Современная наука и инновации. 2024. № 4. С. 22-28.
ТЕХНИЧЕСКИЕ НАУКИ
ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Modern Science and Innovations. 2024;(4):22-28.
TECHNICAL SCIENCE
INFORMATICS, COMPUTER ENGINEERING AND MANAGEMENT

Научная статья
УДК 519.23
https://doi.org/10.37493/2307-910X.2024.4.2

Разработка системы криптографической защиты информации, передаваемой по открытым каналам связи

Владимир Феохарович Антонов

Северо-Кавказский федеральный университет, Пятигорский институт (филиал), г. Пятигорск, Россия
antonovpgtu@mail.ru

Аннотация. Введение. *Объектом исследования в данной работе является система защиты информации. Целью данного исследования является разработка системы криптографической защиты служебной информации, передаваемой по открытым каналам связи по протоколу TCP/IP между TCP сервером и клиентом в концепции системы информационной защиты информации. В работе приведены примеры различных алгоритмов криптографической защиты информации, при передаче информации по открытым каналам связи.* ***Материалы и методы.*** *В предлагаемой статье рассматриваются специальные алгоритмы шифрования: DES, Triple DES, Rijndael, RC2 и RSA. Выбор нужного алгоритма в конкретном сеансе работы осуществляется выбором из раскрывающегося списка. После указания вида алгоритма следует выбрать в следующем раскрывающемся списке длину ключа. Наличие нескольких алгоритмов шифрования и наличие разных длин ключей позволит значительно улучшить криптографическую стойкость разрабатываемо системы, поскольку при перехвате пересылаемого сообщения алгоритм и длина ключа может оказываться произвольным, что затруднит несанкционированную дешифрацию сообщений.* ***Результаты и обсуждения.*** *Мировой опыт показывает, что успехи в области защиты информации во многом зависят от степени использования новейших технологий, реализующие большинство используемых открытых криптографических алгоритмов. Огромное количество организации тратят большие средства для обеспечения безопасности информации, передаваемой как вне, так и внутри организации. Причем во втором случае, как правило, уделяется меньше внимания. А ведь это актуальная проблема на сегодняшний день и для решения ее необходимо программный продукт. Конечно, проблемы защиты информации не могут быть решены только разработкой программных продуктов, т.к. человеческий фактор остается уязвимым местом любой системы.* ***Заключение.*** *Решения, которые предлагаются по результатам выполненной работы в рамках рассматриваемой статьи, дадут возможность пользователям передавать и принимать информацию по открытым каналам связи, как внутри организации, так и вне, обеспечивая тем самым защиту информации от несанкционированного доступа и изменения.*

Ключевые слова: алгоритм, шифрование, симметричный и ассиметричный алгоритмы, зарытый и секретный ключи

Для цитирования: *Антонов В. Ф. Разработка системы криптографической защиты информации, передаваемой по открытым каналам связи // Современная наука и инновации. 2024. № 4. С. 22-28. https://doi.org/10.37493/2307-910X.2024.4.2*

Research article

Development of a cryptographic protection system for information transmitted over open communication channels

Vladimir F. Antonov

North-Caucasus Federal University, Pyatigorsk Institute (branch), Pyatigorsk, Russia
antonovpgtu@mail.ru

