УДК 003.26(076.1)

К ВОПРОСУ ПРИМЕНЕНИЯ КРИПТОГРАФИИ

Наталия Владимировна Пчелинцева
старший преподаватель
natas79@mail.ru
Илья Валерьевич Чепраков
студент
i.cheprakov@mail.ru
Анастасия Александровна Гущина
студент
nastya.gushchina02@mail.ru
Мичуринский государственный аграрный университет
Мичуринск, Россия

Аннотация. Статья посвящена изучению криптографии. В ней рассматривается история криптографии, криптографические методы, а также использование криптографии в современном мире.

Ключевые слова: криптография, сетевая безопасность, хэширование, шифрование.

Криптография - это наука о защите информации путем преобразования ее в форму, которую непреднамеренные получатели не могут понять. В криптографии исходное сообщение, читаемое человеком, называемое открытым текстом, преобразуется с помощью алгоритма или серии математических операций в зашифрованный текст [1, 2].

Одним из важных аспектов процесса шифрования является то, что он почти всегда включает в себя как алгоритм, так и ключ. Ключ - это просто еще одна часть информации, почти всегда номер, который определяет, как алгоритм применяется к открытому тексту для его шифрования. Даже если известен метод, с помощью которого шифруется какое-либо сообщение, его трудно или невозможно расшифровать без этого ключа [3, 4].

На самом деле развитие компьютеров и достижения в области криптографии шли рука об руку. Во время Второй мировой войны немцы использовали электромеханическую машину Enigma для шифрования сообщений - и, как известно, Алан Тьюринг возглавлял команду в Великобритании, которая разработала аналогичную машину для взлома кода, в процессе заложив некоторые основы для первых современных компьютеров. Криптография радикально усложнилась с появлением компьютеров, но оставалась прерогативой шпионов и генералов еще несколько десятилетий. Однако в 1960-х годах ситуация начала меняться.

Формирование первых компьютерных сетей заставило гражданских лиц задуматься о важности криптографии. Компьютеры общались друг с другом по открытой сети, а не только через прямые соединения друг с другом; такого рода сети были преобразующими во многих отношениях, но также позволяли легко отслеживать данные, передаваемые по сети. А поскольку финансовые услуги были ранним вариантом использования компьютерной связи, необходимо было найти способ сохранить информацию в секрете.

IBM лидировала в конце 1960-х годов с помощью метода шифрования, известного как "Люцифер", который в конечном итоге был кодифицирован Национальным бюро стандартов США в качестве первого стандарта

шифрования данных (DES). По мере того как Интернет начал приобретать все большее значение, требовалось все более совершенное шифрование, и сегодня значительная часть данных, передаваемых по всему миру, шифруется с использованием различных методов [3].

Мы уже обсуждали некоторые конкретные области применения криптографии, от сохранения военной тайны до безопасной передачи финансовых данных через Интернет. Однако в целом, как объясняет консультант по кибербезопасности Гэри Кесслер, существуют некоторые общие цели в области кибербезопасности, для достижения которых мы используем криптографию. Используя криптографические методы, специалисты по безопасности могут [1, 6, 7, 9]:

- сохранять конфиденциальность содержимого данных;
- проверять подлинность отправителя и получателя сообщения;
- обеспечение целостности данных, показав, что они не были изменены;
- демонстрировать, что предполагаемый отправитель действительно отправил это сообщение, принцип, известный как «отказ от отказа» [3]

Существует множество используемых криптографических алгоритмов, но в целом их можно разделить на три категории: криптография с секретным ключом, криптография с открытым ключом и хэш-функции.

Криптография с секретным ключом. Шифр Цезаря - это то, что известно, как шифр замещения, потому что каждая буква заменяется другой; тогда другие варианты этого будут заменять блоки букв или целые слова, является отличным примером криптографии с секретным ключом. Но ключ должен оставаться в секрете между ними отправителем и получателем. Криптография с секретным ключом, иногда также называемая симметричным ключом, широко используется для сохранения конфиденциальности данных. Это может быть очень полезно, например, для сохранения конфиденциальности локального жесткого диска; поскольку один и тот же пользователь обычно шифрует и расшифровывает защищенные данные, совместное использование секретного ключа не является проблемой. Криптография с секретным ключом также может

быть использована для обеспечения конфиденциальности сообщений, передаваемых через Интернет; однако, чтобы это произошло успешно, необходимо развернуть следующую форму криптографии в тандеме с ней [4].

Для безопасного функционирования Интернету необходим способ, позволяющий взаимодействующим сторонам устанавливать безопасный канал связи, общаясь только друг с другом по изначально небезопасной сети. Это работает с помощью криптографии с открытым ключом.

В криптографии с открытым ключом, иногда также называемой асимметричным ключом, у каждого участника есть два ключа. Один из них является общедоступным и отправляется всем, с кем сторона желает связаться. Это ключ, используемый для шифрования сообщений. Но другой ключ является закрытым, им никто не делится, и необходимо расшифровать эти сообщения.

