Научная статья
УДК 681.3; DOI: 10.61260/2307-7476-2024-1-53-59

ОСОБЕННОСТИ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ

✉**Лабинский Александр Юрьевич.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***labynsciy@yandex.ru***

Аннотация. Рассмотрены особенности криптографических протоколов, используемых для защиты данных, передаваемых по компьютерной сети. В связи с ростом количества сетевых атак актуальность проблемы сетевой безопасности постоянно увеличивается.

В процессах обмена информационными сообщениями между узлами компьютерной сети используются алгоритмы, реализующие различные криптографические преобразования. Описание переменных, операций, выражений и структур, а также набор правил по их использованию в алгоритмах, реализующих криптографические преобразования, содержатся в криптографических протоколах.

Дана классификация криптографических протоколов по различным признакам, рассмотрены свойства безопасности протоколов, характеризующие их стойкость к различным атакам.

Подробно рассмотрен криптографический протокол SSL, который позволяет производить аутентификацию ключей обмена с помощью асимметричного алгоритма шифрования. Кроме того, протокол SSL в целях сохранения конфиденциальности обмена данными регламентирует использование симметричного шифрования данных и в целях проверки целостности данных использование специальных кодов аутентификации. В последнее время наблюдается использование протокола SSL в электронной почте в целях обеспечения конфиденциальности таких процессов обмена данными, как обмен мгновенными сообщениями и передача голосовых сообщений.

Достаточно подробно рассмотрено шифрование и хэширование данных (алгоритмы шифрования MD5, SHA-1, DES). По рассмотренным алгоритмам были разработаны компьютерные модели шифрования данных (алгоритм DES), расчета контрольной суммы текстовых данных (алгоритм CRC32) и подбора символов пароля. Компьютерные модели были реализованы в виде программ для ЭВМ, причем первые две модели в виде консольных программ, а третья – в виде программы с графическим интерфейсом.

Ключевые слова: защита информации, криптографический протокол, хэширование и шифрование данных, алгоритмы и протоколы шифрования, компьютерная модель, программа для ЭВМ

Для цитирования: Лабинский А.Ю. Особенности криптографических протоколов // Природные и техногенные риски (физико-математические и прикладные аспекты). 2024. № 1 (49). С. 53–59. DOI: 10.61260/2307-7476-2024-1-53-59.

Scientific article

FEATURES OF CRYPTOGRAPHIC PROTOCOLS

✉**Labinskiy Alexander Yu.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***labynsciy@yandex.ru***

Abstract. The article considers the features of cryptographic protocols used to protect data transmitted over a computer network. Due to the increase in the number of network attacks, the urgency of the problem of network security is constantly increasing.

The cryptographic protocol contains a description of the structures used and a set of rules governing the use of cryptographic transformations and algorithms in information communication processes between two or more participants.

The article provides classification of cryptographic protocols on various features and considers security properties of protocols, characterizing their resistance to various attacks.

The SSL data encryption protocol, which uses asymmetric cryptography for key authentication, symmetric encryption to preserve confidentiality and authentication codes to verify message integrity, is discussed in detail. The SSL protocol has been widely used in recent years for instant messaging and IP voice transmission in applications such as e-mail, Internet fax and others.

© Санкт-Петербургский университет ГПС МЧС России, 2024

The article deals with encryption and hashing of data (MD5, SHA-1, DES encryption algorithms). Computer models of data encryption (DES algorithm), text data checksum calculation (CRC32 algorithm) and password character matching were developed according to the algorithms considered. The computer models were implemented as computer programs, with the first two models as console programs and the third model as a program with graphical interface.

Keywords: information protection, cryptographic protocol, data hashing and encryption, algorithms and encryption protocols, computer model, computer program

For citation: Labinskiy A.Yu. Features of cryptographic protocols // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty) = Natural and man-made risks (physico-mathematical and applied aspects). 2024. № 1 (49). P. 53–59. DOI: 10.61260/2307-7476-2024-1-53-59.

