Криптография

Широкое использование информационных систем, которые передают и обрабатывают большие объемы информации государственного, военного и коммерческого назначения, требует исключения доступа к ней посторонних лиц.

С другой стороны, современные компьютеры, технологии сетевых вычислений, нейронные сети сделали возможным сделали возможными раскрытие систем шифрования считавшихся ранее нераскрываемыми.

Поэтому в настоящее время использование криптографических методов для защиты информации в информационных системах встала особенно актуально

Проблемой защиты информации путем ее преобразования занимается криптология (греч. kryptos — тайный, logos — наука). В криптологии выделяют два направления:

- криптография (от греч. κρυπτός — скрытый и γράφω — пишу) – наука о математических методах обеспечения конфиденциальности информации;
- криптоанализ – исследование возможности расшифровывания информации без знания ключей.

Как видим, цели этих направлений прямо противоположны.

Криптография – одна из старейших наук. Можно даже утверждать, что письменность изначально была сама по себе криптографической системой, владели которой только избранные.

Широкое распространение письменности способствовало формированию криптографии как отдельной науки. Первые криптосистемы возникли уже в начале нашей эры. Первая и вторая мировая войны способствовали бурному развитию криптографии. Бурное развитие и внедрение в повседневную жизнь информационных систем ускорило разработку и совершенствование криптографических методов.

Основные понятия и методы шифрования изложим на основе Интернет- ресурса http://ru.science.wikia.com/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F

Основные понятия

Сообщение, которое вы хотите передать адресату, будем называть **открытым текстом.** Для сохранения сообщения в тайне оно преобразуется криптографическими методами и только после этого передается адресату. Преобразованное сообщение будем называть шифрованным – **шифртекст**, а сам процесс преобразования - **шифрование**. Параметр определяющим правило шифрование называется **ключом.**

Для удобства дальнейшего изложения введем следующие обозначения: M – открытый текст, C – шифротекст, E – функция шифрования, D – обратная функция функции E.

Таким образом процесс кодирования будет представлен в виде формул:

E(M) = C – шифрование открытого текста M по алгоритму E

D(C) = M – дешифрование шифртекста C по алгоритму D

Используя понятие ключа, процесс зашифрования можно описать в виде соотношения, где K – ключ:

E_K(M) = C

D_K(C) = M

Все многообразие существующих криптографических методов можно свести к следующим классам преобразований:

Моно- и многоалфавитные подстановки Наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

Перестановки Также несложный метод криптографического преобразования. Используется, как правило, в сочетании с другими методами.

Гаммирование Этот метод заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

Блочные шифры Представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем “чистые” преобразования того или иного класса в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе шифров.

Шифр замены

Шифр Цезаря

Историческим примером шифра замены является шифр Цезаря (I век до н.э.), описанный историком Древнего Рима Светонием. Гай Юлий Цезарь в своей переписке использовал шифр собственного изобретения. Применительно к русскому языку он состоял в следующем: каждая буква алфавита заменялась другой буквой, из этого алфавита, идущей за первой через некоторый интервал.

Например:

Выпишем алфавит

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ю Я

И запишем под ним тот же алфавит, но с циклическим сдвигом

Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ю Я А Б В

При шифровании буква А заменялась буквой Г, Б заменялась на Д, и так далее. Так, например, слово «Империя» превращалось в слово «Лптзулв». Получатель сообщения

искал буквы, из которых написано послание, и заменял их на буквы из верхней строки – в этом заключался способ декодирования.

Естественное развитие шифра Цезаря очевидно: нижняя строка двустрочной записи букв алфавита может быть произвольным расположением этих букв. Если в алфавитном расположении букв существует всего 32 варианта (для русского языка, без буквы «ё»), то при произвольном расположении число ключей становиться 33!≈10^35.

Квадрат Полибия

Одним из криптографических изобретений древних греков является так называемы квадрат Полибия (Полибий – греческий государственный деятель, полководец, историк, III век до н.э.). Другое название этого шифра – шифр Плайфера, используемый применительно к английскому языку, мы же будем пользоваться именем Полибия.

Применительно к современному латинскому алфавиту из 26 букв, шифрование заключалось в следующем. В квадрат размером 5x5 клеток выписываются все буквы алфавита, при этом буквы I, J не различаются.

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Шифруемая буква заменялась на координаты квадрата, в котором она записана. Так, B заменялась на AB, F заменялась на BA, R на DB, и т.д. При расшифровании каждая такая пара определяла соответствующую букву сообщения.

Сообщение «THE TABLE», будет иметь вид: DD BC AE DD AA AB CA AE

Заметим, что секретом в данном случае является сам способ замены букв. Ключом является порядок следования букв.

К примеру, квадрат вида

	A	B	C	D	E
A	T	H	E	A	B
B	L	C	D	F	G
C	I	K	M	N	O
D	P	Q	R	S	U
E	V	W	X	Y	Z

зашифрует послание «THE TABLE» следующим образом: AA AB AC AA AD AE BA AC.

