8. Основные модели криптосистем. Требования к криптосистемам. назначение и основные функции криптосистем

О важности сохранения информации в тайне знали уже в древние времена, когда с появлением письменности появилась и опасность прочтения ее нежелательными лицами. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. С широким распространением письменности криптография стала формироваться как самостоятельная наука.

Точное время возникновения этих способов обмена тайной информацией теряется в глубине веков, и установить его невозможно. Историки полагают, что первые протокриптографические приемы появились в Древнем Египте около 4 тыс. лет назад. Писцы, составлявшие жизнеописания правителей, стремились придать стандартным иероглифам необычный вид на монументах и гробницах, чтобы сообщить надписям менее обыденный и более почтительный стиль. Жрецы пользовались этим же приемом при переписывании религиозных текстов, чтобы те выглядели для мирян загадочнее и внушительнее. Такие «переводы» становились все менее понятными простому люду, который в результате оказывался во все большей зависимости от жрецов.

По мере развития египетской цивилизации ширилось использование иероглифов. С увеличением количества надписей, высекавшихся на стенах храмов, люди теряли к ним интерес. Египтологи считают, что писцы тогда стали еще больше видоизменять некоторые знаки в стремлении пробудить любопытство и привлечь внимание населения.

Эти модификации никоим образом не были кодами или шифрами, но они заключали в себе два основных принципа криптологии, а именно: изменение письма и сокрытие его смысла.

Примерно с 500 г. до н. э. в Индии также широко применялись секретные записи, в частности в донесениях шпионов и текстах, предположительно использовавшихся Буддой.

Методы засекречивания включали в себя фонетическую замену, когда согласные и гласные менялись местами, использование перевернутых букв и запись текста под случайными углами. Существуют проблемы тайной передачи информации и ее сокрытия от злоумышленника на расстоянии.

Путей ее решения существует множество, среди которых можно выделить три основных направления:

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 таком преобразованном виде, чтобы восстановить ее мог только адресат.

Проанализируем эти возможности:

1. С древних времен практиковалась охрана документа (носителя информации) физическими лицами, передача его специальным курьером (человеком (дипломатом) или животным (голубиная почта)) и т.д. Но, документ можно выкрасть, курьера можно перехватить, подкупить, в конце концов, убить. В настоящий момент для реализации данного механизма защиты используются современные телекоммуникационные каналы связи. Однако следует заметить, что данный подход требует значительных капитальных вложений. При современном уровне развития науки и техники сделать такой канал связи между удаленными абонентами для многократной 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. Так, в трудах древнегреческого историка Геродота встречается описание двух методов сокрытия информации: на обритую голову раба записывалось необходимое сообщение, а когда его волосы отрастали, он отправлялся к адресату, который вновь брил его голову и считывал доставленное сообщение. Второй способ заключался в следующем: сообщение наносилось на деревянную дощечку, а потом она покрывалась воском, и, тем

самым, не вызывала никаких подозрений. Потом воск соскабливался, и сообщение становилось видимым. В настоящий момент стенографические методы в совокупности с криптографическими нашли широкое применение в целях сокрытия и передачи конфиденциальной информации.

3. Разработкой методов преобразования информации с целью ее защиты от несанкционированного прочтения занимается криптография.

В истории развития криптографии можно выделить три этапа:

- наивная криптография;
- формальная криптография;
- математическая криптография.

Наивная криптография

Для наивной криптографии (до начала XVI в.) характерно использование любых, обычно примитивных, способов запутывания противника относительно содержания передаваемых сообщений.

На начальном этапе для защиты информации использовались методы кодирования и стеганографии, которые родственны, но не тождественны криптографии. Шифровальные системы сводились к использованию перестановки или замены букв на различные символы (другие буквы, знаки, рисунки, числа и т.п.).

Одни и те же способы шифрования использовались повторно, ключи были короткими, использовались примитивные способы преобразования исходной информации в зашифрованное сообщение. Это позволяло, однажды установив алгоритм шифрования, быстро расшифровывать сообщения.

