Автоматизация и моделирование в проектировании и управлении. 2022. № (17). С. 10-15.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2022. № 3 (17). P. 10-15.

Научная статья
Статья в открытом доступе
УДК 004.056.57
doi:10.30987/2658-6436-2022-3-10-15

ПРИМЕНЕНИЕ РАНДОМИЗАЦИИ АЛГОРИТМОВ ШИФРОВАНИЯ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Наталья Михайловна Кузнецова [1], Татьяна Владимировна Карлова [2], Анна Николаевна Запольская [3]

[1] Московский государственный технологический университет «СТАНКИН»
[2,3] Институт конструкторско-технологической информатики Российской академии наук
[1] knm87@mail.ru
[2] karlova-t@yandex.ru
[3] zap-ann@yandex.ru

Аннотация. *Целью научной работы является разработка методики применения рандомизации используемых алгоритмов шифрования в автоматизированных системах защиты информационных ресурсов промышленного предприятия. Статья посвящена решению задачи формирования с помощью механизма рандомизации последовательностей алгоритмов и ключей шифрования для обеспечения конфиденциальности коммуникаций между территориально распределенными департаментами промышленного предприятия. Новизной работы является предложенная креативная концепция автоматизации процессов шифрования, позволяющая повысить уровень защиты информационных ресурсов. Результатом исследования являются рекомендации по построению комплексных автоматизированных систем шифрования, использующих трассы алгоритмов.*

Ключевые слова: автоматизация, шифрование, защита информации, рандомизация, информационная безопасность

Для цитирования: Кузнецова Н.М., Карлова Т.В., Запольская А.Н. Применение рандомизации алгоритмов шифрования в автоматизированной системе защиты информационных ресурсов промышленного предприятия // Автоматизация и моделирование в проектировании и управлении. 2022. №3 (17). С. 10-15. doi: 10.30987/2658-6436-2022-3-10-15.

Original article
Open Access Article

APPLYING RANDOMIZED ENCRYPTION ALGORITHMS IN AN INDUSTRIAL ENTERPRISE AUTOMATED SYSTEM FOR INFORMATION RESOURCE PROTECTION

Natalya M. Kuznetsova [1], Tatyana V. Karlova [2], Anna N. Zapolskaya [3]

[1] Moscow State University of Technology «STANKIN»
[2,3] Institute for Design-Technological Informatics of the Russian Academy of Sciences
[1] knm87@mail.ru
[2] karlova-t@yandex.ru
[3] zap-ann@yandex.ru

Abstract. *The aim of the study is to develop a methodology for applying randomized encryption algorithms in automated systems of an industrial enterprise for protecting information resources. The article is devoted to solving the problem of generating sequences of algorithms and encryption keys using the randomization mechanism to ensure communication confidentiality between geographically distributed departments of an industrial enterprise. The novelty of the work is the proposed creative concept of encryption process automation, which allows increasing the level of information resource protection. The study results are recommendations for constructing complex automated encryption systems using algorithm traces.*

Keywords: automation, encryption, data security, randomization, information security
For citation: Kuznetsova N.M., Karlova T.V., Zapolskaya A.N. Applying randomized encryption algorithms in an indastrial enteprise automated system for information resourse protection. Automation and modeling in design and management, 2022, no. 3 (17). pp. 10-15. doi: 10.30987/2658-6436-2022-3-10-15.

Введение

В современном информационном обществе диапазон применения методов шифрования довольно широк. Целью любого вида шифрования является сохранение в тайне хранимых, передаваемых и обрабатываемых данных. Как правило, для хранения используют методы симметричного и асимметричного шифрования, а также функции хеширования. Для пред- и постобработки используются методы симметричного шифрования. Для передачи информации – методы симметричного и асимметричного шифрования. В статье предложен механизм рандомизации алгоритмов шифрования для обеспечения защиты передаваемых данных с помощью методов симметричного шифрования. Данный механизм позволит увеличить криптостойкость передаваемых сообщений.