Abstract. Introduction. *The object of the study in this paper is the information security system. The purpose of this study is to develop a system of cryptographic protection of service information transmitted over open communication channels using the TCP/IP protocol between the TCP server and the client in the concept of an information security system. The paper provides examples of various algorithms for cryptographic protection of information when transmitting information over open communication channels.* ***Materials and methods.*** *This article discusses special encryption algorithms: DES, Triple DES, Rijndael, RC2 and RSA. The selection of the desired algorithm in a specific work session is carried out by selecting from the drop-down list. After specifying the type of algorithm, you should select the key length in the next drop-down list. The presence of several encryption algorithms and the presence of different key lengths will significantly improve the cryptographic strength of the system being developed, since when a sent message is intercepted, the algorithm and key length can be arbitrary, which will make it difficult for unauthorized decryption of messages.* ***Results and discussions.*** *World experience shows that success in the field of information security largely depends on the degree of use of the latest technologies that implement the majority of open cryptographic algorithms used. A huge number of organizations spend large amounts of money to ensure the security of information transmitted both outside and within the organization. Moreover, in the second case, as a rule, less attention is paid. But this is a pressing problem today and to solve it you need a software product. Of course, information security problems cannot be solved only by developing software products, because the human factor remains the weak point of any system.* ***Conclusion.*** *The solutions that are proposed based on the results of the work performed within the framework of this article will enable users to transmit and receive information through open communication channels, both within the organization and outside, thereby ensuring the protection of information from unauthorized access and modification.*

Keywords: algorithm, encryption, symmetric and asymmetric algorithms, private and secret keys

For citation: *Antonov VF. Development of a cryptographic protection system for information transmitted over open communication channels. Modern Science and Innovations. 2024;(4):22-28. https://doi.org/10.37493/2307-910X.2024.4.2*

Введение. Система защиты информации предназначена для выполнения шифрования файлов, обладающих коммерческой тайной и передачи их по сети. Система защиты информации должна производить идентификацию пользователей систем по их паролю, для чего следует предусмотреть соответствующий пункт меню, вызывающий окно идентификации пользователя. Для каждого пользователя предусмотрено сохранение его открытого ключа, для облегчения работы с системой и ускорения ввода исходных данных.

Система защиты информации должна работать как в режиме сервера, так и клиента, то есть должна осуществлять как шифрование и передачу файлов по каналам связи, так и их прием и дешифрование. Наиболее просто реализовать эти функции введя пункт меню «Передача файлов», выбор которого позволит загрузить форму, содержащую кнопки: «Прием» и «Отправка», при нажатии на которые будут выполняться необходимые для реализации данных функций действия.

Небольшие текстовые файлы, а также ключи симметричных алгоритмов целесообразно шифровать методом RSA как более надежным с точки зрения криптостойкости. Большие же файлы (более 1 Mb) шифровать следует только симметричными алгоритмами, так как алгоритм RSA является весьма медленным алгоритмом.

Материалы и методы исследований. При использовании ассиметричного алгоритма RSA могут использоваться механизмы цифровой подписи. Два ключа шифрования (секретный и публичный) и два ключа подписи (секретный и публичный)

после создания могут (и должны) сохраняться в разные файлы, из которых их можно легко подгружать для использования в программе.

Открытый ключ шифрования распространяется свободно и может быть использован только для шифрования файлов. Секретный ключ шифрования используется только хозяином-создателем для дешифрации файла зашифрованного с помощью открытого ключа. Секретный ключ подписи используется только хозяином-создателем для подписи сообщения (шифрованного файла). Проверяется подпись с помощью открытого ключа, который распространяется в виде отдельного файла и подгружается в программу перед дешифрацией.

Поскольку использование цифровой подписи, хеширование, а также создание ключей подписи и ключей шифрования используются только для алгоритма RSA, то данными видами настроек интерфейс лучше не перегружать, а выделить эту группу настроек в отдельный пункт меню «Настройки RSA».

Таким образом, учитывая вышеизложенное разрабатываемая система зашиты информации должна содержать главное окно, содержащее строку меню с пунктами: «Настройки RSA», «Передача файлов» и «Идентификация пользователя». Примерный вид главной формы с учетом вышеизложенного представлен на рис. 1.