Одним из первых зафиксированных примеров является **шифр Цезаря.**

Другой шифр, **полибианский квадрат**, авторство которого приписывается греческому писателю Полибию, является шифром простой однозначной замены.

С VIII века н. э. развитие криптографии происходит в основном в арабских странах. Считается, что арабский филолог Халиль аль-Фарахиди первым обратил внимание на возможность использования стандартных фраз открытого текста для дешифрования.

Он предположил, что первыми словами в письме на греческом языке византийскому императору будут «Во имя Аллаха», что позволило ему прочитать оставшуюся часть сообщения. Позже он написал книгу с описанием данного метода — «Китаб аль-Муамма» («Книга тайного языка»).

В 855 г. выходит «Книга о большом стремлении человека разгадать загадки древней письменности» арабского учёного Абу Бакр Ахмед ибн Али Ибн Вахшия ан-Набати, одна из первых книг о криптографии с описаниями нескольких шифров, в том числе с применением нескольких алфавитов.

В древние времена широкое применение нашли различные простейшие криптографические устройства.

Греческим поэтом Архилохом, жившим в VII веке до н. э. упоминается устройство под названием **сцитАла** (греч. - жезл). Оно представляет собой цилиндр (иногда жезл командующего) и узкую полоску пергамента, обматывавшуюся вокруг него по спирали, на которой в свою очередь писалось сообщение.

Шифруемый текст писался на пергаментной ленте по длине палочки, после того как длина палочки оказывалась исчерпанной, она поворачивалась и текст писался далее, пока либо не заканчивался текст, либо не исписывалась вся пергаментная лента. В последнем случае использовался очередной кусок пергаментной ленты.

Для расшифровки адресат использовал палочку такого же диаметра, на которую он наматывал пергамент, чтобы прочитать сообщение. Античные греки и спартанцы в частности, использовали этот шифр для связи во время военных кампаний. Однако такой шифр может быть легко взломан.

Например, метод взлома сциталы был предложен ещё Аристотелем. Он состоит в том, что, не зная точного диаметра палочки, можно использовать конус, имеющий переменный диаметр и перемещать пергамент с сообщением по его длине до тех пор, пока текст не начнёт

читаться - таким образом дешифруется диаметр сциталы.

Другим широко известным криптографическим устройством защиты информации был **«диск Энея»** - инструмент для защиты информации, придуманный Энеем Тактиком в IV веке до н. э. Устройство представляло собой диск диаметром 13-15 см и толщиной 1-2 см с проделанными в нём отверстиями, количество которых равнялось числу букв в алфавите. Каждому отверстию ставилась в соответствие конкретная буква. В центре диска находилась катушка с намотанной на неё ниткой.

Механизм шифрования был очень прост. Для того, чтобы зашифровать послание, необходимо было поочерёдно протягивать свободный конец нити через отверстия обозначающие буквы исходного не зашифрованного сообщения. В итоге, сам диск, с продетой в его отверстия ниткой, и являлся зашифрованным посланием.

Получатель сообщения последовательно вытягивал нить из каждого отверстия, тем самым получал последовательность букв. Но эта последовательность являлась обратной по отношению к исходному сообщению, то есть он читал сообщение наоборот. Зашифрованное сообщение было доступно к прочтению любому, кто смог завладеть диском. Так как сообщение предавали обычные гонцы, а не воины, Эней предусмотрел возможность быстрого уничтожения передаваемой информации. Для этого было достаточно вытянуть всю нить за один из её концов, либо сломать диск, просто наступив на него.

На самом деле «диск Энея» нельзя назвать настоящим криптографическим инструментом, поскольку прочитать сообщение мог любой желающий. Но это устройство стало прародителем первого по истине криптографического инструмента, изобретение которого также принадлежит Энею.

