УДК 004

Давлетшина Э.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Фатхелисламов А.Ф.
Уфимский университет науки и технологий, Уфа

ИСПОЛЬЗОВАНИЕ RSA-КЛЮЧЕЙ ДЛЯ АВТОРИЗАЦИИ

Аннотация. В данной статье рассматривается концепция RSA-ключей, их сущность и значение, а также роль RSA-ключей в процессе авторизации. В рамках исследования будут рассмотрены практические аспекты использования RSA-ключей для авторизации. RSA (Rivest-Shamir-Adleman) представляет собой один из наиболее распространенных алгоритмов асимметричного шифрования, который обеспечивает безопасность передачи данных и аутентификацию пользователей. Статья освещает основные принципы работы RSA, его применение в современных системах безопасности и значимость для защиты информации.

Ключевые слова: авторизация, RSA, RSA-ключи, информационная безопасность.

Безопасность информации является одной из важнейших задач в XXI в. Многие специалисты ИТ-отрасли ежедневно разрабатывают различные методы и способы защиты информации, а хакеры, напротив, с каждым днем создают все новые вредоносы, эксплоиты и другие инструменты для взлома системы и кражи данных. Своеобразная гонка между хакерами и «защитниками информации» приводит к необходимости развития развитием информационных технологий. При развитии информационных технологий происходит и увеличением объема передаваемых данных. Таким образом, возрастает необходимость в надежных методах аутентификации и защиты информации. Один из методов защиты информации является ее шифрование, т. е. приведине информации в такое состояние, в котором хакер не сможет ее понять или как-либо использовать. В рамках данной статьи будет рассматриваться в основном асимметричное шифрование, а в частности алгоритм RSA. Данный алгоритм стал основой для многих современных систем безопасности. Под системой безопасности в данной статье рассматривается комплекс программно-технических и/или аппаратных инструментов, которые помогают защитить цифровую информацию - базы данных, текстовую информацию и другие виды. Итак, RSA-ключи, это часть криптографического алгоритма шифрования. Они состоят из пары открытого и закрытого ключей, обеспечивают безопасный обмен данными

и аутентификацию пользователей, что делает их важным инструментом в области кибербезопасности.

Алгоритм RSA имеет свои принципы работы, которые позволяют обеспечить защиту информации, путем использования вычислительных мощностей цифровой техники. Алгоритм RSA основан на математических свойствах больших простых чисел и сложности задачи факторизации [1]. Процесс генерации RSA-ключей включает следующие этапы:

Первый – это выбор двух больших простых чисел: Пусть p и q – два больших простых числа, которые должны быть выбраны случайным образом. Размер этих чисел определяет уровень безопасности ключа. Например, для обеспечения достаточной безопасности в текущем году рекомендуется использовать ключи длиной не менее 2048 бит.

Второй – это вычисление модуля, так модуль n вычисляется как $n=p\times q$. Этот модуль используется как основа для шифрования и дешифрования.

Третий этап – это вычисление функции Эйлера. Функция Эйлера $\phi(n)=(p-1)(q-1)$ используется для определения количества чисел, меньших n, которые взаимно просты с n.

Четвертым этапом будет являться как раз выбор открытого ключа. Алгоритм выбирает целое число e, такое что $1<e<\phi(n)$ и e взаимно просто с $\phi(n)$. Обычно выбирается стандартное значение $e = 65537$, так как оно обеспечивает хороший баланс между безопасностью и эффективностью.

Последний этап – это вычисление закрытого ключа. В таком виде закрытый ключ d вычисляется как мультипликативная обратная к e по модулю $\phi(n)$, то есть $d\cdot e \equiv 1 mod \phi(n)$. Это можно сделать с помощью алгоритма Евклида.

Пара ключей (e,n) и (d,n) образует открытый и закрытый ключи соответственно. Открытый ключ может быть свободно распространен, в то время как закрытый ключ должен храниться в секрете.

Рассмотрим практическое применение RSA-ключей для авторизации.

RSA-ключи находят широкое применение в различных аспектах авторизации и аутентификации. Основные области их использования включают: шифрование данных, цифровые подписи, аутентификацию пользователей и безопасный обмен ключами.

Рассмотрим каждую область:

Шифрование данных – открытый ключ используется для шифрования сообщений, которые могут быть расшифрованы только с помощью соответствующего закрытого ключа. Это обеспечивает конфиденциальность передаваемой информации.

Цифровые подписи – RSA позволяет создавать цифровые подписи, которые подтверждают подлинность и целостность сообщения. Отправитель шифрует хэш-сумму сообщения с помощью своего закрытого ключа, а получатель может проверить подпись, расшифровав ее открытым ключом отправителя. Для создания хэш-суммы обычно используются криптографические хэш-функции, такие как SHA-256.