Введение

Криптографический протокол (Cryptographic protocol) содержит описание переменных, операций, выражений и структур, а также набор правил по их использованию в алгоритмах, реализующих криптографические преобразования, которые используются в целях защиты данных в процессах информационного обмена между клиентами компьютерной сети.

Криптографический протокол выполняет следующие функции:

- формирование ключей;
- обмен ключами;
- аутентификация сторон;
- доказательство целостности и происхождения данных;
- разделение ключей;
- безопасные распределённые вычисления;
- обеспечение конфиденциальности данных;
- обеспечение невозможности отказа;
- обеспечение целостности данных.

Криптографический протокол регламентирует деление информационного процесса на отдельные этапы в виде проходов и циклов, в которых участвует только один клиент. Проходы реализуются в виде отдельных шагов, представляющих собой законченные действия одного участника информационного процесса. Совокупность проходов как результат реализации криптографического протокола называется сессией (сеансом). Таким образом, поведение каждого клиента информационного процесса описывается в криптографическом протоколе.

Сформулируем постановку задачи. Нужно рассмотреть особенности криптографических протоколов, используемых для защиты данных, передаваемых по компьютерной сети.

В связи с ростом количества сетевых атак актуальность проблемы сетевой безопасности постоянно увеличивается, и средствам защиты информации в сети посвящено много работ [1–10].

Новизна исследования, отражающая личный вклад автора, заключается в разработке компьютерных моделей шифрования данных, расчета контрольной суммы текстовых данных и подбора символов пароля, реализованных в виде программ для ЭВМ.

Классификация протоколов

В настоящее время используется деление криптографических протоколов на прикладные и примитивные. Первые используются в практических целях обеспечения безопасности. Вторые, как части прикладного протокола, обеспечивают реализацию одной абстрактной функции обеспечения безопасности.

Классификация криптографических протоколов по различным признакам:

1. По числу участников: двусторонний; трёхсторонний; многосторонний.

2. По числу передаваемых сообщений: интерактивный (взаимный обмен) и не интерактивный (однократная передача).

3. По назначению: с аутентификацией и без аутентификации источника.

4. По цифровой подписи: индивидуальная и групповая.

5. По обмену сообщениями: обычная конфиденциальная и конфиденциальная широковещательная передача сообщений.

6. По распределению ключей: предварительная передача ключа (обмен ключами) и открытое распределение ключей.

7. По типу криптографических систем: симметричные, асимметричные и смешанные системы.

8. По способу функционирования: интерактивный и не интерактивный; однопроходной / двух- / трёх- и т.д. проходной; протокол с посредником.

Свойства безопасности протокола

Свойства протоколов, характеризующие их стойкость к различным атакам, формулируют как цели (goals) или требования к протоколам. Под свойствами безопасности в документах международной организации IETF в настоящее время понимаются следующие 20 целей, сгруппированные в 10 групп:

1. Аутентификация: G1(субъекта), G2(сообщения), G3(защита от повтора).
2. Аутентификация рассылки: G4(получателя), G5(источника).
3. Авторизация: G6(доверенной третьей стороны).
4. Генерация ключа: G7(аутентификация), G8(правильность ключа), G9(защищенность), G10(новый ключ), G11(безопасность).
5. Конфиденциальность: G12.
6. Анонимность: G13(несвязываемость), G14(защита от участников).
7. G15(защита от атак DoS – «отказ в обслуживании»).
8. G16(инвариантность отправителя).
9. Невозможность отказа от ранее совершённых действий: G17(подотчетность), G18(доказательство источника), G19(доказательство получателя).
10. G20(безопасное временное свойство).

Протоколы шифрования данных

Протоколом, обеспечивающим безопасный обмен информацией, является протокол SSL (Secure Sockets Layer). Данный протокол регламентирует использование кодов проверки подлинности в целях обеспечения защищенности сообщений, симметричное шифрование в целях обеспечения конфиденциальности процесса обмена данными и асимметричное шифрование в целях проверки подлинности ключей шифрования данных.

