Т. 12. №6 2026
https://doi.org/10.33619/2414-2948/127

УДК 004.056.55 https://doi.org/10.33619/2414-2948/127/27

ЗАЩИТА ДАННЫХ IoT-УСТРОЙСТВ АЛГОРИТМОМ RSA

©***Маликова З. Т.***, *ORCID: 0000-0002-7490-4884, SPIN-код: 5381-8170, Ошский технологический университет им. М. М. Адышева, г. Ош, Кыргызстан, zirek.malicova@mail.ru*
©***Закирова Д. А.***, *ORCID: 0009-0002-6723-690X, SPIN-код: 4158-0909, Ошский технологический университет им. М. М. Адышева, г. Ош, Кыргызстан, zakirovadinara03@gmail.com*
©***Маткаликов А. М.***, *Ошский технологический университет им. М. М. Адышева, г. Ош, Кыргызстан*

PROTECTING IOT DEVICE DATA WITH THE RSA ALGORITHM

©***Malikova Z.***, *ORCID: 0000-0002-7490-4884, SPIN-code: 5381-8170, Osh Technological University named after M. Adyshev, Osh, Kyrgyzstan, zirek.malicova@mail.ru*
©***Zakirova D.***, *ORCID: 0009-0002-6723-690X, SPIN-code: 4158-0909, Osh Technological University named after M. Adyshev, Osh, Kyrgyzstan, zakirovadinara03@gmail.com*
©***Matkalikov A.***, *Osh Technological University named after M. Adyshev, Osh, Kyrgyzstan*

Аннотация. Данное исследование посвящена проблеме исследованию методов защиты IoT устройств с использованием алгоритма RSA. Актуальность темы обусловлена широким распространением технологий интернет вещей и необходимостью обеспечения безопасности передаваемой информации в условиях открытых сетей. Цель исследования — изучение особенности применения алгоритма RSA для защиты данных в IoT-устройствах и оценить его эффективность его применения. Результат исследования – реализована модель защищенной передачи данных с использованием языка Python. Предложенная модель выглядит как мессенджер, где ведут переписку два человека. Каждое слово или каждая буква автоматически шифруется и передается отправителем. Шифрованный вариант данных отражается в нижней части интерефейса программы. Установлено, что алгоритм RSA обеспечивает высокий уровень защиты данных, однако его применение в IoT-системах ограничено вычислительными ресурсами устройств. Рекомендуется использование гибридных криптографических схем.

Abstract. This study examines methods for protecting IoT devices using the RSA algorithm. The topic is relevant due to the widespread adoption of Internet of Things technologies and the need to ensure the security of transmitted information in open networks. The aim of the study is to examine the specifics of using the RSA algorithm to protect data in IoT devices and to evaluate its effectiveness. The study resulted in the implementation of a secure data transfer model using Python. The proposed model resembles a messenger in which two people communicate. Each word or letter is automatically encrypted and transmitted by the sender. The encrypted version of the data is displayed at the bottom of the program interface. The study found that the RSA algorithm provides a high level of data protection; however, its use in IoT systems is limited by the computing resources of the devices. Therefore, the use of hybrid cryptographic schemes is recommended.

Ключевые слова: шифрование, расшифровка, мессенджер

Keywords: encryption, decryption, messenger

Т. 12. №6 2026
https://doi.org/10.33619/2414-2948/127

С равитием технологий интернета вещей (IoT) все больше устройств подключаются к сети и обмениваются данными в режиме реального времени. Умные дома, промышленные системы управления и носимая электроника активно используют IoT, что делают вопросы безопасности и защиты данных актуальными. Уязвимость таких устройств может привести к утечке конфиденциальной информации, несанкционированному доступу и даже к нарушению работы критически важных систем. Одной из ключевых задач обеспечения безопасности IoT-устройств является защита передаваемых данных. Для решения этой задачи применяются криптографические методы, среди которых алгорим RSA занимает особое место. Данный алгоритм относится к семейству ассимметричных и основывается на сложности факторизации больших чисел, что делает его надежным инструментом для защиты данных. Использование алгоритма RSA в IoT-устройствах позволяет обеспечить конфиденциальность, целостность аутентификацию данных. Он применяется в сочетании с другими методами шифрования, обеспечивая высокий уровень безопасности.

Актуальность темы исследования обусловлена стремительным ростом количества IoT-устройств и увеличением числа кибератак, направленных на них. В условиях цифровизации различных сфер жизни необходимость надежной защиты данных становится критически важной, особенно для систем, связанных с персональными и промышленными данными.

Целью данного исследования является изучение особенности применения алгоритма RSA для защиты данных в IoT-устройствах и оценить его эффективность его применения.