Аутентификация пользователей – в системах, требующих аутентификации, RSA-ключи могут использоваться для подтверждения личности пользователя. При входе в систему пользователь может предоставить свой открытый ключ, а сервер проверяет его подлинность, используя соответствующий закрытый ключ.

Безопасный обмен ключами – RSA может быть использован для безопасной передачи симметричных ключей, которые затем применяются для шифрования данных с использованием более быстрых симметричных алгоритмов, таких как AES [2]. Это позволяет комбинировать преимущества асимметричного и симметричного шифрования.

Использование RSA-ключей для авторизации имеет несколько ключевых преимуществ, например, безопасность, ведь RSA обеспечивает высокий уровень безопасности благодаря сложности задачи факторизации больших чисел. Это делает его устойчивым к атакам, что особенно важно в условиях современных угроз.

Примером будет являться гибкость использования данных ключей, ведь RSA-ключи могут быть использованы в различных сценариях, включая шифрование, цифровые подписи и аутентификацию, что делает их универсальным инструментом в области кибербезопасности.

Использование цифровых подписей и аутентификации на основе RSA способствует созданию доверительных отношений между пользователями и системами, что является важным аспектом в электронной коммерции и других областях. Также, RSA является стандартом в области криптографии и широко поддерживается различными протоколами и системами, такими как SSL/TLS, PGP и другие, что упрощает его интеграцию в существующие решения.

Рассмотрим практические кейсы, которые помогут подчеркнуть ценность RSA-ключей. Необходимо создать защищенный канал передачи данных - для этого отлично подойдет шифрование канала. В таком случае открытый ключ используется для шифрования сообщения, а закрытый ключ – для его расшифровки. То есть информация будет передаваться, но при этом, она будет полезна только тем, у кого есть закрытый ключ.

RSA также широко используется для создания цифровых подписей, которые подтверждают подлинность и целостность данных. Рассмотрим этот случай подробнее. Процесс цифровой подписи, путем использования RSA включает следующие шаги:

1. Создание подписи. Этап, когда отправитель создает хэш-сумму сообщения с помощью криптографической хэш-функции (например, SHA-256) и затем шифрует эту хэш-сумму своим закрытым ключом. Полученная подпись прикрепляется к сообщению.

2. Проверка подписи. Этап, в котором получатель может расшифровать подпись с помощью открытого ключа отправителя, чтобы получить хэш-сумму. Затем он сравнивает ее с хэш-суммой, вычисленной из полученного сообщения. Если они совпадают, это подтверждает, что сообщение не

было изменено и действительно было отправлено указанным отправителем.

Разумеется, при использовании данного шифрования в информационных системах, все операции происходят в автоматическом режиме, путем использования технических мощностей вычислительной техники.

Другой пример – RSA является основой для многих протоколов безопасности, таких как SSL/TLS, которые используются для защиты интернет-трафика. В этих протоколах RSA-ключи применяются для установления защищенного соединения и аутентификации сторон. При инициации соединения клиент и сервер обмениваются открытыми ключами и используют их для шифрования данных, что обеспечивает защиту от перехвата и подмены информации. После сервер может использовать свой закрытый ключ для создания цифровой подписи, подтверждающей его подлинность, что позволяет клиенту убедиться, что он подключается к правильному серверу.

Резюмируя, RSA-ключи представляют собой важный инструмент для обеспечения безопасности и аутентификации в цифровом мире. Их применение в шифровании данных, цифровых подписях и аутентификации пользователей способствует защите информации и созданию доверительных отношений между сторонами. В условиях растущих угроз кибербезопасности использование RSA-ключей становится необходимым для обеспечения конфиденциальности и целостности данных, что подчеркивает их значимость в современных информационных системах.

Список использованных источников:

1. Белоус А.И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения: учебник / А.И. Белоус. М.: Техносфера, 2021. 483 с. (дата обращения 28.03.2025). Текст: непосредственный.

2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. М.: ФОРУМ: ИНФРА-М, 2021. 416 с. (дата обращения 28.03.2025). Текст: непосредственный.

Davletshina E.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

USE OF RSA KEYS FOR AUTHORIZATION

Abstract. This article discusses the concept of RSA keys, their essence and meaning, as well as the role of RSA keys in the authorization process. The study will consider the practical aspects of using RSA keys for authorization. RSA

(Rivest-Shamir-Adleman) is one of the most common asymmetric encryption algorithms that ensures the security of data transmission and user authentication. The article covers the basic principles of RSA, its application in modern security systems and its importance for information protection.

Keywords: authorization, RSA, RSA keys, information security.