www.volsu.ru

CC BY

DOI: https://doi.org/10.15688/NBIT.jvolsu.2025.2.2

УДК 004.056.55
ББК 32.972.53

РОЛЬ ШИФРОВАНИЯ В РАЗРАБОТКЕ ЗАЩИЩЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Владислав Георгиевич Яриков

Кандидат педагогических наук,
доцент кафедры информационной безопасности,
Волгоградский государственный университет
yarikov.vladislav@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Александра Николаевна Панченко

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBm-241_744165@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В данной работе рассматривается важность защиты данных в условиях постоянного развития информационных технологий. Основное внимание уделяется шифрованию данных как ключевому инструменту для предотвращения киберугроз и обеспечения безопасности программного обеспечения. Обсуждаются два основных вида шифрования: симметричное и асимметричное, с примерами популярных алгоритмов, таких как AES, RSA, Blowfish и SHA. Также подчеркивается роль шифрования в различных аспектах разработки программного обеспечения, включая хранение и передачу данных, аутентификацию и цифровые подписи.

Ключевые слова: защита данных, шифрование, симметричное шифрование, асимметричное шифрование, AES, RSA, безопасность программного обеспечения.

Введение

В условиях постоянного развития информационных технологий вопрос защиты данных является ключевым. В повседневной жизни мы часто сталкиваемся со сбоями программ, это может доставить достаточно много неудобств. Однако, если ненадежное ПО будет использоваться стратегически важными объектами, последствия ошибок будут колоссальными. Безопасность программного обеспечения – это важная задача для IT-специалистов. Защита ПО осуществляется с использованием большого количества методов, среди которых важную роль занимает шифрование данных.

Шифрование – это полезный инструмент для предотвращения различных киберугроз, который защищает информацию от неавторизованных пользователей, путем использования механизмов преобразования данных в нечитаемый формат. Внедрение шифрования не только защитит данные, но и укрепит доверие пользователей, и сделает использование программ более надежным. Для разработки защищенного ПО важно учитывать все сильные и слабые стороны шифрования.

© Яриков В.Г., Панченко А.Н., 2025

Методы шифрования информации

Шифрование данных делится на два основных вида: симметричное и ассиметричное.

1. Симметричное шифрование является достаточно простым и эффективным. Примеры такого шифрования: DES, AES. Это осуществляется за счет того, что для шифрования и дешифрования используется один и тот же ключ. Перед обменом информации участники выбирают ключ, доступ к которому будут иметь только они. Недостаток данного метода заключается в невозможности его использования при большом числе участников, так как злоумышленнику будет легче узнать ключ и похитить данные [2].

2. Ассиметричное шифрование отличается от симметричного тем, что имеет два ключа: для шифрования открытый, доступ к которому не ограничен, и для расшифровки, которую могут осуществлять только владельцы – закрытый (см. рис. 2). Пример такого шифрования: RSA, PGP, S/MIME. Недостатком этого типа шифрования выступает то, что во время передачи информации злоумышленники могут ее перехватить и подменить, но владелец и получатель об этом не догадаются [3].

Современные распространенные криптографические алгоритмы шифрования, такие как AES, RSA, Blowfish, SHA обладают высокой степенью надежности защиты данных, все они отличаются между собой уровнем безопасности, подверженности к различным видам атак, скоростью и т. п. (см. рис. 2).

AES (Advanced Encryption Standard) – использует симметричное блочное шифрование с фиксированным размером блока 128 бит (если сообщение меньше его увеличивают, чаще всего это делают путем добавления нулей, когда сообщение больше, его разбивают), и ключами различной длины – 128, 192 и 256 бит. Главный недостаток AES заключается в зависимости сложности управления от длины ключа. При использовании длинных ключей, увеличивается безопасность, но тратится больше вычислительных ресурсов, что может привести к снижению производительности, особенно на устройствах с ограниченными вычислительными ресурсами. Несмотря на это AES считается самым надежным алгоритмом шифрования.

RSA (Rivest-Shamir-Adleman) – асимметричный криптографический алгоритм, обычно используется в целях защиты данных и проверки цифровых подписей. Недостатком данного метода является низкая скорость, это связанно с тем, что RSA использует большие ключи около 2048 бит.

Blowfish – симметричный алгоритм шифрования, состоящий из двух частей: расширения ключа и шифрования данных. За счет изменения длины ключа от 32 до 448, данную технику лучше применять в условиях, когда ключ шифрования меняется редко [4]. Существенный минус данного алгоритма – сложная фаза инициализации до начала шифрования, связанная с использованием множества подключей, которые должны быть вычислены до начала операции шифрования / дешиф-

