сделать путём перепрограммирования ПЗУ компьютера, замены на загрузочную запись, драйвер, утилиту, прикладную или служебную программу, полученную от источника, заслуживающего доверия, можно попытаться добыть исходный текст, убрать из него имеющиеся закладки или подозрительные фрагменты, а затем заново откомпилировать [3].

Защитить информацию может только сам пользователь или владелец информационного ресурса. Для этого нужно правильно организовать работу и ограничить доступ к ценной информации. И принять все меры для предотвращения её утечки.

Литература

Анин Б. Ю. «Защита компьютерной информации». – СПб.: БХВ-Петербург, 2000. – 384 с.

Казарин О.В. «Безопасность программного обеспечения компьютерных систем». – М.: МГУЛ, 2003. - 212 с.

Романец Ю., Тимофеев П., Шаньгин В. «Защита информации в компьютерных системах и сетях». – М.: Радио и связь, 2001 – 376 с.

Криптография как наука. Типы криптосистем

Краснова А.К.
Научный руководитель:Ковалькова И.А.
Белорусский национальный технический университет

Криптография – это наука об использовании математики для зашифрования и расшифрования данных.

История криптографии насчитывает несколько тысячелетий. Первые системы шифрования появились одновременно с письменностью в четвёртом тысячелетии до н.э.. В Древней Греции и Древнем Риме криптография широко использовалась в разных областях деятельности, особенно в государственной сфере. В годы средневековья практика шифрования сохранялась в строжайшей тайне. В годы крестовых походов шифровальщики, служившие у Папы Римского, после года работы подлежали физическому уничтожению.

настоящее время, в связи с увеличением вычислительной мощности компьютеров, криптография стала значительно более сложной. Теперь она способна намного надёжнее гарантировать безопасность информации. Шифры, какие когда-то использовал Цезарь, сегодня можно расшифровать за пару секунд [1].

Практическое применение криптографии стало неотъемлемой частью жизни современного общества – её используют в таких отраслях как

электронная коммерция, электронный документооборот, телекоммуникации и других.

Основным компонентом криптографии является шифрование. Сообщения шифруются и расшифровываются с помощью сложных алгоритмов, созданных комбинацией информатики и математики.

Шифрование использует алгоритм и ключ для преобразования входных данных в зашифрованные выходные данные. Этот метод защиты позволяет просматривать сообщения исключительно отправителю и получателю, поскольку зашифрованную информацию может прочесть только тот, кто имеет секретный ключ для преобразования сообщения в простой текст.

Классификация криптографических систем строится на основе следующих трёх характеристик:

числу применяемых ключей;

типу операций по преобразованию открытого текста в шифрованный;

методу обработки открытого текста.

По числу применяемых ключей различают:

Симметричные криптосистемы. Имеютсамымый простой алгоритм. Криптографы часто называют его секретным ключом криптографии (SKC) или общим, поскольку шифрование и расшифровка информации происходит с использованием одного и того же ключа. Симметричное шифрование подразумевает, что секретный цифровой ключ должен быть известен как получателю, так и отправителю. (Например, DES, CAST, RC5, IDEA, Blowfish, классические шифры).

Асимметричные криптосистемы. Этот алгоритм широко используется во Всемирной сети. Его также называют открытым ключом криптографии. Таокй алгоритм использует два ключа: открытый и закрытый.

Открытый ключ может быть известен многим. Расшифровать данные с его помощью невозможно. Например, адрес электронной почты является открытым ключом.

Закрытый ключ является секретным, используется для расшифровки сообщения, никогда не раскрывается другой стороне. Например, пароль учётной записи электронной почты является ключом к открытию электронных писем.

По типу операций по преобразованию открытого текста в шифрованный различают:

подстановочные шифры– шифрование основано на замещении каждого элемента открытого текста (бита, буквы, группы битов или букв) другим элементом (шифры: Цезаря, Плейфейера, Хилла);

перестановочные шифры – шифрование основано на изменении порядка следования элементов открытого текста (шифры: Лесенка, перестановка столбцов);

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

По методу обработки открытого текста различают:

блочные шифры – 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, т.е. бит за битом, байт за байтом (например, шифры Виженера).

Блочные шифры обладают более широкой областью применения, чем поточные [2].

Преимущества криптографии:

Конфиденциальность. Использование криптографии защищает конфиденциальную информацию от несанкционированного доступа.

Контроль и управление доступом. Криптография, используя различные алгоритмы шифрования, обеспечивает ограниченный контроль доступа к хранящейся или передаваемой информации.

Проверка подлинности. Криптографические методы, такие как коды аутентификации сообщений и цифровые подписи, могут защитить информацию от подмены и подделки.

Целостность данных. Криптографические хэши используются для сохранения целостности сообщений [3].

Литература

Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.

Классификациякриптографическихсистем.Режим доступа:https://studizba.com/lectures/10-informatika-i-programmirovanie/316-lekcii-po-bezopasnosti-informacii/4240-3-klassifikaciya-kriptograficheskih-sistem.htm.

Современная криптография. Алгоритмы шифрования. Режим доступа: https://artismedia.by/blog/sovremennaya-kriptografiya-algoritmy-shifrovaniya/.