Шифр перестановки

Вторым примером исторического шифра является шифр перестановки.

Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые разновидности этого метода, которые могут быть использованы в автоматизированных системах.

Самая простая перестановка — написать исходный текст задом наперед и одновременно разбить шифрограмму на группы из нескольких букв. Пусть группа состоит из пяти букв. Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ.

получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЪ ТСУП

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его дополнить незначащей буквой (например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительные изменения, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Кажется, ничего сложного, но при расшифровке проявляются серьезные неудобства.

Во время Гражданской войны в США в ходу был такой шифр: исходную фразу писали в несколько строк. Например, по пятнадцать букв в каждой (с заполнением последней строки незначащими буквами).

П У С Т Ь Б У Д Е Т Т А К К А

К М Ы Х О Т Е Л И К Л М Н О П

После этого вертикальные столбцы по порядку писали в строку с разбивкой на пятерки букв:

ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП

Если строки укоротить, а количество строк увеличить, то получится прямоугольник-

решетка, в который можно записывать исходный текст. Но тут уже потребуется предварительная договоренность между адресатом и отправителем посланий, поскольку сама решетка может быть различной длины-высоты, записывать к нее можно по строкам, по столбцам, по спирали туда или по спирали обратно, можно писать и подиагоналями, а для шифрования можно брать тоже различные направления. В общем, здесь масса вариантов.

Гаммирование

Гаммирование - представляет собой преобразование исходного текста, при котором символы исходного текста складываются, по модулю, равному количеству символов алфавита из которого составлено сообщение, с символами псевдослучайной последовательности, вырабатываемой по некоторому правилу.

Пусть нам дано некоторое сообщение, состоящее из n символов, включая пробел. Ключом является последовательность из некоторого числа i символов. Под открытый текст подписывается ключ

$i_0 i_1 i_2 ... i_n$

$x_0 x_1 x_2 ... x_n$

Если длина ключа меньше длины сообщения, то ключ периодически повторяется. Каждому знаку открытого текста и ключа ставится в соответствие некоторый вычет по модулю n.

Ключом является символы последовательности Γ_i= ($x_1, x_2, ...x_n$)– ее называют гаммой. А шифртекст получается по правилу y(t)=i_t+x_t(mod n).

Гаммирование чаще осуществляется:

• по модулю 2, если открытый текст представляется в виде бинарной последовательности;

• по модулю 256, если открытый текст представляется в виде последовательности байтов;

• по модулю 10, если открытый текст последовательность цифр.

Какие же требования должны быть предъявлены, чтобы обеспечить достаточное качество шифра?

1. Необходимо, чтобы период повторения генерируемой гаммы был достаточно большим, лучше – максимально возможным. По крайней мере, он должен превосходить наибольшее возможное количество символов в шифруемом сообщении.

2. Необходимо, чтобы соседние или близкие по расположению элементы последовательности $\{\Gamma_i\}$ отличались друг от друга. Было бы крайне желательно, чтобы различия между ними были в каждом позиции.

Смысл в том, что метод гаммирования по своей сути требует одноразовой гаммы, иначе он легко вскрывается по алгоритмической линии. Если же период повторения вырабатываемой гаммы недостаточно велик, различные части одного и того же длинного сообщения могут оказаться зашифрованными с помощью одинаковых участков гаммы. Второе требование является менее очевидным, и, вообще говоря, имеет место только для шифров вполне определенных архитектур, в которых шаг шифрования является комбинацией нескольких сравнительно простых преобразований, в ходе каждого из которых различия в шифруемых блоках данных увеличиваются весьма незначительно.

Блочные шифры

Блочный шифр представляют собой последовательность, с возможным повторением и чередованием, основных методов преобразования, применяемую к блоку шифруемого текста. Другими словами блочный шифр - шифр работающий с блоками конечной длины исходного сообщения.

Исходное сообщение разбивается на блоки длины n, и с каждым блоком производятся операции шифрования, после чего блоки объединяют в один – шифртекст. Таким образом, криптостойкость блочного шифра есть произведение криптостойкости шифров входящих в алгоритм кодирования блока.

Алгоритм блочного шифрования

Блочные шифры на практике встречаются чаще, чем «чистые»преобразования того или иного класса в силу их более высокойкриптостойкости. Еще важной особенностью блочных шифров является параллельная обработка данных, что дает более высокую скорость шифрования. Российский и американский стандарты шифрования основаны именно на этом классе шифров.

Машинные методы шифрования

В криптографии, всегда использовались всевозможные устройства, как для облегчения кодирования сообщения, так и повышения стойкости шифра.

Одним из самых известных устройств являются роторные машины.