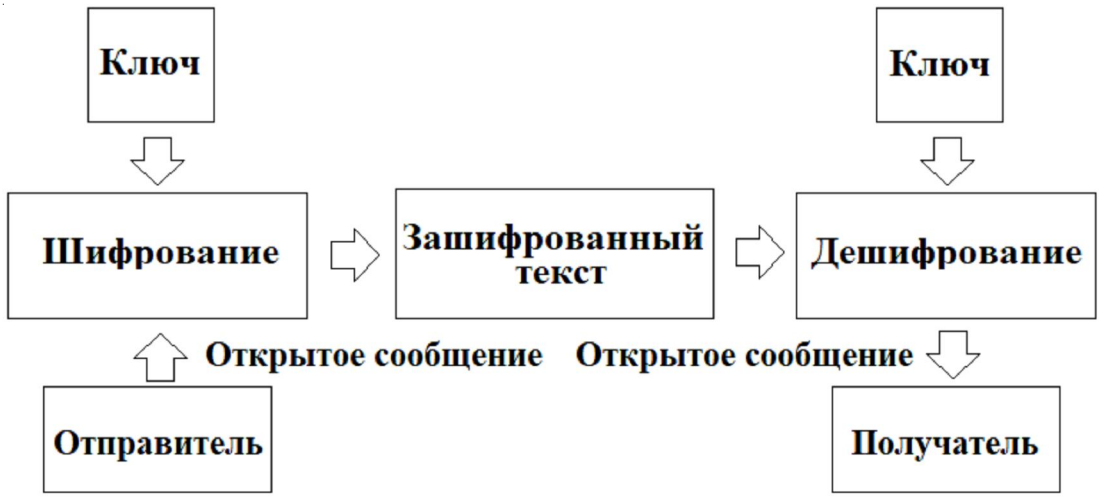


Рис. 1. Процесс шифрования

ровании, однако на современных мощных процессорах это не играет большой роли [5].

SHA (Secure Hash Algorithm) – это криптографическая хеш-функция, которая преобразует входные данные произвольной длины в фиксированный хеш-код определенной длины [4]. Хеш-функции SHA используются для проверки целостности данных, например, при загрузке файлов или передаче данных по сети в случае, если хеш совпадает с ожидаемым значением, данные не были изменены. Основной недостаток алгоритмов хеширования – уязвимость к атакам на коллизии. Такие ситуации возникают, когда два разных входных значения выдают одинаковый хеш.

Роль шифрования в разработке программного обеспечения

Для обеспечения защиты и безопасности программного обеспечения на различных уровнях применяются различные криптографические методы: кодирование, сжатие, хеширование, стеганография и шифрование [1].

В приложениях шифрование используется в различных аспектах, включая:

1. Хранение и передача данных. Шифрование позволяет обеспечить надежную передачу данных между узлами сети и исключает риск перехвата информации, так алгоритм AES используется для защиты данных на серверах и в облачных хранилищах. Примеры шифрования в программном обеспечении:

1) шифрование сообщений электронной почты для обеспечения целостности и конфиденциальности с помощью программ PGP (Pretty Good Privacy) и S/MIME (Secure/ Multipurpose Internet Mail Extensions);

2) мессенджеры, например, WhatsApp* используют сквозное шифрование для защиты сообщений на всех этапах передачи;

3) программы, такие как BitLocker (Windows) и FileVault (macOS), обеспечивают полное шифрование жесткого диска, защищая данные от доступа в случае кражи или потери устройства;

4) программы, такие как Docker, могут использовать шифрование для защиты данных, хранящихся в контейнерах, что обеспечивает безопасность при развертывании приложений в облачной среде.

2. Аутентификация. Шифрование используется для защиты паролей для обеспечения защиты от рисков, связанных с изменением и подделкой данных. Алгоритм Blowfish может применяться для шифрования паролей, а хеширование паролей с помощью алгоритмов, таких как SHA, позволяет создать уникальные пароли, которые невозможно восстановить в исходный вид.

3. Цифровые подписи. Алгоритм RSA используется для создания цифровых подписей, обеспечивая защиту от подделки и подтверждая, что документ был подписан конкретным пользователем.

Применение криптографических методов является обязательным условием для создания безопасных ПО, и позволяет организациям и пользователям эффективно защищать свои данные от киберугроз.

Заключение

В условиях стремительного развития информационных технологий защита данных



Рис. 2. Методы криптографии

* WhatsApp принадлежит компании MetaPlatforms, Inc., включенной в Перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму. Деятельность данной организации запрещена на территории Российской Федерации.

становится критически важной задачей для организаций и пользователей. Шифрование, как один из основных методов обеспечения безопасности, играет ключевую роль в предотвращении киберугроз и защите конфиденциальной информации. Симметричное и асимметричное шифрование, представленные такими алгоритмами, как AES и RSA, обеспечивают различные уровни защиты, подходящие для различных сценариев использования.

Эффективное применение шифрования в разработке программного обеспечения, включая хранение и передачу данных, аутентификацию и создание цифровых подписей, способствует укреплению доверия пользователей и повышает надежность систем. Важно учитывать, как преимущества, так и недостатки различных подходов к шифрованию, чтобы обеспечить максимальную защиту информации. В конечном итоге внедрение криптографических методов играет ключевую роль в создании безопасного программного обеспечения.

