Криптография как наука. Основные модели криптосистем

Криптография – это фундаментальная наука, изучающая методы преобразования информации, направленные на сокрытие ее содержания.

Слово «криптография» (cryptography) происходит от греческих слов «kryptus» - тайный, «graphein» - писать, т.е. дословно «тайнопись».

Криптоанализ – это наука, изучающая методы взлома шифров.

Криптология – наука, которая занимается изучением шифров и их стойкости.

Криптология = Криптография + Криптоанализ

История криптографии насчитывает несколько тысячелетий. Первые системы шифрования появились одновременно с письменностью в четвертом тысячелетии до н.э..

Дэвид Кон (David Kohn) в своей эпической книге о криптоанализе «Выдающиеся взломщики шифров» привел данные о том, что криптография использовалась в Египте в 1900 г. до н.э., при написании Библии – в 500 г. до н.э.. В Древней Греции и Древнем Риме криптография уже широко использовалась в разных областях деятельности, особенно в государственной сфере. (Юлий Цезарь «Записки о галльской войне», 1 век до н.э..) В мрачные годы средневековья практика шифрования сохранялась в строжайшей тайне. В годы крестовых походов шифровальщики, служившие у Папы Римского, после года работы подлежали физическому уничтожению.

Период развития криптологии с древних времен до 1949 г. принято называть эрой донаучной криптологии, поскольку достижения тех времен основаны на интуиции и не подкреплялись доказательствами. Криптологией занимались тогда почти исключительно как искусством, а не как наукой.

Вторая мировая война явилась поворотным пунктом в истории криптографии: если до войны криптография представляла собой достаточно узкую область, то после войны она стала широким полем деятельности.

Публикация в 1949 г. статьи Клода Шеннона «Теория связи в секретных системах» стала началом новой эры научной криптологии с секретными ключами. В этой блестящей работе Шеннон связал криптографию с теорией информации.

На последние 25-30 лет пришлось значительное повышение активности в области развития криптографии, наблюдался бурный рост открытых академических исследований. До этого времени криптография использовалась исключительно в военных и разведовательных целях.

В 70-х годах произошло два события, серьезно повлиявших на дальнейшее развитие криптографии. Во-первых, был принят (и опубликован!) первый стандарт шифрования данных (DES). Во-вторых, после работы американских математиков У.Диффи и М.Хеллмана родилась «новая криптография» - криптография с открытым ключом. Оба этих события были рождены потребностями бурно развивающихся средств коммуникаций, в том числе локальных и глобальных компьютерных сетей, для защиты которых потребовались легко доступные и достаточно надежные криптографические средства. Криптография стала широко востребованной не только в военной, дипломатической, государственной сферах, но также в коммерческой, банковской и т.д..

Стеганография – совокупность методов, предназначенных для сокрытия факта существования сообщения.

Например:

1.                      Расстановка слов или букв открытого текста так, чтобы он нес в себе скрытое сообщение.

2.                      Пометка символов.

3.                      Невидимые чернила.

4.                      Прокалывание бумаги.

5.                      Печать между строк с использованием корректирующей ленты.

Сами по себе подобные методы выглядят архаично, но у них есть современные эквиваленты. Например, сокрытие сообщений с помощью использования незначащих бит в видеокадрах компакт-дисков.

В настоящее время разработано множество программных пакетов, позволяющих осуществлять подобные операции. Преимущество стеганографии состоит в том, что она может скрывать сам факт передачи сообщений, а не только их содержимое. Ведь само шифрование вызывает подозрение – значит есть что скрывать.

Краеугольный камень криптографии – шифрование (криптографическая обработка информации с помощью одного из алгоритмов).

Исходное сообщение называется открытым текстом. Зашифрованное сообщение называется шифртекстом.

Любой алгоритм шифрования должен быть дополнен алгоритмом расшифрования, чтобы привести зашифрованный текст в исходный вид.

(Дешифрование – восстановление исходного текста без знания ключа)

Пара процедур – шифрование и расшифрование – называется криптосистемой.

Во введении к книге «Прикладная криптография» у Б. Шнайера написано: «В мире различают два типа криптографии: криптография, которая помешает вашей младшей сестре читать ваши файлы, и криптография, которая помешает читать ваши файлы правительствам крупных стран. Эта книга посвящена криптографии второго типа».