В рамках данного исследования в качестве теоретической базы использовались научные труды в области криптографии, информационной безопасности и программной инженерии, а также учебные и методические материалы, посвящённые асимметричным алгоритмам шифрования. Особое внимание уделялось изучению принципов функционирования алгоритма RSA и особенностей его применения в IoT-устройствах. Драгилев Е. В. в своем исследовании рассмотрел некоторые аспекты информационной безопасности, применяемые к интернету вещей. Точнее рассмотрен ряд примеров реализации таких угроз, обсуждены перспективные меры защиты информации на основе машинного обучения [1].

Детально рассмотрена проблема защиты персональных данных в сети IoT устройств, провели анализ соблюдения требований информационной безопасности в сетях IoT. В результате — даны рекомендации предотвращения кибератаки и обеспечения комплексной защиты IoT устройств [2].

Рассмотрены проблемы обеспечения информационной безопасности IoTсистемы «умный дом» с применением криптографической защиты данных. Определен стандарт выполнения криптографических преобразований. Обоснован выбора устройства и разработана функциональная схема модуля, выполняющего обработку входных сигналов с датчиков системы и необходимые криптографические преобразования [3].

Д. Р. Исламгалеев и Л. Я. Узбекова описали технологию самоверифицирующихся идентификаторов (SSI) и ее важность в обеспечении безопасности данных IoT. Она основана на принципе децентрализации и самоверификации, что делает ее более надежной и безопасной по сравнению с централизованными системами. Каждое устройство в сети получает уникальный идентификатор, который подтверждается криптографически, что обеспечивает защиту от подделки и несанкционированного доступа [4].

Описаны методы оптимизации существующих алгоритмов (AES, RSA) и предложен гибридный алгоритм на основе эллиптических кривых [5].

Детальное рассмотрение вопроса безопасности IoT устройств выполнено в исследовании, где проведен обзор работ различных исследователей, предлагающие тот или иной подход к формированию структурированной формы определения безопасности. На

Т. 12. №6 2026
https://doi.org/10.33619/2414-2948/127

основе рассмотренных моделей авторами предлагается собственная трехуровневая структура безопасности, включающая также свойства «fog» слоя в архитектуре среды «Интернет вещей»: исполнительные и сенсорные устройства, шлюзы и сеть Интернет, приложения и облачные сервисы. Описаны основные методы повышения безопасности для всех трех слоев, а также приведена математическая модель, с помощью которой можно сделать качественную и количественную оценку безопасности [6].

Рассмотрев и проанализировав все исследования, в данном исследовании был применен принцип работы алгоритма RSA в качестве защиты данных при передачи и получении данных в IoT устройствах. Программная реализация производилось на языке Python и с помощью его дополнительных криптографических модулей PyCrypto. Этот инструментарий представляет собой набор хеш-функций и различных алгоритмов шифрования. Структура пакета легко позволяет добавлять новые модули. Программа представляет собой чат между двумя собеседниками. Они подключаются к друг другу через основной IP-адрес. Принцип работы мессенджера: отправитель и получатель генерируют ключи, и обмениваются открытыми ключами. Именно открытый ключ будет связывать получателя с отправителем. Отправитель пишет сообщение и отправляет получателю. При отправке сообщение автоматически шифруется. У получателя программа показывает процесс дешифрования полученного сообщения. Сообщение автоматически расшифровывается и получатель видит отправленное сообщение.

Результаты исследования и выводы

Интерфейс программы представлен на Рисунке 1.