В случае, если промышленное предприятие имеет филиалы, удаленные офисы – распределенную геолокацию – применение представленной в статье методики позволит обеспечить высокий уровень конфиденциальности коммуникаций между территориально распределенными департаментами предприятия. Важной особенность предлагаемой методики является отсутствие зависимости от технологии физической передачи данных. Другими словами, зашифрованные данные могут передаваться по любому каналу связи: оптоволокно; витая пара; беспроводной канал и т.д.

Особенности применения алгоритмов симметричного шифрования в автоматизированных системах защиты

Основным правилом шифрования является обеспечение секретности послания за счёт секретности ключа, но не алгоритма. Для симметричного шифрования применяется один и тот же ключ как в процессе зашифровки, так и в процессе расшифровки [1].

Все основные современные алгоритмы симметричного шифрования можно условно разделить на: алгоритмы на основе сети Фейстеля; SP-сети (substitution-permutation network) – подстановочно-перестановочные сети.

При этом длины ключей для разных современных алгоритмов приблизительно равны (для алгоритма «Магма» – 256 бит [2, 3], для алгоритма «Кузнечик» – 256 бит [2 – 4], для алгоритма «AES» – 256 бит [1, 5]).

На рис. 1 представлена схема работы симметричного алгоритма шифрования.

Рис. 1. Схема работы симметричного алгоритма шифрования
Fig. 1. Scheme of operation of symmetric encryption algorithm

Таким образом, возможно последовательное применение алгоритмов с одним и тем же ключом. (Если длины ключей не совпадают, необходимо введение процедуры расширения ключа и использование в качестве общего ключа максимального по длине).

На рис. 2 представлена схема последовательного использования алгоритмов симметричного шифрования с использованием одного ключа.

При использовании такой схемы секретным является не только ключ, но и последовательность алгоритмов шифрования $\{A_1, A_2, ..., A_N\}$.

С целью повышение уровня криптостойкости необходимо менять последовательность алгоритмов из множества $\{A_1, A_2, ..., A_N\}$ – применить рандомизацию.

Основные принципы реализации методики применения рандомизации алгоритмов шифрования

Для реализации методики необходимо, чтобы на отправляющей и принимающей сторонах были:

– списки алгоритмов шифрования;
– генераторы псевдослучайных чисел (ГПСЧ);
– вычислительное оборудование.

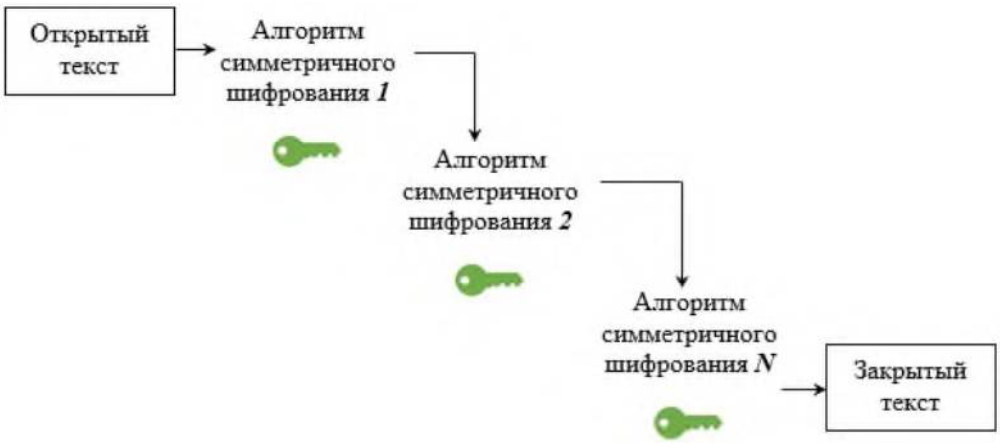

Рис. 2. Схема последовательного использования алгоритмов симметричного шифрования с использованием одного ключа

Fig. 2. Scheme of sequential use of symmetric encryption algorithms using a single key

На рис. 3 представлена схема формирования ключа шифрования на основе рандомизации последовательности алгоритмов.