Сегодня широко распространено 2 типа шифрования:

1.     Традиционное

2.     Шифрование с открытым ключом.

Процесс традиционного шифрования включает две составляющие:

1.     Алгоритм шифрования.

2.     Ключ – значение, не зависящее от открытого текста.

Результат, достигаемый при выполнении алгоритма, зависит от применяемого ключа. Изменение ключа приводит к изменению шифрованного текста.

Надежность традиционного шифрования определяет нескольких факторов:

1.                         Сложность алгоритма шифрования (должен быть достаточно сложным, чтобы невозможно было расшифровать сообщение при наличии только шифрованного текста).

2.                         Секретность ключа – основной фактор надежности традиционного шифрования. Сам алгоритм может быть несекретным.

В традиционной (классической) криптографии принято фундаментальное правило, сформулированное в 19 веке - правило Керкхоффа:

Стойкость шифра должна определяться только секретностью ключа.

Эта особенность традиционного шифрования обусловливает его широкую популярность и признание. Т.к. нет необходимости хранить в секрете алгоритм, то производители могут реализовать алгоритмы шифрования в виде дешевых общедоступных микросхем, которыми оснащены многие современные системы.

Рассмотрим модель традиционной криптосистемы более подробно.

Теоретические основы традиционной модели симметричной криптосистемы впервые были изложены в 1949 году в работе Клода Шеннона.

Источник создает сообщение в форме открытого текста:

Х=[x1, x2, …, xm]

Элементами хi открытого текста Х являются символы некоторого конечного алфавита А, состоящего из n символов:

хi  A

Традиционно использовался алфавит из 26 букв английского языка, но сегодня чаще применяется двоичный алфавит {0,1}.

Для шифрования генерируется ключ в форме:

К=[к1, к2, …, кj]

Если ключ генерируется там же, где и само сообщение, то его необходимо переправлять получателю по секретным каналам. Либо ключ создается третьей стороной, которая должна защищенным способом обеспечить доставку ключа отправителю и получателю сообщения.

Имея Х и К с помощью алгоритма шифрования фомируется шифрованный текст

У=[у1, у2, …, уn]

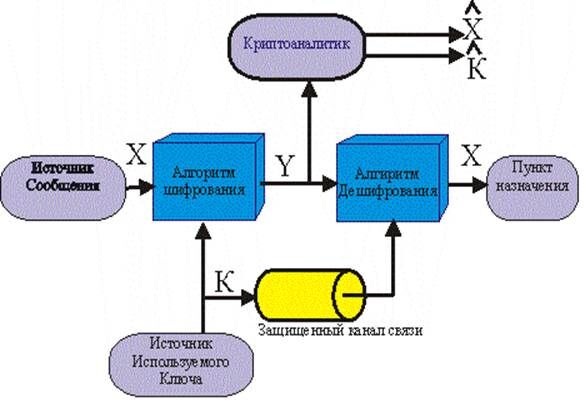
Это можно записать в виде формулы:

У = Еk(Х)

У получается путем применения алгоритма шифрования Е к открытому тексту Х при использовании ключа К.

Обратное преобразование:

Х = Dk (У)



2. Типы криптосистем.

Классификация криптографических систем строится на основе следующих трех характеристик:

1)    Число применяемых ключей.

2)    Тип операций по преобразованию открытого текста в шифрованный.

3)    Метод обработки открытого текста.

1) По числу применяемых ключей.

Различают:

1)    Симметричные криптосистемы;

2)    Асимметричные криптосистемы.

·        Если отправитель и получатель используют один и тот же ключ, система шифрования называется симметричной, системой с одним ключом, системой с секретным ключом, схемой традиционного шифрования. (Например, DES, CAST, RC5, IDEA, Blowfish, классические шифры);

·        Если отправитель и получатель используют разные ключи, система называется асимметричной, системой с двумя ключами, схемой шифрования с открытым ключом. (RSA, Эль-Гамаля).

2) По типу операций по преобразованию открытого текста в шифрованный.

·        Подстановочные шифры - шифрование основано на замещении каждого элемента открытого текста (бита, буквы, группы битов или букв) другим элементом. (Цезаря, Плейфейера, Хилла);

·        Перестановочные шифры – шифрование основано на изменении порядка следования элементов открытого текста. (Лесенка, перестановка столбцов);

·        Продукционные шифры – шифрование основано на комбинации нескольких операций замены и перестановки. Продукционные шифры применяются в большинстве реальных современных систем шифрования. (DES).