СПИСОК ЛИТЕРАТУРЫ

1. Бутин, А. А. Технологии защиты программного обеспечения / А. А. Бутин // Информационные технологии и математическое моделирование в управлении сложными системами. – 2019. – № 2 (3). – С. 53–63.

2. Ересь, А. В. Анализ современных методов шифрования информации / А. В. Ересь // Постулат. – 2018. – № 1(27). – С. 74.

3. Завгородний, С. Д. Алгоритм Blowfish / С. Д. Завгородний // Научные исследования и разработки студентов : сб. материалов IV Междунар. студ. науч.-практ. конф. (Чебоксары, 29 июня 2017 г.). – Чебоксары : Центр науч. сотрудничества «Интерактив плюс», 2017. – С. 147–149.

4. Москвин, А. Д. Анализ современных алгоритмов шифрования данных / А. Д. Москвин, Л. Э. Петросян // Инженерный вестник Дона. – 2023. – № 4 (100). – С. 102–115.

5. Фисун, С. Н. Сравнительный анализ симметричных алгоритмов шифрования в информационных коммуникационных сетях / С. Н. Фисун, Р. Г. Вихров //Проблемы безопасности в современном мире : тез. докл. (Севастополь, 26–28 мая 2016 г.). – Севастополь : Моск. гос. ун-т им. М.В. Ломоносова, фил. в Севастополе, 2016. – С. 225–228.

REFERENCES

1. Butin A.A. Tehnologii zashchity programmnogo obespecheniya [Software Protection Technologies]. *Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami* [Information Technology and Mathematical Modeling in the Management of Complex Systems], 2019, no. 2 (3), pp. 53-63.

2. Eres A.V. Analiz sovremennyh metodov shifrovaniya informacii [Analysis of Modern Methods of Information Encryption]. *Postulat* [Postulate], 2018, no. 1 (27), p. 74.

3. Zavgorodnij S.D. Algoritm Blowfish [Blowfish Algorithm]. *Nauchnye issledovaniya i razrabotki studentov: sb. materialov IV Mezhdunar. stud. nauch.-prakt. konf. (Cheboksary, 29 iyunya 2017 g.)* [Scientific Research and Development of Students. Proceedings of the 6th International Student Scientific and Practical Conference. Cheboksary, June 29, 2017]. Cheboksary, Centr nauch. sotrudnichestva «Interaktiv plyus», 2017, pp. 147-149.

4. Moskin A.D., Petrosyan L.E. Analiz sovremennyh algoritmov shifrovaniya dannyh [Analysis of Modern Data Encryption Algorithms]. *Inzhenernyj vestnik Dona* [Engineering Journal of Don], 2023, no. 4 (100), pp. 102-115.

5. Fisun S.N., Vihrov R.G. Sravnitelnyj analiz simmetrichnyh algoritmov shifrovaniya v informacionnyh kommunikacionnyh setyah [Comparative Analysis of Symmetric Encryption Algorithms in Information Communication Networks]. *Problemy bezopasnosti v sovremennom mire: tez. dokl. (Sevastopol, 26–28 maya 2016 g.)* [Security Problems in the Modern World. Abstracts of Reports. Sevastopol, May 26–28, 2016]. Sevastopol, Mosk. gos. un-t im. M.V. Lomonosova, fil. v Sevastopole, 2016, pp. 225-228.

THE ROLE OF ENCRYPTION IN THE DEVELOPMENT OF SECURE SOFTWARE

Vladislav G. Yarikov

Candidate of Sciences (Pedagogy),
Associate Professor, Department of Information Security,
Volgograd State University
yarikov.vladislav@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Alexandra N. Panchenko

Student, Department of Information Security,
Volgograd State University
IBm-241_744165@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. This article explores the critical role of data protection in the development of secure software, a paramount concern amidst the rapid evolution of information technologies. The study positions encryption as a fundamental tool for mitigating cyber threats and safeguarding information from unauthorized access by transforming it into an unreadable format. The authors provide a comparative analysis of the two primary encryption paradigms: symmetric (e.g., AES, Blowfish) and asymmetric (e.g., RSA), detailing their core mechanisms, advantages, and inherent limitations, such as key distribution challenges and computational overhead. Furthermore, the paper examines specific widely used algorithms – AES, RSA, Blowfish, and the SHA hashing function – highlighting their distinct applications, strengths, and vulnerabilities. The research extends beyond theory to practical implementation, underscoring encryption's integral function in various aspects of software development. This includes ensuring the confidentiality and integrity of data during storage and transmission (e.g., in cloud environments, email, and messaging apps), reinforcing authentication processes through password hashing, and enabling the creation of secure digital signatures. The conclusion emphasizes that the judicious selection and application of these cryptographic methods are indispensable for building robust, trustworthy software systems, ultimately enhancing user confidence and protecting sensitive information in an increasingly digital world.

Key words: data protection, encryption, symmetric encryption, asymmetric encryption, AES, RSA, software security.