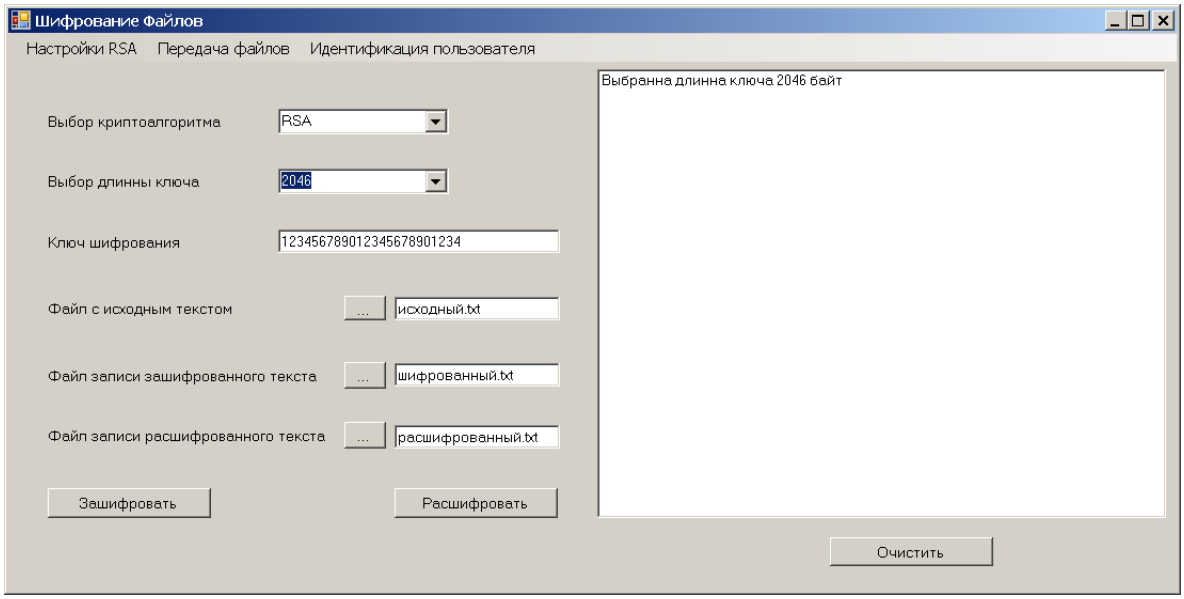

Рисунок 1 – Внешний вид главной формы системы защиты информации / Figure 1 – External view of the main form of the information security system

Как уже отмечалось, выбор пункта меню «Идентификация пользователя» должно загружать соответствующую форму, позволяющую вводить пароль для каждого конкретно пользователя системы защиты информации и кнопку «Вход», подтверждающую введенный пользователем пароль. Примерный вид формы представлен на рис. 2.

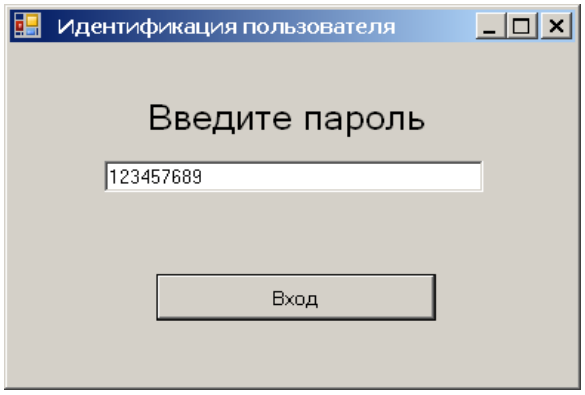

Рисунок 2 – Вид окна «Идентификация пользователя» / Figure 2 – View of the "User Identification" window

Выбор пункта меню «Передача файлов» в свою очередь должен вызывать загрузку окна обмена файлов. В данном диалоговом окне следует предусмотреть поля для ввода IP адреса и порта, а также кнопки «Отправка» и «Прием», инициирующие начало выполнения соответствующих действий. Примерный вид формы обмена файлами представлен на рис.3.