Формальная криптография

Этап формальной криптографии (конец XV – начало XX вв.) связан с появлением формализованных и относительно стойких к ручному крипто анализу шифров.

Отцом западной криптографии называют учёного эпохи Возрождения Леона Баттисту Альберти.

Изучив методы вскрытия использовавшихся в Европе моно алфавитных шифров (шифров однозначной замены), он попытался создать шифр, который был бы устойчив к частотному крипто анализу. Он предложил вместо единственного секретного алфавита, как в моно алфавитных шифрах, использовать два или более, переключаясь между ними по какому-либо правилу.

Однако флорентийский учёный так и не смог оформить своё открытие в полную работающую систему, что было сделано уже его последователями (Блез Вижинер).

В 1550 г. итальянский математик Джероламо Кардано, состоящий на службе у папы римского, предложил новую технику шифрования - решётку Кардано.

Значительный толчок криптографии дало изобретение телеграфа. Сама передача данных перестала быть секретной, и сообщение, в теории, мог перехватить кто угодно. Интерес к криптографии возрос, в том числе, и среди простого населения, в результате чего многие попытались создать индивидуальные системы шифрования.

Преимущество телеграфа было явным и на поле боя, где командующий должен был отдавать немедленные приказы на поле сражения, а также получать информацию с мест событий. Это послужило толчком к развитию полевых шифров.

В 1883 г. голландец Огюст Керкгоффс2 опубликовал труд под названием «Военная криптография» (фр. «La Cryptographie Militaire»). В нём он описал шесть требований, которым должна удовлетворять защищённая система. Хотя к некоторым из них стоит относиться с подозрением, стоит отметить труд за саму попытку:

1. шифр должен быть физически, если не математически, невскрываемым;
2. система не должна требовать секретности, на случай, если она попадёт в руки врага;
3. ключ должен быть простым, храниться в памяти без записи на бумаге, а также легко изменяемым по желанию корреспондентов;
4. зашифрованный текст должен (без проблем) передаваться по телеграфу;
5. аппарат для шифрования должен быть легко переносимым, работа с ним не должна

требовать помощи нескольких лиц;
6. аппарат для шифрования должен быть относительно прост в использовании, не требовать значительных умственных усилий или соблюдения большого количества правил.

Им же был сформулирован известный **«принцип Керкгоффса»** - правило разработки криптографических систем, согласно которому в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен быть открытым.

Другими словами, при оценке надёжности шифрования необходимо предполагать, что противник знает об используемой системе шифрования всё, кроме применяемых ключей.

Математическая криптография

После Первой мировой войны правительства стран засекретили все работы в области криптографии. К началу 1930-х годов окончательно сформировались разделы математики, являющиеся основой для будущей науки: общая алгебра, теория чисел, теория вероятностей и математическая статистика. К концу 1940-х годов построены первые программируемые счётные машины, заложены основы теории алгоритмов, кибернетики.

Тем не менее, в период после Первой мировой войны и до конца 1940-х годов в открытой печати было опубликовано совсем немного работ и монографий, но и те отражали далеко не самое актуальное состояние дел. Наибольший прогресс в криптографии достигается в военных ведомствах.

В 1960-х годах начали появляться различные блочные шифры, которые обладали большей крипто стойкостью по сравнению с результатом работы роторных машин. Однако они предполагали обязательное использование цифровых электронных устройств - ручные или полумеханические способы шифрования уже не использовались.

Примерно в это же время Хорст Фейстель переходит из Военно-воздушных сил США на работу в лабораторию корпорации IBM. Там он занимается разработкой новых методов в криптографии и разрабатывает ячейку Фейстеля, являющуюся основой многих современных шифров, в том числе шифра Lucifer, ставшего прообразом шифра DES – бывшего стандарта шифрования США, первого в мире открытого государственного стандарта на шифрование данных. На основе ячейки Фейстеля были созданы и другие блочные шифры, в том числе TEA (1994 г.), Twofish (1998 г.), IDEA (2000 г.), а также ГОСТ 28147-89, являющийся стандартом шифрования в России.