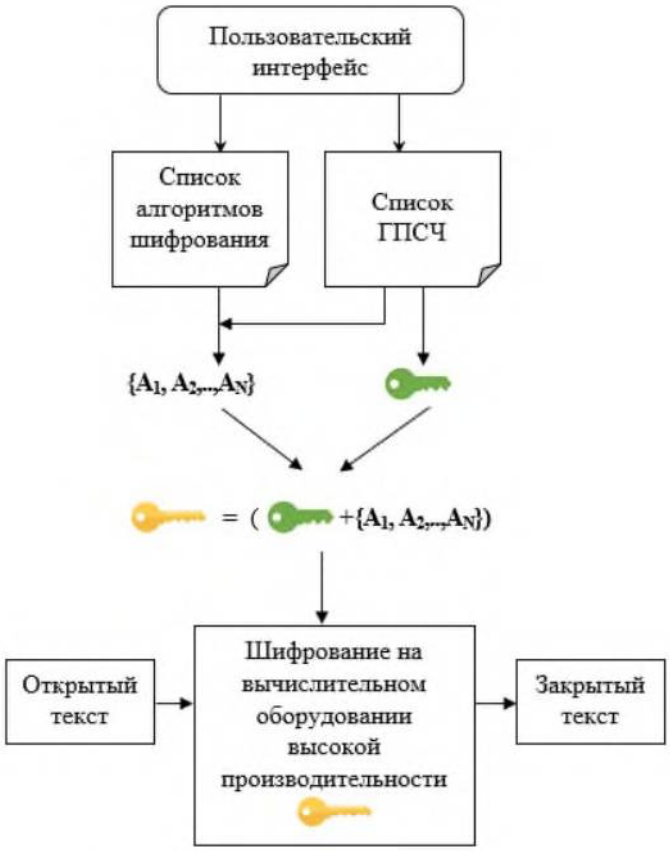

Рис. 3. Схема формирования ключа шифрования на основе рандомизации последовательности алгоритмов

Fig. 3. Encryption key generation scheme based on algorithm sequence randomization

Согласно рис. 3, итоговый ключ шифрования содержит классический ключ, а также информацию о последовательности используемых алгоритмов шифрования.

Классический ключ формируется с помощью выбранного пользователем ГПСЧ.

Последовательность алгоритмов шифрования формируется также с помощью ГПСЧ из списка выбранных через пользовательский интерфейс алгоритмов шифрования: пользователь формирует список алгоритмов, далее ГПСЧ производит рандомизированную перестановку элементов данного списка.

Список алгоритмов шифрования, а также список ГПСЧ задаются системным программистом в файле конфигурации (с целью минимизации ошибок пользователей: пользователь не сможет выбрать не зарегистрированные алгоритмы и ГПСЧ).

Таким образом, системный программист формирует множество M алгоритмов шифрования. Пользователь выбирает из множества M множество необходимых ему алгоритмов шифрования N. Далее с помощью ГПСЧ формируется последовательность алгоритмов шифрования $\{A_1, A_2, ..., A_i, ..., A_N\}$.

Далее производится шифрование на вычислительном оборудовании высокой производительности с помощью ключа, содержащего классический ключ шифрования и информацию о последовательности алгоритмов.

Рационализация реализации методики

Для повышения производительности комплекса вычислительного оборудования необходимо применение распараллеливания алгоритмов шифрования. Для этого последовательность $\{A_1, A_2, ..., A_i, ..., A_N\}$ должна состоять из алгоритмов, приблизительно равной вычислительной сложности (в пределах одного порядка).

Формирование пользователем трасс алгоритмов

На этапе формирования последовательности алгоритмов шифрования возможно задание трасс алгоритмов пользователем [6, 7].

Пример трассы алгоритмов, формируемой пользователем, представлен на рис. 4.