Весьма продолжительное время протокол SSL использовался в процессах обмена текстовой и голосовой информацией по электронной почте и в рамках других услуг сети Интернет. Однако затем появились сообщения об уязвимости этого протокола, что потребовало его замены на протокол TLS (Transport Layer Security).

Когда фирма Netscape Communications разработала веб-браузер Netscape Navigator, она включила в него протокол HTTPS, созданный на базе протокола SSL. Затем, в январе 1999 г., на базе протокола SSL 3.0 был разработан протокол TLS с целью последующей замены (при необходимости) на него протокола SSL. В 2018 г. протокол TLS 1.3 был признан стандартом.

Особенности шифрования. Существует два основных способа шифрования данных: симметричное (общий секретный ключ) и асимметричное (пара-открытый/приватный ключ). SSL использует как асимметричную, так и симметричную криптографию. Алгоритмы шифрования, использующиеся в SSL:

1. Для обмена ключами и проверки их подлинности применяются: RSA, Diffie-Hellman, ECDH, SRP, PSK.
2. Для аутентификации: RSA, DSA, ECDSA.

3. Для симметричного шифрования: RC2, RC4, IDEA, DES, Triple DES.
4. Для хеш-функций: SHA, MD5, MD4 и MD2.

Для проверки подлинности клиента и сервера по протоколу SSL применяется шифрование с открытым ключом. Для шифрования большого объема данных в протоколе SSL используется симметричное шифрование.

Хеширование. Для проверки целостности передачи данных используются хеш-функции, с помощью которых осуществляется сжатие передаваемых данных. Алгоритмы реализации хеш-функций разнообразны и обеспечивают получение хеш-значений различной длины: 128-битных (алгоритм MD5), 160-битных (алгоритмы SHA-1, SHA-2 и SHA-3). Сокращение MD означает Message Digest, а SHA – Secure Hash Algorithm.

Применение. При проектировании приложений SSL реализуется под любым другим протоколом прикладного уровня, таким как HTTP, FTP, SMTP, NNTP и XMPP. Использование протокола SSL в веб-сайтах привело к формированию протокола HTTPS (Hypertext Transfer Protocol Secure), поддерживающего шифрование.

Браузеры. По состоянию на начало 2017 г. основные веб-браузеры, поддерживающие протоколы SSL/TLS: Chrome (Android, iOS, Linux, Mac OS X, Windows), Firefox (Linux, Mac OS X, Windows), IE (Windows), Opera (Linux, Mac OS X, Windows), Safari (Mac OS X, Windows).

Шифрование и хэширование данных

Шифрование – изменение передаваемых данных, обеспечивающее искажение их содержимого. Хэширование – одностороннее математическое преобразование, создающее дайджест (хэш-код) сообщения или данных. Хэш-функция – функция, используемая для получения дайджеста.

Алгоритм шифрования MD5. Хэш-алгоритм MD5 (Message Digest) предназначен для создания дайджеста сообщения произвольной длины, в результате чего получается дайджест длиной 128 бит. Алгоритм реализуется в виде нескольких шагов (этапов). На первых двух этапах создается сообщение, длина которого кратна 512 битам (сообщение равно последовательности 512-битовых блоков). На следующих шагах производится обработка последовательности 512-битовых блоков с помощью четырех циклов по 16 операторов. На каждом цикле используется своя логическая функция: fF, fG, fH и fK. Каждая функция имеет общую структуру:

$$fF(X,Y,Z) = (X \wedge Y) \vee ((\neg X) \wedge); \; fG(X,Y,Z) = (X \wedge Y) \vee (Y \wedge (\neg Z));$$
$$fH(X,Y,Z) = X \oplus Y \oplus Z; \; fK(X,Y,Z) = Y \oplus (X \wedge (\neg Z)),$$

где $\wedge$ – побитовая операция И; $\vee$ – побитовая операция ИЛИ; $\neg$ – побитовая операция НЕ; $\oplus$ – побитовая операция Исключающее ИЛИ (XOR).

