Научная статья
Original article
УДК 004.424

ШИФРОВАНИЕ ДАННЫХ

DATA ENCRYPTION

Зацепа Ангелина Ивановна студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), lina.zacepa@bk.ru

Zatsepa Angelina Ivanovna Bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), lina.zacepa@bk.ru

Аннотация. В данной статье описаны различные виды шифрования, используемые для организации информационной безопасности данных пользователей. Информационная безопасность компьютеров и через Интернет обеспечивается различными методами. Простой, но понятный метод защиты — хранить личную информацию только на переносных флэш-накопителях или внешних жестких дисках. Но все самые популярные формы безопасности основаны на шифровании — процессе кодирования информации таким образом, что ее может расшифровать только человек (или компьютер), у которого есть ключ.

Annotation. This article describes various types of encryption used to organize the information security of user data. Information security of computers and via the Internet is provided by various methods. A simple but understandable method of protection is to store personal information only on portable flash drives or external hard drives. But all of the most popular forms of security are based on

encryption, the process of encoding information in such a way that only a person (or computer) who has the key can decrypt it.

Ключевые слова: шифрование, информационная безопасность, стандарт шифрования

Keywords: encryption, information security, encryption standard

Долгий процесс шифрования начался с древних времен, когда не было компьютеров и других современных вычислительных средств, и наши предки использовали их только для замены символов. Процесс расшифровки был долгим и утомительным.

В прежние десятилетия, когда у людей не было проблем с защитой информации своих компьютеризированных систем, шифрование использовалось только государственными органами для облегчения передачи секретной информации во время их общения. В настоящее время шифрование широко применяется для передачи данных, то есть, когда информация передается через сети, устройства Bluetooth, банковские банкоматы и т. д., поскольку этот метод помогает защитить информацию, которую часто трудно физически защитить периодически.

В настоящее время стало чрезвычайно легко манипулировать компьютерными приложениями, продавать и покупать вещи, не пересекая больших расстояний, даже не общаясь друг с другом, но заполняя форму или около того, чтобы общаться с родственниками за границей, кажется жизненно важной задачей в Интернете. , особенно когда вы пытаетесь отправить конфиденциальную личную информацию между сторонами. (Информация о кредитной карте, личные данные, информация о банковском счете, личная переписка и т. д.)

Как упоминается в одной из статей о безопасности данных Питера Сучиу, такие сайты, как «PayPal», используют некоторые из отраслевых методов шифрования для обеспечения высокой безопасности информации о клиентах и данных компании, — говорит представитель PayPal Аманда Пирес. «Система PayPal была создана одним из самых уважаемых криптографов в

отрасли, Максом Левчиным. Макс построил финансовую систему PayPal с нуля, используя высокоуровневое шифрование».

Другой тип шифрования, используемый в основном малыми предприятиями, представляет собой алгоритм ключа, используемый как в криптографии с открытым ключом, так и в криптографии с закрытым ключом. С помощью этого метода пользователь отправляет данные с помощью открытого ключа, который зашифрован, а получатель, который является единственной стороной, которая может расшифровать информацию, использует закрытый ключ. Именно так информация кредитной карты защищена, когда клиент делает онлайн-заказ с вашего веб-сайта. Недостаток этого типа ключа в том, что в случае успешного взлома сайта информация пользователя подвергается опасности.

Особенно, если принять во внимание, что кредитные карты обычно проходят по почте, квитанции об оплате могут быть потеряны с такой четко напечатанной важной информацией, а карты часто крадут, шифрование действительно надежно.

1- Симметричное шифрование

Симметричное шифрование, также известное как шифрование с секретным ключом, выполняется с использованием одного и того же ключа для шифрования и расшифровки информации. Секретный ключ также отправляется получателю вместе с секретным текстом, и с помощью этого ключа выполняется преобразование зашифрованного текста в обычный текст.