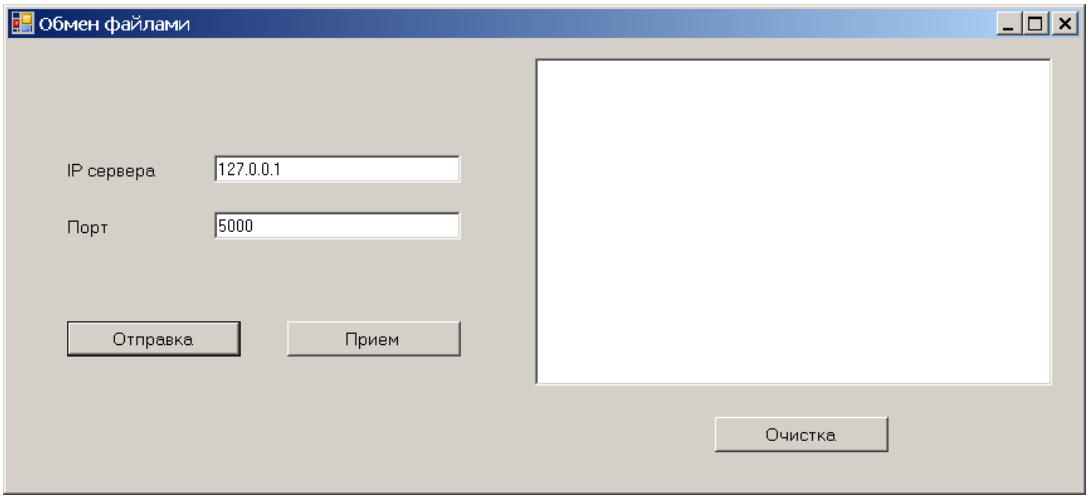

Рисунок 3 – Вид окна «Обмен файлами» / Figure 3 – View of the "File Exchange" window

Результаты исследований и их обсуждение. Разработанная система защиты информации будет содержать три окна, одно загружается после загрузки самой программы, а два других вызываются через соответствующие пункты меню.

Пункты меню «Передача файлов» и «Идентификация пользователя» содержит по одному пункту, которые вызывают загрузку соответствующих диалоговых окон. Структура пункта меню «Настройки RSA» более сложная поскольку он содержит дополнительные вложенные пункты, содержание которых уже было намечено ранее.

Для реализации процедуры шифрования передаваемого файла, разработан специальный пункт меню «Настройки RSA», который содержит следующие подпункты (см. рис. 4.):

– алгоритм подписи;
– хеш;
– ключи подписи;
– ключи шифрования.

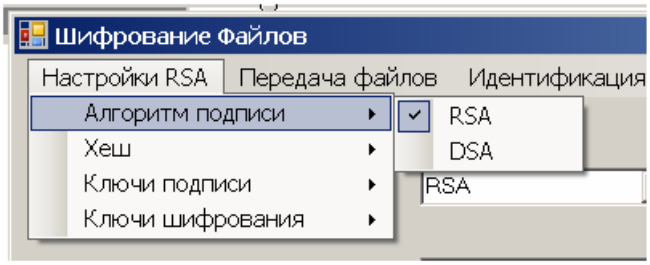

Рисунок 4 – Структура пункта меню «Настройки RSA – Алгоритм подписи» / Figure 4 – Structure of the menu item “RSA Settings – Signature Algorithm”

В данном пункте пользователь системы защиты информации может выбрать в случае использования алгоритма шифрования RSA вариант алгоритма для создания цифровой подписи (предусмотрены два варианта: RSA или DSA).

А при выборе в качестве алгоритма подписи - RSA, в свою очередь может быть выбран алгоритм хеширования (MD5 или SHA-1), как показано на рис. 5.

При выборе в качестве алгоритма создания цифровой подписи -DSA используется только хеширование SHA-1 (по умолчанию) и возможность выбора способа хеширования отключается.