3) По методу обработки открытого текста.

·          Блочные шифры –  Блочными называются шифры, в которых логической единицей шифрования является некоторый блок открытого текста, после преобразования которого получается блок шифрованного текста такой же длины.  
Например: DES, шифр Файстеля.

·          Поточные шифры – подразумевают шифрование всех элементов открытого текста последовательно, одного за другим (бит за битом, байт за байтом).  
Примерами классических поточных шифров являются шифры Виженера (с автоматическим выбором ключа) и Вернама.

Блочные шифры изучены гораздо лучше. Считается, что они обладают более широкой областью применения, чем поточные. Большинство сетевых приложений, в которых применяется схема традиционного шифрования, используют блочные шифры.

3.    Типы криптоатак и стойкость алгоритмов.

Процесс воссоздания открытого текста (Х) и/или ключа (К) называется криптоанализом.

Алгоритм шифрования считается раскрытым, если найдена процедура, позволяющая подобрать ключ за реальное время.

Сложность алгоритма раскрытия является одной из важных характеристик криптосистемы и называется криптостойкостью.

Самым древним и самым простым из известных подстановочных шифров является шифр Юлия Цезаря. В шифре Цезаря каждая буква алфавита заменяется буквой, которая находится на 3 позиции дальше в этом же алфавите.

В общем случае сдвиг может быть любым (от 1 до 25). Если каждой букве назначить числовой эквивалент, то:

Y = Ek(X) = (x + k)mod26

Получаем обобщенный алгоритм Цезаря.

Шифр Цезаря со сдвигом на 13 букв вправо обозначается rot13.

Раскрыть такой шифр можно путем простого последовательного перебора вариантов. Применение простого перебора оправдано следующим:

1)    известны алгоритмы шифрования и расшифрования;

2)    всего 25 вариантов;

3)    известен язык открытого текста.

В большинстве случаев при защите сетей выполняется 1), но не 2). Важная характеристика – 3). Если исходный текст предварительно сжат, то это сильно затрудняет распознавание.

Для криптоаналитика существует и другая возможность раскрытия шифра (кроме перебора вариантов). Если криптоаналитик имеет представление о природе открытого текста, можно использовать  информацию о характерных признаках, присущих текстам на соответствующем языке (статистические методы). Например, анализ частот появления букв алфавита.

Моноалфавитные шифры легко раскрываются, т.к. они наследуют частотность употребления букв оригинального алфавита. Чтобы в тексте, шифрованном с помощью методов подстановок, структура исходного текста проявлялась менее заметно, можно использовать:

-         многобуквенное шифрование, т.е. замещение не отдельных символов открытого текста, а комбинаций нескольких символов;

-         несколько алфавитов.

Один из наиболее известных шифров, базирующихся на методе многобуквенного шифрования, - шифр Плейфейера (Playfair). В нем биграммы (комбинации из двух букв) открытого текста рассматриваются как самостоятельные единицы, преобразуемые в заданные биграммы шифрованного текста. Анализ частот биграмм сложнее. Долго считалось, что шифр Плейфейера взломать нельзя. Он служил стандартом шифрования в британской армии во время 1-й мировой войны и даже использовался в годы 2-й мировой войны в США.

Примером многобуквенного шифра является также шифр Хилла (1929г.). В его основе лежит алгоритм, который заменяет каждые m последовательных букв открытого текста  m буквами шифрованного текста.

Одна из возможностей усовершенствования простого моноалфавитного шифра заключается в использовании нескольких моноалфавитных подстановок в зависимости от определенных условий. Семейство шифров, основанных на применении таких методов шифрования, называется полиалфавитными шифрами. Они обладают следующими свойствами:

-         используется набор связанных моноалфавитных подстановок;

-         имеется ключ, по которому определяется, какое конкретное преобразование должно применяться для шифрования на данном этапе.

Полиалфавитные подстановочные шифры были придуманы в 15-м веке. Леоном Баттистой-Альберти. Они пользовались популярностью до 19 века, когда их начали взламывать.

Самым известным и простым алгоритмом такого рода является шифр Виженера (поточный).

Лучшей защитой от статистических методов криптоанализа (т. е. по частоте появления букв) является выбор ключевого слова, по длине равного длине открытого текста, но отличающегося от открытого текста по статистическим показателям. Такая система была предложена инженером компании AT&T Гилбертом Вернамом в 1918 году. В алгоритме Вернама шифрованный текст генерируется путем побитового выполнения операции XOR для открытого текста и ключа.