В 1976 г. публикуется работа Уитфилда Диффи и Мартина Хеллмана «Новые направления в криптографии» (англ. «New Directions in Cryptography»). Данная работа открыла новую область в криптографии, теперь известную как криптография с открытым ключом. Также в работе содержалось описание алгоритма Диффи - Хеллмана - Меркла, позволявшего сторонам сгенерировать общий секретный ключ, используя открытый канал связи.

Чарльз Беннет (Charles Bennet) и Жиль Брассард (Gilles Brassard), опираясь на работу Стивена Уиснера (Stephen Wiesner), разработали теорию квантовой криптографии, которая базируется скорее на квантовой физике, нежели на математике.

Применение криптографии в решении вопросов аутентификации, целостности данных, передачи конфиденциальной информации по каналам связи и т.п. стало неотъемлемым атрибутом информационных систем.

В современном мире криптография находит множество различных применений - она используется в сотовой связи, платном цифровом телевидении, при подключении к Wi-Fi, для защиты билетов от подделок на транспорте, в банковских операциях, в системах электронных платежей и т.д.

Современные методы использования криптографии

Появление доступного интернета перевело криптографию на новый уровень. Криптографические методы стали широко использоваться частными лицами в электронных коммерческих операциях, телекоммуникациях и многих других средах. Первая получила особенную популярность и привела к появлению новой, не контролируемой государством

валюты — биткойна.

Многие энтузиасты быстро смекнули, что банковский перевод — штука, конечно, удобная, однако, для покупки таких приятных в быту вещей, он не подходит. Не подходит он и при запущенных случаях паранойи, ибо требует от получателя и отправителя обязательной аутентификации.

В 2009 году Сатоши Накамото разработал платежную систему нового типа — BitCoin. Так родилась криптовалюта. Ее транзакции не требуют посредника в виде банка или другой финансовой организации, отследить их невозможно. Сеть полностью децентрализована, биткойны не могут быть заморожены или изъяты, они полностью защищены от государственного контроля. В то же время биткойн может использоваться для оплаты любых товаров — при условии согласия продавца.

Новые электронные деньги производят сами пользователи, предоставляющие вычислительные мощности своих машин для работы всей системы BitCoin.

Такой род деятельности называется **майнинг (mining — добыча полезных ископаемых**). Заниматься майнингом в одиночку не очень выгодно, гораздо проще воспользоваться специальными серверами — пулами. Они объединяют ресурсы нескольких участников в одну сеть, а затем распределяют полученную прибыль.

Крупнейшей площадкой купли-продажи биткойнов является японская Mt. Gox, через которую проводятся 67% транзакций в мире. Заядлые анонимы предпочитают ей российскую BTC-E: регистрация здесь не требует идентификации пользователя. Курс криптовалюты довольно-таки нестабилен и определяется только балансом спроса и предложения в мире.

Предостережением новичкам может служить известная история о том, как 10 тысяч единиц, потраченых одним из пользователей на пиццу, превратились через некоторое время в 2,5 миллиона долларов.

Криптология разделяется на два направления – криптографию и криптоанализ.

Криптография– наука, изучающая методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность.

Современная криптография включает в себя четыре крупных раздела:

- симметричные криптосистемы;
- криптосистемы с открытым ключом;
- системы электронной подписи;
- управление ключами.

Основные направления использования криптографических методов – передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Виды шифров

По типу преобразований шифры можно разделить на следующие группы:

- шифры замены (подстановки);
- шифры перестановки;
- шифры гаммирования;
- шифры на основе аналитических преобразований.

При этом надо учитывать, что некоторые современные шифры совместно используют преобразования различных типов.

Шифры замены (подстановки): преобразование заключается в том, что символы шифруемого текста заменяются символами того или иного алфавита (алфавита криптограммы) в соответствии с заранее обусловленной схемой замены.