Для указанных побитовых операций можно составить таблицу истинности:

A	B	$\neg$ A	A $\wedge$ B	A $\vee$ B	A $\oplus$ B
Л	Л	И	Л	Л	И
Л	И	И	Л	И	Л
И	Л	Л	Л	И	Л
И	И	Л	И	И	Л

Примечание: И – истина (1); Л – ложь (0)

Алгоритм шифрования SHA-1. Безопасный хэш-алгоритм SHA (Secure Hash Algorithm) получает на входе сообщение максимальной длины 2^{64} бит и создает дайджест сообщения длиной 160 бит. Как и в MD5 на первых двух этапах шифрования создается сообщение, длина которого кратна 512 битам. На следующих шагах производится обработка последовательности 512-битовых блоков с помощью константы K[t], которая принимает четыре различных значения: от 0 до 19, от 20 до 39, от 40 до 59 и от 60 до 79. Для каждого диапазона значений K[t] используется логическая функция ft(B, C, D):

– $0 \le K[t] \le 19$: $ft(B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$;
– $20 \le K[t] \le 39$: $ft(B, C, D) = B \oplus C \oplus D$;
– $40 \le K[t] \le 59$: $ft(B, C, D) = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$;
– $60 \le K[t] \le 79$: $ft(B, C, D) = B \oplus C \oplus D$.

Алгоритм шифрования DES. Хэш-алгоритм DES (Data Encryption Standard) шифрует данные блоками по 64 бита. DES является симметричным алгоритмом: для шифрования и дешифрования используются одинаковые алгоритм и ключ. Длина ключа равна 56 бит. Шифрование состоит из 16 этапов. На каждом этапе биты ключа сдвигаются, а затем из 56 битов ключа выбираются 48 бит.

Алгоритм вычисления контрольной суммы пакета данных CRC32. Циклический алгоритм вычисления контрольной суммы пакета данных CRC (Cyclic Redundancy Check – циклический избыточный код) используется для проверки целостности данных, передаваемых по сети. Вместе с пакетом данных отправляется контрольная сумма данных, вычисленная с помощью CRC32. Если отправленная контрольная сумма и вычисленная получателем сумма не совпадают, то следует запросить повторную передачу пакета данных.

Компьютерное моделирование

По рассмотренным выше алгоритмам были разработаны компьютерные модели шифрования данных (алгоритм DES), расчета контрольной суммы текстовых данных (алгоритм CRC32) и подбора символов пароля. Первые две модели реализованы в виде консольных программ, а третья – в виде программы с графическим интерфейсом.

Интерфейс программы шифрования данных представлен на рис. 1.

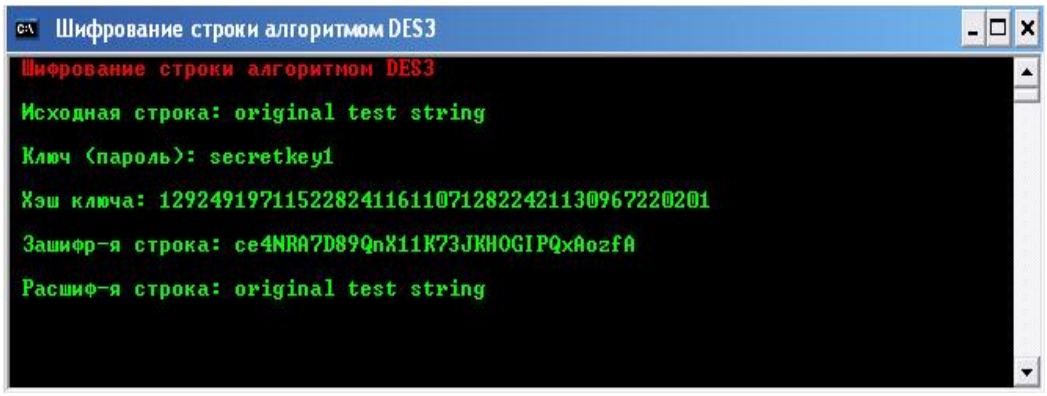

Рис. 1. **Консольная программа шифрования по алгоритму DES3**

В окне вывода представлены: исходная строка текста, ключ (пароль) шифрования, хэш-ключа, зашифрованная строка и расшифрованная строка.