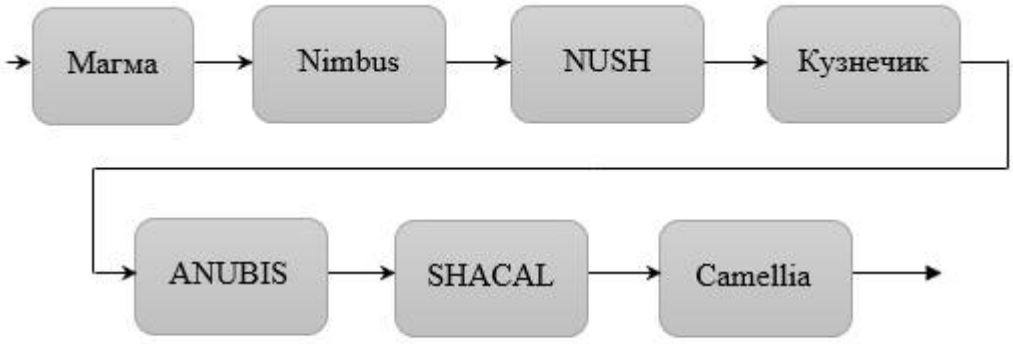

Рис. 4. Пример трассы алгоритмов, формируемой пользователем
Fig. 4. Example of Algorithm Trace Generated by User

Недостатки методики применения рандомизации алгоритмов шифрования и решения по их устранению

Для реализации представленной в статье методики необходимо наличие больших вычислительных мощностей. Также необходимо выполнение строгих требований к производительности оборудования.

Частичным косвенным решением к задаче выбора оборудования является распараллеливание алгоритмов.

Также важно, чтобы совместимость алгоритмов была эмпирически доказана (во избежание увеличения чувствительности к ряду атак). Для частичного устранения данного недостатка также возможно применение различных ключей для каждого алгоритма из последовательности $\{A_1, A_2, \ldots, A_i, \ldots, A_N\}$.

На рис. 5 представлена схема формирования итогового ключа, включающего совокупность N ключей шифрования, уникально используемых для каждого из последовательности алгоритмов $\{A_1, A_2, ..., A_i, ..., A_N\}$.

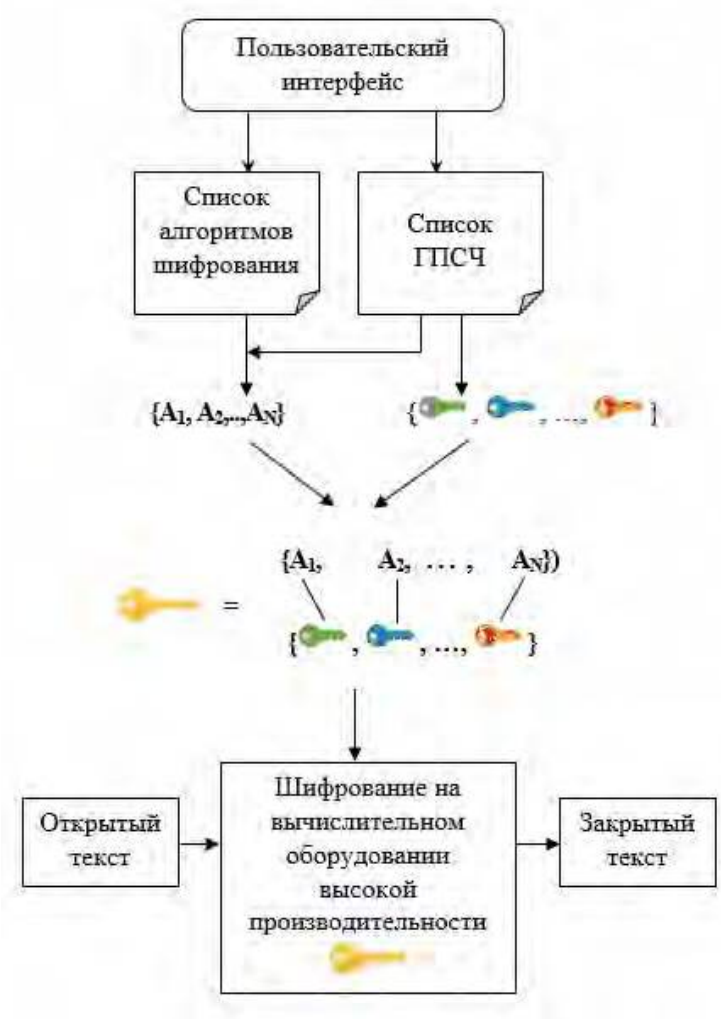

Рис. 5. Схема формирования итогового ключа, включающего совокупность *N* ключей шифрования
Fig. 5. The scheme of formation of the total key including set N keys of enciphering

Заключение

Применение механизма рандомизации алгоритмов шифрования позволит обеспечить высокий уровень информационной безопасности промышленного предприятия за счет повышения криптостойкости «итогового алгоритма».