DES (стандарт шифрования данных)

Это своего рода стандарт шифрования данных, принятый международными стандартами после того, как он был разработан в IBM в 1970 году. Зашифрованный текст делится на части, и каждая часть шифруется независимо друг от друга, так что шифрование выполняется в определенных блоках. При этом те же операции выполняются над блоками для открытия зашифрованного текста. Этот метод шифрования создает новый ключ, специфичный для этого использования, каждый раз, когда он используется. Он использует 54-битный метод шифрования, несмотря на 64-битные длинные

ключи. Следовательно, беспрепятственная передача информации и секретность были нашей самой важной предпосылкой.

Шифр RC4

Алгоритм шифрования, разработанный в 1987 году, также известен как «Rivest Cipher 4». Его безопасность зависит от использования случайного ключа, хотя обычно используется ключ длиной 5–16 байт. Он воспринимает последовательность, подлежащую шифрованию, как текущую последовательность. Основная логика алгоритма основана на случайной перестановке. В то время как высокая скорость считается одной из его сильных сторон, однократное использование ключа алгоритма является слабой чертой.

Тройной DES (TDES)

Это алгоритм шифрования, разработанный IBM в 1978 году. Он работает с методом шифрования методом шифрования Des 3 раза и с использованием разных ключей. Вот почему он считается эффективной формой шифрования. Два или 3 ключа по 112 или 168 бит исполняются один за другим. Это двунаправленный алгоритм. Данные хранятся в зашифрованном виде и могут быть вызваны в любое время. Но недостатком этого алгоритма является медленная работа. Он используется в интернет-протоколе и банковских транзакциях.

AES (расширенный стандарт шифрования)

Он был разработан в 2000 году двумя бельгийскими криптографами с использованием блочного шифра Rijndael. Для этого алгоритма шифрования используются ключи длиной 128,192 и 256 бит, которые более надежны, чем DES. Данные используются в алгоритме путем их разделения на матрицы (4x4), называемые состояниями. Когда шифрование AES завершено, отдельные циклы выделяются для ключей длиной 128, 192 и 256 бит. Согласно алгоритму DES, он прост в применении и требует меньше памяти, что является одной из его сильных сторон.

иглобрюх

Этот метод шифрования, представляющий собой блочный шифр, разработанный Брюсом Шнайером в 1993 году, представляет собой алгоритм, который можно использовать вместо DES или IDEA. Он использует ключи длиной 32–448 бит. Это бесплатный алгоритм шифрования, доступный бесплатно для всех пользователей.

2- Асимметричное шифрование

В асимметричном шифровании, также известном как шифрование с открытым ключом, есть 2 разных ключа, открытый и закрытый ключи, в отличие от симметричного алгоритма. Ключ расшифровки и шифрования отличается от симметричного ключа шифрования. Ключ к шифру — это открытый ключ, а дешифратор — закрытый ключ. Текст, зашифрованный с помощью открытого ключа, может быть расшифрован только с помощью ключа, принадлежащего этому пользователю. Это делает его намного более эффективным, чем симметричное шифрование.

ЮАР

Он был разработан в 1978 году Роном Ривестом, Ади Шамиром и Леонардом Адлеманом и получил свое название от инициалов людей, которые его разработали. RSA обрабатывает как шифрование, так и дешифрование. Этот алгоритм шифрования можно использовать для обеспечения конфиденциальности и цифровой подписи. Принцип работы основан на модульной арифметике больших чисел. Образуется целое число, образованное произведением двух очень больших простых чисел. Хотя размер номера обеспечивает преимущество с точки зрения надежности, он является одним из недостатков медлительности транзакций. Алгоритм RSA состоит из 3 шагов, известных как генерация ключа, шифрование и дешифрование.