Подстановки разделяются на одноалфавитные и многоалфавитные.

В первом случае, определенному символу алфавита исходного сообщения всегда ставится в соответствие один и тот же символ алфавита криптограммы. Один из наиболее известных шифров данного класса – шифр Цезаря. К достоинству таких шифров относится простота преобразования. Но они легко взламываются путем сравнения частоты появления

различных символов в естественном языке и криптограмме.

При использовании многоалфавитных подстановок, учитываются дополнительные параметры (например, положение преобразуемого символа в тексте) и в зависимости от них символ исходного алфавита может заменяться на один из нескольких символов алфавита шифртекста. Например, нечетные символы сообщения заменяются по одному правилу, четные – по-другому.

Шифры перестановок: шифрование заключается в том, что символы исходного текста переставляются по определенному правилу в пределах блока этого текста. При достаточной длине блока и сложном, неповторяющемся порядке перестановки, можно достичь приемлемой стойкости шифра.

Шифрование гаммированием заключается в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, называемой гаммой шифра или ключевой гаммой.

Стойкость шифрования определяется длиной (периодом) неповторяющейся части гаммы шифра, а также сложностью предугадывания следующих элементов гаммы по предыдущим.

Шифрование аналитическими преобразованиями подразумевает использование аналитического правила (формулы) по которому преобразуется текст.

По типу использования ключей шифры делятся на:

- симметричные, использующие для шифрования и расшифровывания информации один и тот же ключ;
- асимметричные, использующие для шифрования и расшифровывания два различных ключа.

По размеру преобразуемого блока шифры делятся на блочные и потоковые.

Блочные шифры осуществляют преобразование информации блоками фиксированной длины. Если длина шифруемого сообщения некратна размеру блока, то его добавляют до нужной длины последовательностью специального вида. Например, это может быть последовательность 100…0. После расшифровки, последний блок просматривают справа налево и отбрасывают «хвост» до первой единицы включительно. Чтобы подобное дополнение было применимо во всех случаях, если сообщение кратно длине блока, в его конец надо добавить целый блок указанного вида.

Потоковые шифры предназначены для преобразования сообщения поэлементно (элементом может быть бит, символ и т. п.). Примером такого вида шифров являются шифры гаммирования.

В качестве информации, подлежащей шифрованию и расшифрованию, а также электронной подписи будут рассматриваться тексты, построенные на некотором алфавите.

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст – упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных информационных системах, можно привести следующие:

- алфавит Z33 – 32 буквы русского алфавита (исключая «ё») и пробел;
- алфавит Z256 – символы, входящие в стандартные коды ASCII и КОИ-8;
- двоичный алфавит – Z2 = {0,1};
- восьмеричный или шестнадцатеричный алфавиты.

Зашифрование – процесс преобразования открытых данных в зашифрованные при помощи шифра. Вместо термина «открытые данные» часто употребляются термины «открытый текст» и «исходный текст», а вместо термина «зашифрованные данные» – «шифрованный текст».

Расшифрование – процесс, обратный зашифрованию, т.е. процесс преобразования зашифрованных данных в открытые при помощи ключа. В некоторых отечественных источниках отдельно выделяют термин дешифрование, подразумевая под этим восстановление исходного текста на основе шифрованного без знания ключа, т.е. методами

криптоанализа. В дальнейшем будем считать расшифрование и дешифрование синонимами. Криптографическая система, или шифр, представляет собой семейство T обратимых преобразований открытого текста в шифрованный. Участники этого семейства индексируются или обозначаются символом k; параметр k обычно называется ключом. Преобразование Tk определяется соответствующим алгоритмом и значением ключа k.

Ключ – конкретное значение некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из семейства. Секретность ключа должна обеспечивать невозможность восстановления исходного текста по шифрованному.