Интерфейс программы расчета контрольной суммы представлен на рис. 2.

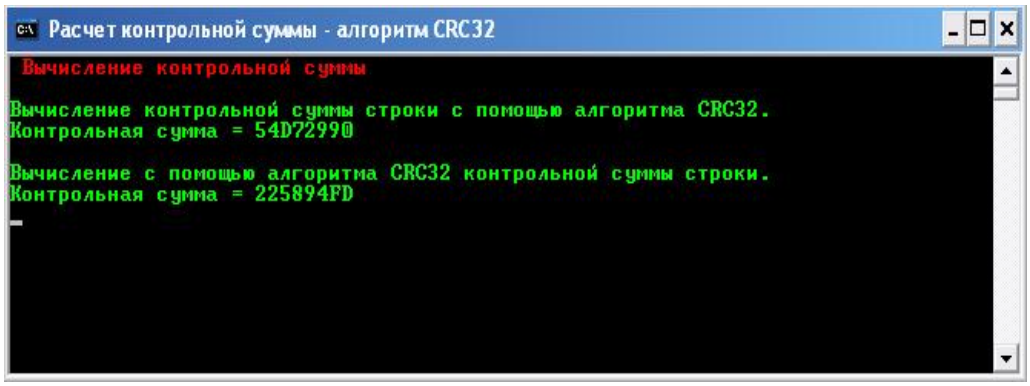

Рис. 2. **Программа расчета контрольной суммы по алгоритму CRC32**

В окне вывода представлены: исходная строка текста, контрольная сумма исходной строки, строка текста с переставленными словами и контрольная сумма строки с переставленными словами.

Интерфейс программы генерации пароля представлен на рис. 3.

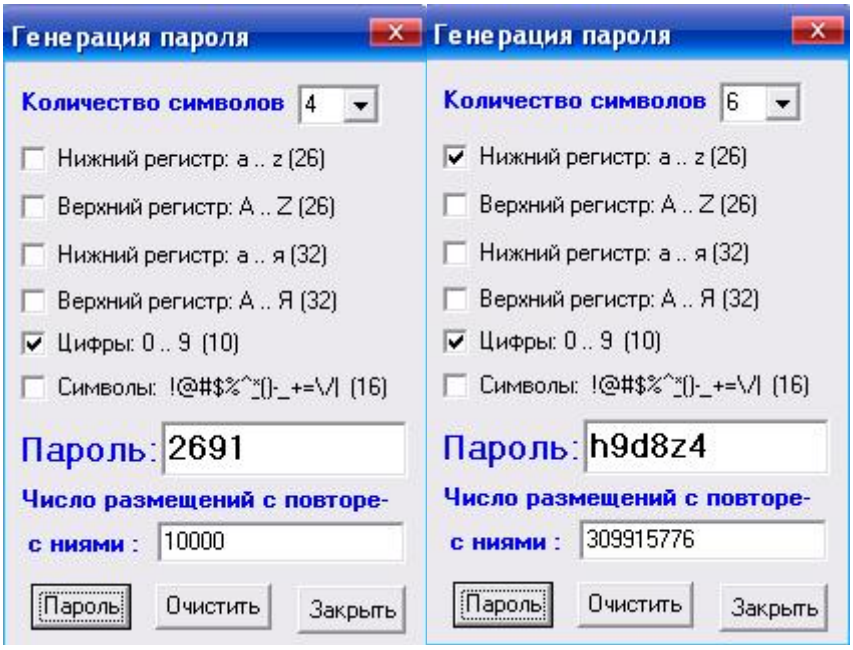

Рис. 3. **Программа генерации пароля**

Программа позволяет генерировать пароль с количеством символов от 4 до 10, состоящий по выбору из символов русского и латинского алфавита (нижнего и верхнего регистра), цифр и других символов. При выводе символов пароля указывается число комбинаций при подборе пароля злоумышленником. В левом окне количество символов пароля равно 4, используются только цифры. В этом случае число комбинаций подбора не более 10 тыс. В правом окне количество символов пароля равно 6, используются буквы и цифры. В этом случае число комбинаций подбора превышает 300 млн.