Предложенные схемы формирования ключей шифрования, трасс алгоритмов шифрования рекомендуется применять как в модулях автоматизированной системы защиты информационных ресурсов предприятия, так и в отдельных программных продуктах обеспечения конфиденциальности коммуникаций.

Список источников:

1. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ Петербург, 2009. 576 с.
2. ГОСТ 34.12-2018 Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2018.
3. ГОСТ 34.13-2018 Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров. М.: Стандартинформ, 2018.
4. Криптографический алгоритм «Кузнечик». URL: https://habr.com/ru/post/459004 (дата обращения: 15.07.2022).
5. Симметричный алгоритм блочного шифрования Advanced Encryption Standard (AES). URL: habr/com/ru/post/534620 (дата обращения: 25.07.2022).

References:

1. Panasenko S.P. Encryption Algorithms. Special Reference. Saint Petersburg: BHV-Petersburg; 2009.
2. GOST 34.12-2018 Information Technology (IT). Cryptographic Data Security. Block Ciphers. Moscow: Standartinform; 2018.
3. GOST 34.13-2018 Information Technology (IT). Cryptographic Data Security. Modes of Operation for Block Ciphers. Moscow: Standartinform; 2018.
4. Cryptographic algorithm «Grasshopper» [Internet] [cited 2022 Jul 15]. Available from: https://habr.com/ru/post/459004.
5. Advanced Encryption Standard (AES) Algorithm [Internet] [cited 2022 Jul 25]. Available from: habr/com/ru/post/534620.

6. Кузнецова Н.М., Карлова Т.В., Шептунов С.А. Криптоанализ сообщений в автоматизированных системах предотвращения утечек информации по каналам связи с применением теории графов // Ученые записки Комсомольского-на-Амуре государственного технического университета. – 2015. – Т. 1. – № 4 (24). – С.33-37.
7. Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Совершенствование симметричного шифрования за счёт внедрения блока информации об используемых алгоритмах в ключ // Вестник Брянского государственного технического университета. – 2015. – №4 (48). – С. 121.

6. Kuznetsova N.M., Karlova T.V., Sheptunov S.A. Cryptanalysis of Messages in Automated Systems for Preventing Information Leaks through Communication Channels Using Graph Theory. Scholarly Notes of KNASTU. 2015;1; 4(24):33-37.

7. Kuznetsova N.M., Karlova T.V., Bekmeshov A.Yu. Symmetric Encryption Upgrade by Introduction Information Block on Used Algorithms in Key. Bulletin of Bryansk State Technical University. 2015;4 (48):121.

Информация об авторах:

Кузнецова Наталия Михайловна
кандидат технических наук, доцент «Московский государственный технологический университет «СТАНКИН»

Карлова Татьяна Владимировна
доктор социологических наук, кандидат технических наук, профессор «Институт конструкторско-технологической информатики Российской академии наук»

Запольская Анна Николаевна
кандидат социологических наук, старший научный сотрудник, ученый секретарь «Институт конструкторско-технологической информатики Российской академии наук»

Information about authors:

Kuznetsova Natalia Mikhailovna
Candidate of Technical Sciences, Associate Professor of Moscow State University of Technology «STANKIN»

Karlova Tatyana Vladimirovna
Doctor of Sociological Sciences, Candidate of Technical Sciences, Professor of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Zapolskaya Anna Nikolaevna
Candidate of Sociological Sciences, Senior Research Fellow, Academic Secretary of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Статья поступила в редакцию 29.07.2022; одобрена после рецензирования 05.09.2022; принята к публикации 09.09.2022.
The article was submitted 29.07.2022; approved after reviewing 05.09.2022; accepted for publication 09.09.2022.

Рецензент – Рытов М.Ю., кандидат технических наук, доцент, Брянский государственный технический университет.

Reviewer – Rytov M. Yu., Candidate of Technical Sciences, Associate Professor, Bryansk State Technical University.