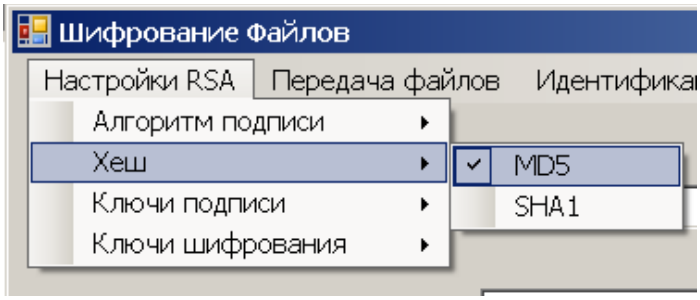

Рисунок 5 – Структура пункта меню «Настройки RSA – Хеш» / Figure 5 – Structure of the menu item "RSA Settings - Hash"

Создание ключей подписи (публичного и секретного) производится через соответствующие подпункты меню: «Настройки RSA – Ключи подписи» и «Настройки RSA – Ключи шифрования» (см. рис. 6 и 7).

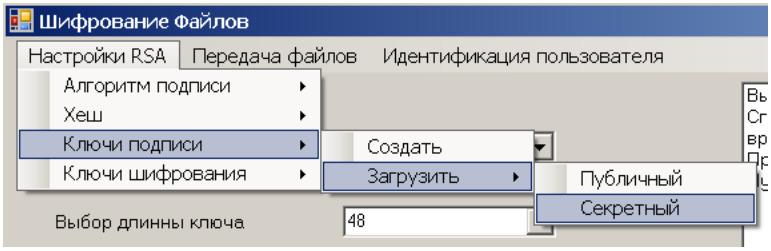

Рисунок 6 – Структура пункта меню «Настройки RSA – Ключи подписи» / Figure 6 – Structure of the menu item “RSA Settings – Signature Keys”

Секретные ключи шифруются с помощью пароля (поле пароль) для обеспечения дополнительной защиты. Секретные файлы должны храниться у их создателя и никому не передаваться. Шифрование секретных файлов паролем не позволит злоумышленнику завладевшему секретным файлом дешифровать сообщение (или соответственно подделать подпись) так как для этого нужен еще и пароль для дешифровки ключа.

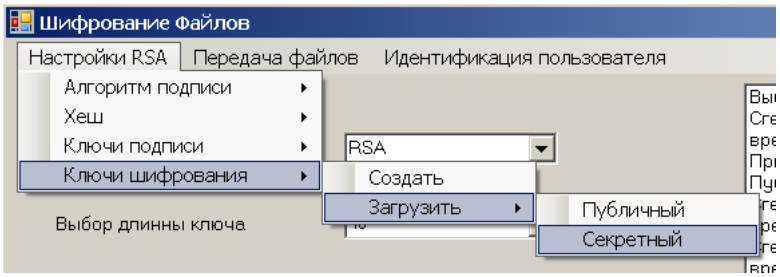

Рисунок 7 – Структура пункта меню «Настройки RSA – Ключи шифрования» / Рисунок 7 – Структура пункта меню «Настройки RSA – Ключи шифрования»

Максимальная длина этого пароля 32 символа (алгоритм AES-32), при введении большей длины пароля лишние символы будут отсекаться автоматически.

Заключение. По результатам тестирования следует сделать вывод, что при использовании ассиметричного алгоритма шифрования, работа с файлами большого объема нецелесообразна по объективным причинам. В случае использования криптографически стойких ключей длиной 1024 байта, комфортно можно работать с файлами объемом до 0,5 мегабайт. Этого обычно достаточно для работы с текстовыми документами.

Следует отметить, что при использовании ассиметричного алгоритма (RSA) скорость работы практически полностью зависит от процессора (загрузка процессора в

диспетчере задач при шифровании, дешифровки или генерации ключей составляет 100%). Это обусловлено большим объемом сложных вычислений в процессе работы. Очевидно, что при использовании мощных современных процессоров, время, потраченное на операции, может в разы отличаться от приведенных данных, однако влияния на сделанные выводы это не оказывает.

