EURASIAN JOURNAL OF ACADEMIC RESEARCH
Innovative Academy Research Support Center
UIF = 8.1 | SJIF = 5.685 www.in-academy.uz

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Имамова Шахноза Фуркатовна
Аспирант Термезского государственного университета по специальности «Компьютерные системы и их программное обеспечение»
shaxnozaimomova1998@gmail.com
https://doi.org/10.5281/zenodo.7588246

ARTICLE INFO

Received: 20th January 2023
Accepted: 30th January 2023
Online: 31th January 2023

KEY WORDS

Криптографическая защита, информация, кодирование информации, целостность информации.

ABSTRACT

Самое ценное богатство в современной реальности – это не золото и не валюта, а информация. Информационные активы представляют собой совокупность личной и конфиденциальной информации, интеллектуальной собственности, секретных разработок, финансовой и иной деятельности предприятий, подпадающих под определение коммерческой тайны. Перечисленные типы данных требуют высокого уровня защиты. В настоящее время наиболее надежным способом обеспечения информационной безопасности являются криптографические методы. В этой статье представлена информация о криптографическом кодировании информации.

Криптография – это наука, изучающая проблему обеспечения безопасности информационного сообщения с помощью секретной записи и расшифровки. Криптографы также обеспечивают безопасность аутентификации и идентификацию пользователей компьютерных систем, которые обмениваются информацией.

Для защиты криптографических данных используются различные средства и методы. Существует два принципа криптографической защиты: принцип конфиденциальности данных и принцип целостности данных. На них основана безопасность используемых средств защиты.

Криптографическое шифрование данных — это процесс преобразования данных с помощью кодирования. Сообщение шифруется с помощью специального алгоритма (ключа) и отправляется получателю. Получатель использует тот же алгоритм дешифрования. Таким образом, информация защищена от разглашения, которое может произойти, если сообщение будет получено третьими лицами. В современном мире этот метод шифрования называется симметричным криптографическим ключом.

Шифрование — это простой метод защиты сообщения с использованием различных наборов символов для замены слов или фраз в кодируемом сообщении. Кодирование, как и шифрование, использовалось веками. Отличие этого метода защиты информации в том, что код угадать легче, чем пароль.

До изобретения компьютеров кодировщики использовали для защиты сообщений целые словари, в которых значение каждого слова указывалось в виде набора кодовых символов. В настоящее время кодирование и обратное преобразование осуществляется с помощью специального программного или аппаратного обеспечения. Шифрование — популярный метод защиты данных в воинских частях и других родах войск.

Сжатие является лишь косвенным средством криптографической защиты данных. Причина этого в том, что изначально сжатие электронных файлов делалось не для защиты информации, а для уменьшения ее размера. Однако, поскольку сжатые данные невозможно прочитать, сжатие стало инструментом криптографической защиты данных.

Сжатие является наименее эффективным из всех средств криптографической защиты. Восстановить сжатые файлы в исходное состояние можно с помощью стандартного пакета программ или методов статистической обработки данных. В связи с этим электронные файлы должны быть зашифрованы перед сжатием для защиты конфиденциальной информации.

Существует множество способов шифрования текстовых сообщений и аудиофайлов. Однако не все из них используются из-за разного уровня надежности. Современная криптография преследует следующие четыре цели:

1. Конфиденциальность. Никто не может понять информацию.
2. Честность. Информация не может быть изменена при хранении или при передаче между отправителем и предполагаемым получателем без обнаружения изменения.
3. Не отказывайся. Создатель/отправитель информации не может на более позднем этапе отрицать свои намерения по созданию или передаче информации.
4. Аутентификация. Отправитель и получатель могут подтвердить личность друг друга и происхождение/назначение данных.

Процедуры и протоколы, отвечающие некоторым или всем вышеперечисленным критериям, называются криптосистемами. О криптосистемах часто думают как о математических процедурах и компьютерных программах; однако они также включают в себя регулирование человеческого поведения, например выбор сложных паролей, выход из неиспользуемых систем и отказ от обсуждения конфиденциальных процедур с незнакомцами.

Криптосистемы используют набор процедур, известных как криптографические алгоритмы или шифры, для шифрования и дешифрования сообщений для защиты связи между компьютерными системами, устройствами и приложениями.

Набор шифров использует один алгоритм для шифрования, другой алгоритм для аутентификации сообщений и еще один алгоритм для обмена ключами. Этот процесс, встроенный в протоколы и написанный в операционных системах (ОС) и программном обеспечении, работающем в сетевых компьютерных системах, включает:

- генерация открытых и закрытых ключей для шифрования/дешифрования данных
- цифровая подпись и проверка подлинности сообщения
- обмен ключами

Хакеры могут обойти криптографию, скомпрометировать компьютеры, ответственные за шифрование и расшифровку данных, и использовать уязвимости, такие как использование ключей по умолчанию. Однако криптография затрудняет доступ злоумышленников к сообщениям и данным, защищенным алгоритмами шифрования.

Криптографию можно разделить на три различных типа:

- Криптография с секретным ключом
- Криптография с открытым ключом
- Хэш-функции

Криптография с закрытым ключом или симметричная криптография использует один ключ для шифрования данных. В симметричной криптографии и шифрование, и дешифрование используют один и тот же ключ, что делает его самой простой формой криптографии. Криптографический алгоритм использует ключ в шифре для шифрования данных, и когда к данным необходимо получить доступ снова, лицо, которому доверен секретный ключ, может расшифровать данные. Криптография с закрытым ключом может использоваться как для данных в пути, так и для данных в состоянии покоя, но обычно используется только для данных в состоянии покоя, поскольку отправка секретного сообщения получателю может привести к компрометации.

Криптография с открытым ключом или асимметричная криптография использует два ключа для шифрования данных. Один из них используется для шифрования, а другой может расшифровать сообщение. В отличие от симметричной криптографии, если для шифрования используется один ключ, этот ключ не может расшифровать сообщение, вместо этого используется другой ключ.

Один ключ хранится в секрете и называется «закрытым ключом», а другой является общедоступным и может использоваться кем угодно, поэтому он называется «открытым ключом». Математическая связь между ключами такова, что закрытый ключ не может быть получен из открытого ключа, но открытый ключ может быть получен из закрытого ключа. Закрытый ключ не должен распространяться и должен оставаться только у владельца. Открытый ключ может быть передан любому другому объекту.

References:

1. Encryption: Strengths and Weaknesses of Public-key Cryptography Matt Blumenthal.
2. Kellogg S. Booth, “Authentication of signatures using public key encryption,” Communications of the ACM, November 1981, pp. 772-774.
3. Amir Herzberg, Markus Jakobsson, Stanisław Jarecki, Hugo Krawczyk, Moti Yung, “Proactive public keys and signature systems Conference on Computer and Communications Security, 1997, pp. 100-110.
4. W. Küchlin, “Public key encryption,” ACM SIGSAM Bulletin, August 1987, pp. 69-73.
5. Aleksandar Jurisic and Alfred J. Menezes, Elliptic Curves and Cryptography, 2008.