Математика того, как вы можете использовать один ключ для шифрования сообщения, а другой - для его расшифровки, гораздо менее понятна, чем то, как работает ключ к шифру Цезаря. Основной принцип, который заставляет процесс работать, заключается в том, что два ключа фактически связаны друг с другом математически, так что легко получить открытый ключ из закрытого ключа, но не наоборот. Например, закрытый ключ может быть двумя очень большими простыми числами, которые вы бы умножили вместе, чтобы получить открытый ключ [1, 8].

Вычисления, необходимые для криптографии с открытым ключом, гораздо более сложны и ресурсоемки, чем те, которые лежат в основе инфраструктуры секретных ключей. Его не нужно использовать его для защиты каждого сообщения, которое отправляете онлайн. Вместо этого обычно происходит то, что одна сторона использует криптографию с открытым ключом для шифрования сообщения, содержащего еще один криптографический ключ. Этот ключ, будучи безопасно передан через небезопасный Интернет, затем станет закрытым ключом, который кодирует гораздо более длительный сеанс связи, зашифрованный с помощью шифрования с секретным ключом.

Таким образом, криптография с открытым ключом способствует обеспечению конфиденциальности. Но эти открытые ключи также являются частью более широкого набора функций, известных как инфраструктура открытых ключей, или PKI. PKI предоставляет способы убедиться в том, что любой данный открытый ключ связан с конкретным лицом или учреждением. Таким образом, сообщение, зашифрованное с помощью открытого ключа, подтверждает личность отправителя, устанавливая аутентификацию и отказ от ответа.

Криптографические алгоритмы с открытым и закрытым ключами включают преобразование открытого текста в зашифрованный текст, а затем обратно в открытый текст. Напротив, хэш-функция - это односторонний алгоритм шифрования: как только открытый текст будет зашифрован, уже не будет возможности его восстановить из результирующего зашифрованного текста (называемого хэшем).

Для любой заданной хэш-функции никакие два открытых текста не будут генерировать один и тот же хэш. Это делает алгоритмы хеширования отличным инструментом для обеспечения целостности данных. Например, сообщение может быть отправлено вместе со своим собственным хэшем. После получения сообщения можно запустить тот же алгоритм хэширования текста сообщения; если созданный хэш отличается от того, который сопровождает сообщение, известно, что сообщение было изменено при передаче [5].

Хеширование также используется для обеспечения конфиденциальности паролей. Хранение паролей в виде открытого текста - это серьезная проблема безопасности, потому что это делает пользователей склонными к краже учетных записей и личных данных в результате утечки. Если вместо этого сохранить хэшированную версию пароля пользователя, хакеры не смогут расшифровать его и использовать в другом месте, даже если им удастся взломать защиту. Когда законный пользователь входит в систему со своим паролем, можно просто хэшировать его и сверять с хэшем, который имеется в файле.

Список литературы:

1. Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриат: под редакцией В. М. Фомичёва. - Москва: Издательство Юрайт, 2019
2. Абалуев Р.Н., Шацкий В.А., Картечина Н.В. Подходы к проектированию модуля web-интерфейса для подсистемы машинного обучения // Наука и Образование. 2022. Т. 5. № 1.
3. Умарзода С.У. Этапы развития криптографии и стеганографии // В сборнике: Права человека в современном мире: концепции, реальность и перспективы. Материалы международной научно-практический конференции, посвящённой Дню прав человека и международному дню борьбы с коррупцией. Душанбе, 2022. С. 404-414.
4. Гущина А.А., Пчелинцева Н.В. Устройства и технологии виртуальной реальности в нашей жизни // Наука и Образование. 2020. Т. 3. № 4. С. 85
5. Криптография будущего - это квантовая криптография // Фотоника. 2020. Т. 14. № 5. С. 412-413.
6. Пчелинцева Н.В. Методические аспекты количественной оценки риска в аграрной сфере производства // Наука и Образование. 2019. № 3. С. 37.
7. Дегтярева А.А., Пчелинцева Н.В, Макова Н.Е. Математические основы криптологии // Наука и Образование. 2020. Т. 3. № 2. С. 46.
8. Иванов С.Г., Доротскар З. Профессиональный соперник криптографии (ПСК): модель разработки игр для изучения криптографии // Международная конференция по мягким вычислениям и измерениям. 2021. Т. 1. С. 312-315.
9. Заболотникова М.А., Картечина О.С., Пчелинцева Н.В Сравнительный анализ хэш-функций // Наука и Образование. 2020. Т. 3. № 2. С. 48.

UDC 003.26(076.1)

ON THE ISSUE OF THE USE OF CRYPTOGRAPHY

Natalia V. Pchelintseva
Senior Lecturer
natas79@mail.ru
Ilya V. Cheprakov
student
i.cheprakov@mail.ru
Anastasia A. Gushchina
student
nastya.gushchina02@mail.ru
Michurinsk State Agrarian University
Michurinsk, Russia

Annotation. The article is devoted to the study of cryptography. It examines the history of cryptography, cryptographic methods, as well as the use of cryptography in the modern world.

Key words: cryptography, network security, hashing, encryption.

Статья поступила в редакцию 29.03.2022; одобрена после рецензирования 11.04.2022; принята к публикации 12.05.2022.

The article was submitted 29.03.2022; approved after reviewing 11.04.2022; accepted for publication 12.05.2022.