При использовании симметричных алгоритмов и работе с файлами большого объема критической характеристикой может оказаться скорость доступа к данным (загрузка процессора в диспетчере задач 30-60%). По всей видимости, современный процессор в состоянии провести необходимые вычисления с большей скоростью, чем эти данные будут считаны/записаны.

Во всех случаях производительность не зависит от объема оперативной памяти. Независимо от выполняемой операции, используемого алгоритма шифрования и размера обрабатываемых файлов количество занимаемой программой оперативной памяти незначительно (от 1Мб до 15 Мб).

Таким образом разработанная система криптографической защиты информации, передаваемой по открытым каналам связи может использована в качестве программного средства для шифрования и дешифрования информации.

ЛИТЕРАТУРА

1. Тарасов А. М. Криптография и электронная цифровая подпись: правовые и организационные аспекты // Вестник академии права и управления. 2011. № 22. С. 9–19.
2. Голубев Е. А., Емельянов Г. В. Стеганография как одно из направлений обеспечения информационной безопасности // T-Comm –Телекоммуникации и Транспорт. 2009. № 8. С. 185–186.
3. Бабенко Л. К., Ищукова Е. А. Современные алгоритмы блочного шифрования и методы их анализа. М.: Гелиос АРВ, 2006.
4. Корченко А. Г. Построение систем защиты информации на нечетких множествах. М.: МК-Пресс, 2006.
5. Вельшенбах М. Криптография на Си и C++ в действии (+CD-ROM). М.: Триумф, 2004.
6. Антонов В. Ф., Мамедов Р. А. Характеристики терминологических единиц измерения распределенных атак на отказ в обслуживании канала. Сборник научных трудов по материалам XIX международной научной конференции «Тенденции развития науки и образования», Пятигорск: ИСТиД (СКФУ), НИЦ «Л-Журнал», 2016. Часть 3. 32 с.

REFERENCES

1. Tarasov AM. Cryptography and electronic digital signature: legal and organizational aspects. Bulletin of the Academy of Law and Management. 2011;(22):9-19.
2. Golubev EA, Emelianov GV. Steganography as one of the directions of ensuring information security. T-Comm – Telecommunications and Transport. 2009;(8):185-186.
3. Babenko LK, Ishchukova EA. Modern algorithms of block encryption and methods of their analysis. Moscow: Gelios ARV; 2006.
4. Korchenko AG. Construction of information security systems on fuzzy sets. Moscow: MK-Press; 2006.
5. Welshenbach M. Cryptography in C and C++ in action (+ CD-ROM). Moscow: Triumph; 2004.
6. Antonov VF, Mamedov RA. Characteristics of terminological units of measurement of distributed attacks on denial of service of the channel. Collection of scientific papers based on the materials of the XIX international scientific conference "Trends in the development of science and education", Pyatigorsk: ISTiD (SKFU), NIC "L-Journal"; 2016. Part 3. 32 p.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Владимир Феохарович Антонов – кандидат технических наук, доцент кафедры систем управления и информационных технологий, Пятигорский институт (филиал), Северо-Кавказский федеральный университет, antonovpgtu@mail.ru

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.

Статья поступила в редакцию: 15.10.2024;
одобрена после рецензирования: 20.11.2024;
принята к публикации: 10.12.2024.

INFORMATION ABOUT THE AUTHOR

Vladimir F. Antonov – Cand. Sci. (Techn.), Associate Professor of the Department of Management Systems and Information Technologies, Pyatigorsk Institute (branch), North-Caucasus Federal University, antonovpgtu@mail.ru

Conflict of interest: the author declares no conflicts of interests.

The article was submitted: 15.10.2024;
approved after reviewing: 20.11.2024;
accepted for publication: 10.12.2024.