошо себя зарекомендовали при использовании в потоковой передаче информации (поточное видео, аудио и видеосвязь), так как искажение отдельных битов не оказывает существенного влияния на прием и правильное дешифрование сообщения, внося в него только искажения. Однако их использование требует предварительной синхронизации источника и приемника.

Суть криптографических *алгоритмов с открытым ключом (асимметричных)* заключается в том, что адресатом генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым (или публичным), а другой – секретным (или личным). Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне. Исходное сообщение шифруется открытым ключом адресата и передается ему. Дешифрование сообщения возможно только с использованием личного ключа, который известен только самому адресату.

Стойкость криптографических алгоритмов с открытым ключом базируется на гипотезе о вычислительной невозможности эффективного решения некоторых математических задач. Например стойкость криптосистемы RSA базируется на сложности задачи факторизации больших чисел, а стойкость алгоритма Эль-Гамаля – на сложности задачи логарифмирования в конечных полях

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах и используются для следующих целей:

1 Защиты передаваемых и хранимых данных.

2 Распределения ключей. Алгоритмы с открытым ключом более трудоемки, чем симметричные криптосистемы. Поэтому часто на практике рациональней их использовать для распределения ключей симметричного шифрования.

3 Аутентификации пользователей.

Среди недостатков криптографических алгоритмов с открытым ключом следует упомянуть:

1 Незначительное количество рабочих схем систем с открытым ключом. Так как в основе каждого алгоритма лежит теоретически не решаемая за разумное время математическая задача, то количество алгоритмов шифрования с открытым ключом ограничено количеством таких задач в отличие от алгоритмов симметричного шифрования, для которых можно создать множество рабочих схем комбинированием большого количества элементарных операций.

2 Потенциальная ненадежность криптографических систем с открытым ключом вследствие гипотезы о трудоемком решении математической задачи, на основе которой они построены.

3 Увеличение размера ключа приводит к усложнению аппаратной реализации криптографической системы.

Один из способов повышения стойкости криптографических алгоритмов –представление блоков информации при шифровании не только в виде чисел (или элементов конечных полей), но и в виде иных алгебраических объектов большей сложности, например точек эллиптических кривых.

1. Хорст Фейстел – сотрудник IBM, один из авторов американского стандарта шифрования DES. Описал модель построения блочных шифров для создания стойких симметричных блочных криптосистем. [↑](#footnote-ref-1)