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

Показатели криптостойкости

- количество всех возможных ключей;
- среднее время, необходимое для криптоанализа.

Требования к криптосистемам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно.

Требования к криптосистемам

1. зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
2. число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

Требования к криптосистемам

3. число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
4. знание алгоритма шифрования не должно влиять на надежность защиты;

Требования к криптосистемам

5. незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
6. структурные элементы алгоритма шифрования должны быть неизменными;

Требования к криптосистемам

7. дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;
8. длина шифрованного текста должна быть равной длине исходного текста;
9. не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемых в процессе шифрования;

Требования к криптосистемам

10. любой ключ из множества возможных должен обеспечивать надежную защиту информации;
11. алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования

Основные алгоритмы шифрования

- симметричные (или алгоритмы секретным ключом) - используют один и тот же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки).

- асимметричные (или алгоритмы с открытым ключом) - используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу шифровки

Симметричные алгоритмы

потоковые шифры - позволяют шифровать информацию побитово

блочные шифры - работают с некоторым набором бит данных (обычно размер блока составляет 64 бита) и шифруют этот набор как единое целое.

симметричные алгоритмы работают быстрее, чем асимметричные.

На практике оба типа алгоритмов часто используются вместе: алгоритм с открытым ключом используется для того, чтобы передать случайным образом сгенерированный секретный ключ, который затем используется для дешифровки сообщения.

Цифровые подписи

Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного ключа.

При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа.

Цифровые подписи

для подтверждения, что сообщение пришло действительно от данного отправителя

для проставления *штампа времени* (*timestamp*) на документах.

для удостоверения (*сертификации — to certify*) того, что документ принадлежит определенному лицу.

Криптографические генераторы случайных чисел

Криптографические генераторы случайных чисел производят случайные числа, которые используются в криптографических приложениях, например — для генерации ключей.

Криптографические генераторы случайных чисел

случайные числа должны основываться на настоящем физическом источнике случайной информации, которую невозможно предсказать.
Примеры таких источников включают шумящие полупроводниковые приборы, младшие биты оцифрованного звука, интервалы между прерываниями устройств или нажатиями клавиш.

Криптографические генераторы случайных чисел

Полученный от физического источника шум затем «дистиллируется» криптографической хэш-функцией так, чтобы каждый бит зависел от каждого бита.

Криптографические генераторы случайных чисел

Достаточно часто для хранения случайной информации используется довольно большой пул (несколько тысяч бит) и каждый бит пула делается зависимым от каждого бита шумовой информации и каждого другого бита пула криптографически надежным (*strong*) способом.

Криптоанализ и атаки на криптосистемы

Криптоанализ — это наука о дешифровке закодированных сообщений при отсутствии знаний о значении ключей.

Атаки на криптосистемы

Атака со знанием лишь шифрованного текста.

Атакующий не знает ничего о содержании сообщения, и ему приходится работать лишь с самим шифрованным текстом. На практике, часто можно сделать правдоподобные предположения о структуре текста, поскольку многие сообщения имеют стандартные заголовки. Даже обычные письма и документы начинаются с легко предсказуемой информации. Также часто можно предположить, что некоторый блок информации содержит заданное слово.

Атаки на криптосистемы

Атака со знанием содержимого шифровки

Атакующий знает или может угадать содержимое всего или части зашифрованного текста. Задача заключается в расшифровке остального сообщения.

Это можно сделать либо путем вычисления ключа шифровки, либо минуя это.

Атаки на криптосистемы

Атака с заданным текстом

Атакующий имеет возможность получить шифрованный документ для любого нужного ему текста, но не знает ключа. Задачей является нахождение ключа. Некоторые методы шифрования и, в частности, RSA, весьма уязвимы для атак этого типа.

Атаки на криптосистемы

Атака с подставкой

Атака направлена на обмен шифрованными сообщениями и, в особенности, на протокол обмена ключами. Идея заключается в том, что когда две стороны обмениваются ключами для секретной коммуникации противник внедряется между ними на линии обмена сообщениями.

Атаки на криптосистемы

Атака с помощью таймера

Этот новый тип атак основан на последовательном измерении времен, затрачиваемых на выполнение операции возведения в степень по модулю целого числа.
Ей подвержены по крайней мере следующие шифры: RSA, Диффи-Хеллман и метод эллиптических кривых.

Критерии эффективности

Выбор для конкретных ИС должен быть основан на глубоком анализе слабых и сильных сторон тех или иных методов защиты. Обоснованный выбор той или иной системы защиты в общем-то должен опираться на какие-то *критерии эффективности*.

К сожалению, до сих пор не разработаны подходящие методики оценки эффективности криптографических систем.

Критерии эффективности

Наиболее простой критерий такой эффективности — ***вероятность раскрытия ключа*** **или** ***мощность множества ключей (M).***

По сути это то же самое, что и ***криптостойкость***.

Для ее численной оценки можно использовать также и сложность раскрытия шифра путем перебора всех ключей.

Однако этот критерий не учитывает других важных *требований к криптосистемам*:

1. невозможность раскрытия или осмысленной модификации информации на основе анализа ее структуры;
2. совершенство используемых протоколов защиты;
3. минимальный объем используемой ключевой информации;
4. минимальная сложность реализации (в количестве машинных операций), ее стоимость;
5. высокая оперативность.