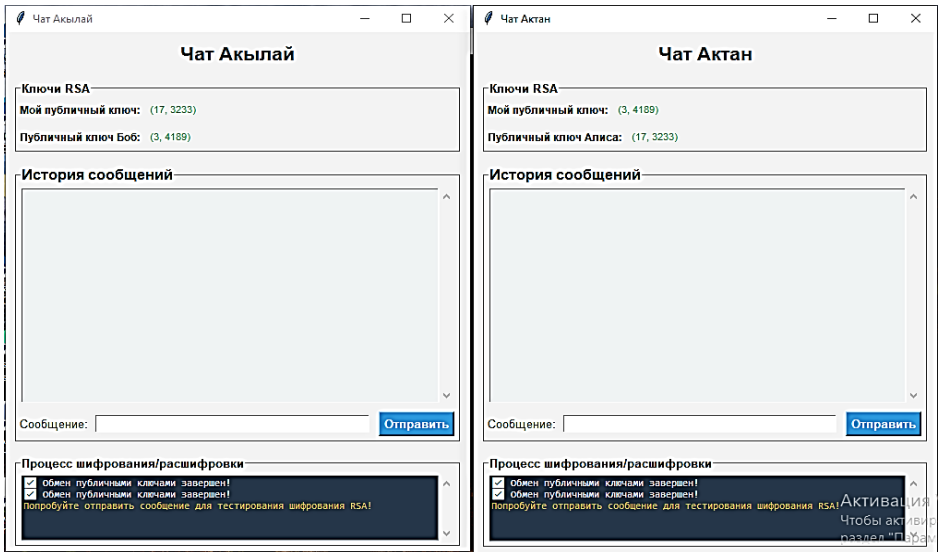

Рисунок 1. Интерфейс программы

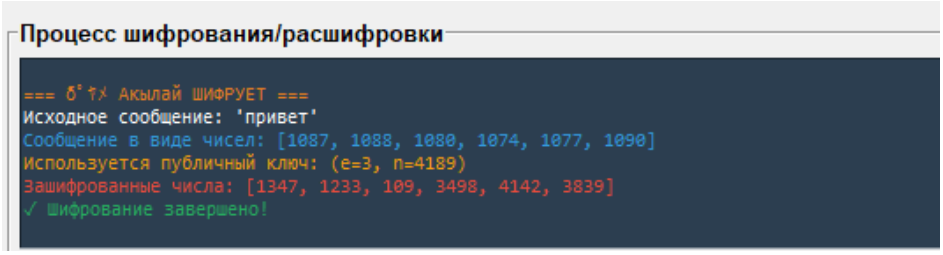

Рисунок 2. Процесс шифрования сообщения

Т. 12. №6 2026
https://doi.org/10.33619/2414-2948/127

Чтобы любому пользователю было понятно и легко в эксплуатации программы, интерфейс программы имеет понятный и интуитивно легкий вид. При запуске программы автоматически генерируются открытый и приватный ключи (Рисунок 2). Получатель (Актан) и отправитель (Акылай) обмениваются открытыми ключами. В поле «сообщение» если написать сообщение «привет», то в окне для отображения процесса шифрования/расшифровки идет пояснение и шифрованный код данного сообщения.

Когда получатель в ответ отправляет сообщение, то в первом окне отразится процесс расшифровки (Рисунок 3).

Большую часть программы представляет собой история сообщений. Там сохраняется переписка между отправителем и получателем (Рисунок 4).

