Научная статья
Original article
УДК 004.424

ШИФРОВАНИЕ ДАННЫХ В ИНФОРМАЦИОННОЙ СРЕДЕ

DATA ENCRYPTION IN THE INFORMATION ENVIRONMENT

Гнутова Ольга Викторовна студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), ol.gnutova@mail.ru

Мотуз Николай Сергеевич студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), motuz0nik@yandex.ru

Gnutova Olga Viktorovna bachelor's student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), ol.gnutova@mail.ru

Motuz Nikolay Sergeevich bachelor's student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), motuz0nik@yandex.ru

Аннотация. 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 данной статье описаны методы шифрования и их особенности.

Annotation. The long process of encryption began in ancient times, when there were no computers and other modern computing tools, and our ancestors used them only to replace characters. The decryption process was long and tedious. This article describes encryption methods and their features.

Ключевые слова: шифрование данных, информационная безопасность, сохранность данных

Keywords: data encryption, information security, data safety

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.

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.

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.

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.

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.

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. Бабаш, А.В. Криптографические методы защиты информации (для бакалавров и магистров) / А.В. Бабаш, Е.К. Баранова. - М.: КноРус, 2015. - 224 с.
2. Бабаш, А.В. Криптографические методы защиты информ.: Учебное пособие: Т.1 / А.В. Бабаш. - М.: Риор, 2018. - 48 с.

3. Бабаш, А.В. Криптографические методы защиты информации.Т. 1. Криптографические методы защиты информации: Учебно-методическое пособие / А.В. Бабаш. - М.: ИЦ РИОР, НИЦ Инфра-М, 2013. - 413 с.
4. Баранова, Е.К. Криптографические методы защиты информации. Лабораторный практикум (для бакалавров) / Е.К. Баранова, А.В. Бабаш. - М.: КноРус, 2018. - 288 с.
5. Васильева, И.Н. Криптографические методы защиты информации: Учебник и практикум для академического бакалавриата / И.Н. Васильева. - Люберцы: Юрайт, 2016. - 349 с.
6. Запечников, С.В. Криптографические методы защиты информации: Учебное пособие / С.В. Запечников, О.В. Казарин, А.А. Тарасов. - Люберцы: Юрайт, 2016. - 309 с.
7. Зубов, А.Ю. Криптографические методы защиты информации. Совершенные шифры / А.Ю. Зубов. - М.: Гелиос АРВ, 2005. - 192 с.
8. Рябко, Б. Криптографические методы защиты информации / Б. Рябко. - М.: Горячая линия -Телеком, 2012. - 229 с.
9. Рябко, Б.Я. Криптографические методы защиты информации: Учебное пособие для вузов / Б.Я. Рябко, А.Н. Фионов. - М.: Горячая линия - Телеком , 2014. - 229 с.
10. Рябко, Б.Я. Криптографические методы защиты информации / Б.Я. Рябко, А.Н. Фионов. - М.: ГЛТ, 2013. - 229 с.

References

1. Babash, A.V. Cryptographic methods of information protection (for bachelors and masters) / A.V. Babash, E.K. Baranov. - M.: KnoRus, 2015. - 224 p.
2. Babash, A.V. Cryptographic methods of information protection: Textbook: V.1 / A.V. Babash. - M.: Rior, 2018. - 48 p.
3. Babash, A.V. Cryptographic methods of information protection.T. 1. Cryptographic methods of information protection: Educational and methodological manual / A.V. Babash. - M.: ITs RIOR, NITs Infra-M, 2013. - 413 p.

4. Baranova E.K. Cryptographic methods of information protection. Laboratory workshop (for bachelors) / E.K. Baranova, A.V. Babash. - M.: KnoRus, 2018. - 288 p.
5. Vasilyeva, I.N. Cryptographic methods of information security: Textbook and workshop for academic bachelor's degree / I.N. Vasiliev. - Lyubertsy: Yurayt, 2016. - 349 p.
6. Zapechnikov S.V. Cryptographic methods of information protection: Textbook / S.V. Zapechnikov, O.V. Kazarin, A.A. Tarasov. - Lyubertsy: Yurayt, 2016. - 309 p.
7. Zubov, A.Yu. Cryptographic methods of information protection. Perfect ciphers / A.Yu. Teeth. - M.: Helios ARV, 2005. - 192 p.
8. Ryabko, B. Cryptographic methods of information protection / B. Ryabko. - M.: Hot line -Telecom, 2012. - 229 p.
9. Ryabko, B.Ya. Cryptographic methods of information protection: Textbook for universities / B.Ya. Ryabko, A.N. Fionov. - M.: Hotline -Telecom, 2014. - 229 p.
10. Ryabko, B.Ya. Cryptographic methods of information protection / B.Ya. Ryabko, A.N. Fionov. - M.: GLT, 2013. - 229 p.

© Гнутова О.В., Мотуз Н.С., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Гнутова О.В., Мотуз Н.С. ШИФРОВАНИЕ ДАННЫХ В ИНФОРМАЦИОННОЙ СРЕДЕ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.