Сi = pi Å ki

Может ли существовать идеальный шифр, который невозможно взломать? Хотите верьте, хотите нет, но абсолютный метод шифрования существует.

Джозеф Моборн придумал улучшение схемы Вернама, которое сделало ее исключительно надежной. Он предложил случайным образом генерировать ключ, по длине равный длине сообщения. Каждый символ ключа используется только один раз и только в одном сообщении. На выходе получается случайная последовательность, не имеющая статистической связи с открытым текстом. Схема получила название лента однократного использования или одноразовый блокнот. Взлому она не поддается, т.к. шифртекст не содержит никакой информации об открытом тексте. Однако, использование одноразового блокнота затруднено, потому что отправитель и получатель должны располагать одним случайным ключом, что  трудно реализуемо на практике.

Понятие идеального шифра ввел в своих работах Шеннон. Он ставил задачу воспрепятствовать попыткам криптоанализа, основанным на статистических методах. Идеальный шифр – это шифр, который полностью скрывает в шифрованном тексте все статистические закономерности открытого текста.

Схема шифрования называется абсолютно стойкой (безусловно защищенной), если шифрованный текст не содержит информации, достаточной для однозначного восстановления открытого текста.

Это означает, независимо от того, сколько времени потратит противник на расшифровку текста, ему не удастся расшифровать его просто потому, что в шифрованном тексте нет информации, требуемой для восстановления открытого текста.

Максимум, что может дать алгоритм шифрования, это выполнение хотя бы одного из следующих условий:

1)                      Стоимость взлома шифра превышает стоимость расшифрованной информации;

2)                      Время, которое требуется для взлома шифра, превышает время, в течение которого информация актуальна.

Если схема шифрования соответствует обоим указанным критериям, она называется защищенной по вычислениям.

Все формы криптоанализа для схем традиционного шифрования разрабатываются на основе того, что некоторые характерные особенности структуры открытого текста могут сохраняться при шифровании, проявляясь в шифрованном тексте.

Криптоанализ для схем с открытым ключом базируется на совершенно другом – на том, что математические зависимости, связывающие пары ключей, дают возможность с помощью логических рассуждений, зная один из ключей, найти второй.

Основные типы криптоатак:

1)    Атака на основе шифртекста.

Криптоаналитик располагает шифртекстами нескольких сообщений, зашифрованных одним и тем же алгоритмом шифрования и возможно ключом.

2)    Атака на основе открытого текста.

Криптоаналитик располагает доступом не только к шифртекстам нескольких сообщений, но и открытому тексту этих сообщений. Его задача состоит в определении ключа или ключей, чтобы он мог расшифровать другие сообщения.

3)    Атака на основе подобранного открытого текста (криптоаналитик может выбирать открытый текст для шифрования).

Во многих сообщениях используются стандартные начала и окончания, которые могут быть известны криптоаналитику (атаки 2, 3).

В этом отношении особенно уязвимы шифрованные исходные коды программ из-за частого использования ключевых слов (define, struct, else, return и т.д.). Те же проблемы и у шифрованного исполняемого кода: функции, циклические структуры и т.д..

4)    Лобовое вскрытие (лобовая атака, метод «грубой силы» – путем перебора всех возможных ключей).

5)    Бандитский криптоанализ.

Для получения ключа “криптоаналитик” прибегает к угрозам, шантажу или пыткам. Возможно также взяточничество, которое называется вскрытием с покупкой ключа. Это очень мощные и, зачастую, самые эффективные методы взлома алгоритма.

Никогда нельзя забывать правило Керкхоффа. Если надежность новой криптосистемы опирается на незнание взломщиком алгоритма, то вы пропали. Вы заблуждаетесь, если думаете, что сохранение в тайне принципа работы алгоритма защитит криптосистему. Это наивное предположение.

“Берегитесь людей, превозносящих достоинства своих алгоритмов, но отказывающихся их опубликовать. Доверять таким алгоритмам – все равно, что верить в целебные свойства знахарских снадобий.” (Б. Шнайер)

Лучшие алгоритмы шифрования – это те, которые были опубликованы, годами вскрывались лучшими криптографами мира, и все-таки остались несокрушенными.