Вывод

Рассмотрены назначение и классификация криптографических протоколов, подробно – свойства безопасности криптографических протоколов.

Описаны протоколы шифрования данных SSL и TLS, а также алгоритмы шифрования MD5, SHA-1, DES и алгоритм CRC32 расчета контрольной суммы пакета текстовых данных с целью проверки целостности данных, передаваемых по сети.

Научная новизна исследования, отражающая личный вклад автора, заключается в создании автором компьютерных моделей, реализованных в виде консольных программ и программ с графическим интерфейсом (рис. 1–3).

Список источников

1. Черёмушкин А.В. Криптографические протоколы: основные свойства и уязвимости // Прикладная дискретная математика. 2009. № 2. С. 115–150.

2. Защита информации: учеб. пособие / С.М. Владимиров [и др.]. М.: МФТИ, 2013.

3. Введение в криптографию / В.В. Ященко [и др.]. М.: МЦНМО, 2012.

4. Шаханова М.В., Варлатая С.К. Криптографические методы и средства обеспечения информационной безопасности: учеб. пособие. Дальневосточный ГТУ: ООО «Проспект», 2015.

5. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 2006.

6. Ronald L. Rivest Adi Shamir. How to Expose an Eavesdropper (англ.) // Communications of the ACM. 1984. Vol. 27. № 4. P. 393–395.
7. Roger M. Needham, Michael D. Schroeder. Using encryption for authentication in large networks of computers // Communications of the ACM. 1978. Vol. 21. № 12. P. 993–999.
8. Bruce Schneier. Applied Cryptography. John Wiley & Sons, 2006.
9. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2. RTFM, Inc., 2008.
10. Karlton P. The Secure Sockets Layer (SSL) Protocol Version 3.0. RTFM, Inc., 2011.

References

1. Cheryomushkin A.V. Kriptograficheskie protokoly: osnovnye svojstva i uyazvimosti // Prikladnaya diskretnaya matematika. 2009. № 2. S. 115–150.
2. Zashchita informacii: ucheb. posobie / S.M. Vladimirov [i dr.]. M.: MFTI, 2013.
3. Vvedenie v kriptografiyu / V.V. Yashchenko [i dr.]. M.: MCNMO, 2012.
4. Shahanova M.V., Varlataya S.K. Kriptograficheskie metody i sredstva obespecheniya informacionnoj bezopasnosti: ucheb. posobie. Dal'nevostochnyj GTU: OOO «Prospekt», 2015.
5. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 2006.
6. Ronald L. Rivest Adi Shamir. How to Expose an Eavesdropper (angl.) // Communications of the ACM. 1984. Vol. 27. № 4. P. 393–395.
7. Roger M. Needham, Michael D. Schroeder. Using encryption for authentication in large networks of computers // Communications of the ACM. 1978. Vol. 21. № 12. P. 993–999.
8. Bruce Schneier. Applied Cryptography. John Wiley & Sons, 2006.
9. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2. RTFM, Inc., 2008.
10. Karlton P. The Secure Sockets Layer (SSL) Protocol Version 3.0. RTFM, Inc., 2011.

Информация о статье:
Поступила в редакцию: 03.02.2024
Принята к публикации: 29.02.2024
The information about article:
Article was received by the editorial office: 03.02.2024
Accepted for publication: 29.02.2024

Информация об авторах:
Лабинский Александр Юрьевич, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат технических наук, доцент, e-mail: labynsciy@yandex.ru, https://orcid.org/0000-0001-2735-4189, SPIN-код: 8338-4230
Information about the authors:
Labinsky Alexander Yu., associate professor of the department of applied mathematics and information technologies of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of technical sciences, associate professor, e-mail: labynsciy@yandex.ru, https://orcid.org/0000-0001-2735-4189, SPIN: 8338-4230