DSA (алгоритм цифровой подписи)

Он был введен в качестве стандарта цифровой подписи Национальным институтом стандартов и технологий (NIST) в 1991 году. DSA, который представляет собой алгоритм шифрования с открытым ключом, такой как RSA, не шифрует с использованием закрытых ключей и не расшифровывает с использованием открытых ключей, в отличие от RSA. Для создания цифровой

подписи, состоящей из 160-битного числа, используется уникальная математическая операция. Поскольку получен хэш сообщения, которое должно быть передано, сообщение, зашифрованное с помощью закрытого ключа, указанного отправителем, создает цифровую подпись. С открытым ключом, ссылающимся на закрытый ключ, это доказывает, что сообщение пришло от правильного получателя.

Диффи-Хеллман

Этот алгоритм, первый алгоритм с открытым ключом, был включен в статью Диффи и Хеллмана 1976 года «Новые направления в криптографии». Он основан на компонентах, которые никогда не передаются напрямую. Целью этого алгоритма является обеспечение безопасной передачи ключа между двумя пользователями и разгадывание зашифрованных сообщений ключа. С помощью этого алгоритма изменение и распределение ключей в алгоритмах симметричного шифрования решается в значительной степени.

Литература

1. Авдошин, С. Дискретная математика. Модулярная алгебра, криптография, кодирование / С. Авдошин. - Москва: СИНТЕГ, 2016. - 260 с.
2. Адаменко, Михаил Основы классической криптологии. Секреты шифров и кодов / Михаил Адаменко. - Москва: Машиностроение, 2014. - 256 с.
3. Ассанж, Джулиан Шифропанки. Свобода и будущее Интернета / Джулиан Ассанж и др. - М.: Азбука-Аттикус, 2014. - 574 с.
4. Бабаш, А. В. История криптографии. Часть I / А.В. Бабаш, Г.П. Шанкин. - М.: Гелиос АРВ, 2002. - 240 с.
5. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2006. - 376 с.
6. Бабенко, Л. К. Современные интеллектуальные пластиковые карты / Л.К. Бабенко, Д.А. Беспалов, О.Б. Макаревич. - М.: Гелиос АРВ, 2015. - 416 с.
7. Байер, Доминик Microsoft ASP .NET. Обеспечение безопасности / Доминик Байер. - М.: Питер, Русская Редакция, 2008. - 430 с.

8. Баричев, С. Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. - Москва: СИНТЕГ, 2011. - 176 с.
9. Введение в криптографию. - М.: ЧеРо, 1998. - 272 с.

References

1. Avdoshin, S. Discrete Mathematics. Modular algebra, cryptography, coding / S. Avdoshin. - Moscow: SINTEG, 2016. - 260 p.
2. Adamenko, Mikhail Fundamentals of classical cryptology. Secrets of ciphers and codes / Mikhail Adamenko. - Moscow: Mashinostroenie, 2014. - 256 p.
3. Assange, Julian Cypherpunks. Freedom and the future of the Internet / Julian Assange et al. - M.: Azbuka-Atticus, 2014. - 574 p.
4. Babash, A. V. History of cryptography. Part I / A.V. Babash, G.P. Shankin. - M.: Helios ARV, 2002. - 240 p.
5. Babenko, L.K. Modern block cipher algorithms and methods of their analysis / L.K. Babenko, E.A. Ischukova. - M.: Helios ARV, 2006. - 376 p.
6. Babenko, L.K. Modern intelligent plastic cards / L.K. Babenko, D.A. Bespalov, O.B. Makarevich. - M.: Helios ARV, 2015. - 416 p.
7. Bayer, Dominic Microsoft ASP .NET. Security / Dominique Bayer. - M.: Peter, Russian Edition, 2008. - 430 p.
8. Barichev, S.G. Fundamentals of modern cryptography / S.G. Barichev, V.V. Goncharov, R.E. Serov. - Moscow: SINTEG, 2011. - 176 p.
9. Introduction to cryptography. - M.: CheRo, 1998. - 272 p.

© Зацепа А.И., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Зацепа А.И. ШИФРОВАНИЕ ДАННЫХ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.