Самым известным роторным устройством является «Энигма» (Enigma). Энигма использовалась немцами во Второй Мировой Войне. Сама идея пришла в голову Артуру Шербиусу (Arthur Scherbius) и Арвиду Даму (Arvid Gerhard Damm) в Европе. В США она

была запатентована Артуром Шербиусом. Немцы значительное усовершенствовали базовый проект для использования во время войны [3].

Рассмотрим работу 4-роторной «Энигмы». 4 ротора – 4 вращающихся на одной оси барабана – диска.

На каждой стороне диска по окружности располагалось 25 электрических контактов, столько же, сколько букв в латинском алфавите. Контакты с обеих сторон соединялись в нутрии диска, достаточно случайным образом, 25 проводами, формировавшими замену символов. Диски складывались вместе и их контакты, касаясь друг друга, обеспечивали прохождение электрических импульсов через весь пакет дисков на регулирующее устройство. На боковой поверхности дисков был нанесен алфавит. Перед началом работы диски поворачивались так, чтобы установить кодовое слово. При нажатии клавиши и кодировании левый барабан поворачивался на один шаг. После того как диск делал полный оборот, поворачивался следующий барабан.

В процессе шифрования на один из контактов левого диска поступал электрический импульс. Так как барабаны соприкасались контактами, то электрический импульс попадал на выход, проходя четыре диска и претерпевая четыре простые замены. Исполняющее устройство (пишущая машинка или перфоратор) фиксировало знак шифрованного текста в соответствии с тем, на какой контакт выходного диска поступал электрический импульс. Поскольку в каждый такт шифрования сдвигался на один шаг хотя бы один диск, подстановка – простая замена, по которой осуществлялось шифрование, менялась для каждого символа открытого текста. Ключом шифратора, который сменялся каждый сеанс, являлся набор начальных угловых положений дисков. Долговременным ключом, он менялся очень редко, служили коммутации дисков – соединения проводов внутри дисков. Для затруднения расшифрования диски выбирались из комплекта, состоящего из 10-20 дисков [1].

Несмотря на сложность Энигмы, она была взломана в течении Второй Мировой войны. Сначала группа польских криптографов взломала немецкую Энигму, а англичане продолжали криптоанализ новых версий. Несмотря на то, что немцы изменили способ передачи и дополнительно усложнили саму машину, англичанам неизменно удавалось проникать в немецкие шифры. Для ускорения процесса расшифровки англичане создали ряд вспомогательных технических приспособлений. Помимо шифров Энигмы, немцы использовали и некоторые другие шифровальные машины дальнего действия, обеспечивавшие высокий уровень связи. Эти машины, имевшие широкое обозначение Geheimschreiber (тайнописные машины), были способны порождать чрезвычайно сложные шифры. Для анализа этих шифров англичане сконструировали целый ряд «протокомпьютеров», с помощью которых они часто успешно взламывали немецкие машинные шифры. Полученные при этом сведения были широко известны под обозначением ULTRA.

Тем временем американцы успешно раскалывали японские шифры. Полученные ими данные были известны широкой публике под кодовым обозначением MAGIC. Вслед за машинами RED и PURPLE криптоаналитики раскрыли устройство японских шифровальных машин JADE и CORAL.

Роторные системы - вершина формальной криптографии, так как относительно просто реализовывали очень стойкие шифры. Успешные криптоатаки на роторные системы стали возможны только с появлением ЭВМ в начале 40-х годов. Главная отличительная черта научной криптографии 30-е - 60-е годы XX века - появление криптосистем со строгим

математическим обоснованием криптостойкости. К началу 30-х годов окончательно сформировались разделы математики, являющиеся научной основой криптологии: теория вероятностей и математическая статистика, общая алгебра, теория чисел, начали активно развиваться теория алгоритмов, теория информации, кибернетика. Своеобразным водоразделом стала работа Клода Шеннона «Теория связи в секретных системах» 1949, где сформулированы теоретические принципы криптографической защиты информации. Шеннон ввел понятия «рассеивание» и «перемешивание», обосновал возможность создания сколь угодно стойких криптосистем. В 60-х годах ведущие криптографические школы подошли к созданию блочных шифров, еще более стойких по сравнению с роторными криптосистемами, однако допускающие практическую реализацию только в виде цифровых электронных устройств.

Компьютерная криптография (с 70-х годов XX века) обязана своим появлением вычислительным средствам с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую защищенность, чем при «ручных» или «механических» [2].

Первым классом криптосистем, практическое применение которых стало возможно с появлением мощных и компактных вычислительных средств, стали блочные шифры. В 70-е годы был разработан американский стандарт шифрования DES (принят в 1978 году). Один из его авторов, Хорст Фейстел (сотрудник IBM), описал модель блочных шифров, на основе которой были построены другие, более стойкие симметричные криптосистемы, в том числе отечественный стандарт шифрования ГОСТ 28147-89.

С появлением DES обогатился и криптоанализ, для атак на американский алгоритм был создано несколько новых видов криптоанализа, практическая реализация которых опять же была возможна только с появлением мощных вычислительных систем.