Пространство ключей K – набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита. Следует отличать понятия «ключ» и «пароль». Пароль также является секретной последовательностью букв алфавита, однако используется не для шифрования (как ключ), а для идентификации субъектов.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Требования к криптографическим системам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

1. Знание алгоритма шифрования не должно снижать криптостойкости шифра.
2. Зашифрованное сообщение должно поддаваться чтению только при наличии ключа.
3. Шифр должен быть стойким даже в случае, если нарушителю известно достаточно большое количество исходных данных и соответствующих им зашифрованных данных.
4. Число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и должно либо выходить за пределы возможностей современных компьютеров, либо требовать создания использования дорогих вычислительных систем.
5. Незначительное изменение ключа или исходного текста должно приводить к существенному изменению вида зашифрованного текста.
6. Структурные элементы алгоритма шифрования должны быть неизменными.
7. Длина шифрованного текста должна быть равной длине исходного текста.
8. Дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте.
9. Не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования.
10. Любой ключ из множества возможных должен обеспечивать надежную защиту информации.

Главным действующим лицом в криптоанализе выступает нарушитель (или криптоаналитик) – лицо или группа лиц, целью которых является прочтение или подделка защищенных криптографическими методами сообщений.

Криптоанализ — наука о методах получения исходного значения зашифрованной информации, не имея доступа к секретной информации (ключу), необходимой для этого.

В отношении нарушителя принимается ряд допущений, которые, как правило, лежат в основе математических или иных моделей:

- Нарушитель знает алгоритм шифрования (или электронную цифровую подпись (ЭЦП)) и особенности его реализации в конкретном случае, но не знает ключа.
- Нарушителю доступны все зашифрованные тексты. Нарушитель может иметь доступ к

некоторым исходным текстам, для которых известен соответствующий им зашифрованный текст.

- Нарушитель имеет в своем распоряжении вычислительные, людские, временные и иные ресурсы, объем которых оправдывает потенциальную ценность информации, которая будет добыта в результате криптоанализа.

При анализе криптостойкости шифра необходимо учитывать и человеческий фактор, например, подкуп конкретного человека, в руках которого сосредоточена необходимая информация, может стоить на несколько порядков дешевле, чем создание суперкомпьютера для взлома шифра.

Попытка прочтения или подделки зашифрованного сообщения, вычисления ключа методами криптоанализа называется криптоатакой, или атакой на шифр. Удачную криптоатаку называют взломом.

Принято различать несколько уровней криптоатаки в зависимости от объема информации, доступной криптоаналитику. По нарастанию сложности можно выделить три уровня криптоатаки.

- **Атака на шифрованный текст (уровень КА1)** – нарушителю доступны все или некоторые зашифрованные сообщения.
- **Атака на пару «исходный текст – шифрованный текст» (уровень КА2)** – нарушителю доступны все или некоторые зашифрованные сообщения и соответствующие им исходные сообщения.
- **Атака на выбранную пару «исходный текст – шифрованный текст» (уровень КА3)** – нарушитель имеет возможность выбирать исходный текст, получать для него шифрованный текст и на основе анализа зависимостей между ними вычислять ключ.

Все современные криптосистемы обладают достаточной стойкостью даже к атакам уровня КА3, т.е. когда нарушителю доступно, по сути, шифрующее устройство.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к расшифрованию без знания ключа (т.е. криптоатаке).

Показатель криптостойкости – главный параметр любой криптосистемы.

В качестве показателя криптостойкости можно выбрать:

- количество всех возможных ключей или вероятность подбора ключа за заданное время с заданными ресурсами;
- количество операций или время (с заданными ресурсами), необходимое для взлома шифра с заданной вероятностью;
- стоимость вычисления ключевой информации или исходного текста.

Все эти показатели должны учитывать также уровень возможной криптоатаки. Однако следует понимать, что эффективность защиты информации криптографическими методами зависит не только от криптостойкости шифра, но и от множества других факторов, включая вопросы реализации криптосистем в виде устройств или программ.