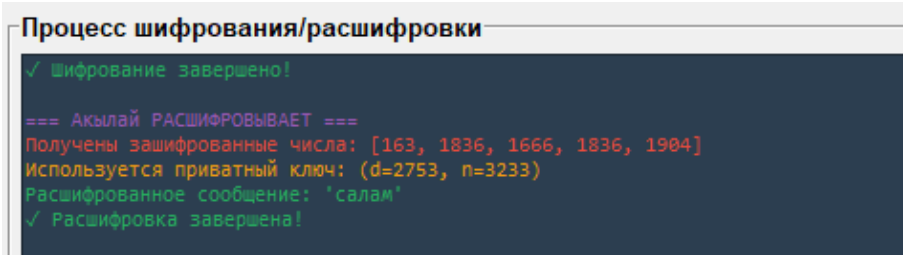

Рисунок 3. Процесс расшифровки сообщения

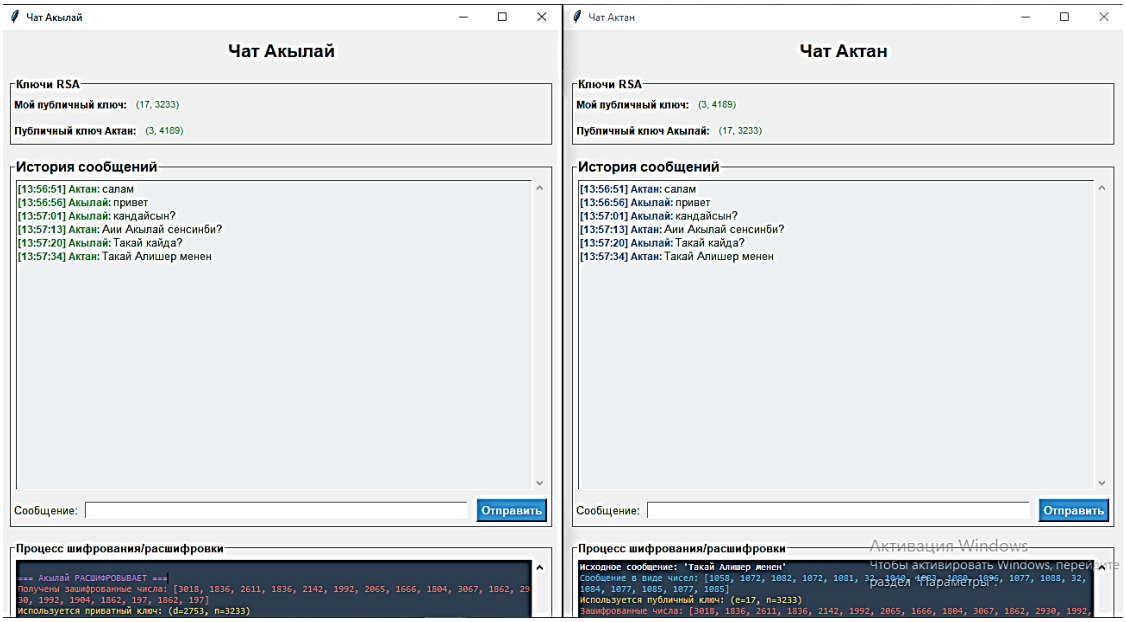

Рисунок 4. История сообщений программы

Итак, алгоритм RSA обеспечивает высокий уровень защиты данных, однако его применение в IoT-системах ограничено вычислительными ресурсами устройств. В связи с этим рекомендуется использование гибридных криптографических схем.

Список литературы:

1. Драгилев Е. В. Интернет вещей и некоторые вопросы информационной безопасности // Наука и техника. Мировые исследования: материалы XVI международной научно-практической конференции. Саратов, 2022. С. 28-31.

2. Биржанов К. К. Некоторые вопросы информационной безопасности // Проблемы обеспечения экономической и информационной безопасности. 2019. С. 16-20.

3. Шишкин, А. О., Воронова Л. И. Проектирование IoT системы "умный дом" с криптографической защитой данных // Телекоммуникации и информационные технологии. 2018. Т. 5. №2. С. 66-71.

4. Исламгалеев Д. Р., Узбекова Л. Я. "SSI" - ключ к защите данных Интернет-вещей // Формирование конкурентной среды, конкурентоспособность и стратегическое управление предприятиями, организациями и регионами: Пенза, 2024. С. 158-161.

5. Гурованов В. Я. Разработка криптоустойчивых алгоритмов шифрования для защиты данных в IOT-устройствах // Современные технологии и инженерия: тенденции и перспективы развития: Сборник научных статей. Краснодар, 2025. С. 86-89.

6. Коробейников А. Г. и др. Информационная безопасность в системе" Интернет вещей" // Вестник Чувашского университета. 2018. №1. С. 117-128.

References:

1. Dragilev, E. V. (2022). Internet veshhej i nekotory`e voprosy` informacionnoj bezopasnosti. In *Nauka i texnika. Mirovy`e issledovaniya: materialy` XVI mezhdunarodnoj nauchno-prakticheskoj konferencii, Saratov,* 28-31. (in Russian).

2. Birzhanov, K. K. (2019). Nekotory`e voprosy` informacionnoj bezopasnosti. In *Problemy` obespecheniya e`konomicheskoj i informacionnoj bezopasnosti* (pp. 16-20). (in Russian).

3. Shishkin, A. O., & Voronova, L. I. (2018). Proektirovanie IoT sistemy` umny`j dom c kriptograficheskoj zashhitoj danny`x. *Telekommunikacii i informacionny`e texnologii, 5*(2), 66-71. (in Russian).

4. Islamgaleev, D. R., & Uzbekova, L. Ya. (2024). In *SSI - klyuch k zashhite danny`x Internet-veshhej // Formirovanie konkurentnoj sredy`, konkurentosposobnost` i strategicheskoe upravlenie predpriyatiyami, organizaciyami i regionami, Penza,* 158-161. (in Russian).

5. Gurovanov, V. Ya. (2025). Razrabotka kriptoustojchivy`x algoritmov shifrovaniya dlya zashhity` danny`x v IOT-ustrojstvax. In *Sovremenny`e texnologii i inzheneriya: tendencii i perspektivy` razvitiya: Sbornik nauchny`x statej, Krasnodar,* 86-89. (in Russian).

6. Korobejnikov, A. G., Grishencev, A. Yu., Dikij, D. I., Artem`eva, V. D., & Sidorkina, I. G. (2018). Informacionnaya bezopasnost` v sisteme Internet veshhej. *Vestnik Chuvashskogo universiteta,* (1), 117-128. (in Russian).

Поступила в редакцию
14.03.2026 г.

Принята к публикации
21.03.2026 г.

Ссылка для цитирования:

Маликова З. Т., Закирова Д. А., Маткаликов А. М. Защита данных IoT-устройств алгоритмом RSA // Бюллетень науки и практики. 2026. Т. 12. №6. С. 219-223. https://doi.org/10.33619/2414-2948/127/27

Cite as (APA):

Malikova, Z., Zakirova, D., & Matkalikov, A. (2026). Protecting IoT Device Data with the RSA Algorithm. *Bulletin of Science and Practice, 12*(6), 219-223. (in Russian). https://doi.org/10.33619/2414-2948/127/27