Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.415.25

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ШИФРОВАНИЯ ДАННЫХ В МИКРОКОНТРОЛЛЕРНОЙ СИСТЕМЕ

Мишкин Александр Евгеньевич
Калужский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
alex.mishkin2000@gmail.com

Федоров Виктор Олегович
Калужский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
fedorov_vo@bmstu.ru

Аннотация

В данной статье рассматриваются три популярных алгоритма шифрования данных: RSA, AES, ГОСТ 28147-89. Шифрование производилось программными средствами в системе под управлением микроконтроллера с тактовой частотой 80 МГц. В статье были разобраны основные этапы работы каждого из алгоритмов. В сравнительном анализе учитывалось время выполнение и объем, занятый каждым из алгоритмов. Были построены таблицы сравнения алгоритмов по времени шифрования и дешифрования, а также графики времени цикла работы системы и объема, занимаемого алгоритмами. Данный сравнительный анализ может помочь в принятии обоснованных решений на основе выявленных различий и сходств.

Ключевые слова: AES, RSA, GOST 28147-89, шифрование данных, микроконтроллер

COMPARATIVE ANALYSIS OF DATA ENCRYPTION ALGORITHMS IN A MICROCONTROLLER SYSTEM

Mishkin Alexander Evgenievich
Kaluga branch of the federal state budgetary educational institution of higher education "Moscow State Technical University named after N.E. Bauman (national research university)"
alex.mishkin2000@gmail.com

Fedorov Viktor Olegovich
Kaluga branch of the federal state budgetary educational institution of higher education "Moscow State Technical University named after N.E. Bauman (national research university)"
fedorov_vo@bmstu.ru

ABSTRACT

This article discusses three popular data encryption algorithms: RSA, AES, GOST 28147-89. Encryption was carried out by software in a system controlled by a microcontroller with a clock frequency of 80 MHz. The article examined the main stages of the operation of each algorithm. The comparative analysis took into account the execution time and volume occupied by each of the algorithms. Tables were constructed comparing algorithms in terms of encryption and decryption time, as well as graphs of the system cycle time and the volume occupied by the algorithms. This comparative analysis can help you make informed decisions based on the differences and similarities identified.

Keywords: AES, RSA, GOST 28147-89, data encryption, microcontroller

В настоящее время технологии становятся все более важным и неотъемлемым элементом жизни. В таких реалиях безопасность и защита данных приобретают ключевое значение.

Микроконтроллерные системы, используемые в широком спектре приложений сталкиваются с растущим спросом на эффективные методы шифрования данных [1]. В этом контексте проведение сравнительного анализа алгоритмов шифрования в микроконтроллерных системах становится весьма актуальным исследованием.

Актуальность данного исследования в контексте ЧМИ проявляется в повседневных сценариях использования, таких как умные дома, медицинские устройства, автомобильные системы и другие области, где данные поступают от пользователя и передаются для обработки и хранения. Разработчики и инженеры ЧМИ сталкиваются с необходимостью выбора оптимальных методов шифрования для обеспечения прозрачности, удобства использования и, в первую очередь, безопасности для конечного пользователя [2].

Цель данного сравнительного анализа – исследование и сравнение производительности и ресурсоемкости различных алгоритмов шифрования данных (RSA, AES, ГОСТ 28147-89) в микроконтроллерных системах для определения оптимального алгоритма в контексте ограниченных ресурсов микроконтроллера.

К задачам исследования относятся:

Исследование основных этапов работы каждого из алгоритмов.

Проведение эксперимента по определению производительности и ресурсоемкости алгоритмов.

Рассмотрим основные этапы каждого из алгоритмов.

Алгоритм RSA. Алгоритм шифрования представляет собой математическую процедуру или набор шагов для кодирования данных.

В основе RSA лежит задача факторизации произведения двух простых больших чисел. Для шифрования используется простая операция возведения в степень по модулю N. Для расшифрования же необходимо вычислить функцию Эйлера от числа N, для этого необходимо знать разложение числа n на простые множители. В RSA открытый и закрытый ключ состоит из пары целых чисел. Закрытый ключ хранится в секрете, а открытый ключ сообщается другому участнику, либо где-то публикуется [3].

Алгоритм AES. AES – это современный стандарт шифрования данных. Он не имеет себе равных по уровню безопасности и защиты, который он предлагает. Преимущество симметричных систем как AES – они намного быстрее, чем асимметричный единицы. Это

связано с тем, что алгоритмы с симметричным ключом требуют меньшей вычислительной мощности. Поэтому, асимметричные ключи лучше всего использовать для передачи внешних файлов. Симметричные ключи лучше подходят для внутреннего шифрования [4].

Алгоритм ГОСТ 28147-89. ГОСТ 28147-89 — симметричный блочный алгоритм шифрования с 256-битным ключом, оперирует блоками данных по 64 бита.

Один из режимов его работы, гаммирования с обратной связью, является потоковым режимом блочного шифра. В общем, алгоритм можно представить следующим образом: исходное сообщение разбивается на блоки по 64 бита; на каждый блок, с помощью функции XOR, «накладывается» гамма, длиной 64 бита; гамма формируется шифрованием 64-битного блока «состояния» с помощью ключа в режиме простой замены; в момент начала шифрования сообщения блок принимается равным синхропосылке или вектору инициализации; в следующей итерации вместо синхропосылки используется зашифрованный блок текста из предыдущей.

Приведённая последовательность действий справедлива как для шифрования, так и расшифрования. Разница в том, откуда берётся зашифрованный блок текста для обработки следующего блока [5].

Сравнительный анализ будет проведен экспериментальным образом. Таким образом, будут получены реалистичные оценки затрат времени на шифрование и дешифрование с использованием алгоритмов, описанных выше. Эксперимент был проведен на системе под управлением микроконтроллера с тактовой частотой 80 МГц.

В ходе проведения эксперимента были получены данные, представленные в таблицах 1-4. В них отображено время выполнения процедуры шифрования и дешифрования, что и отражает производительность алгоритма в конкретной системе.

Сравнительная информация для алгоритма RSA для различных длин ключей представлена в таблицах 1 и 2.

Таблица 1. Сводная таблица для алгоритма RSA, длина ключа 1024 бит

	Время выполнения, с
Шифрование	0,6975
Расшифрование	4,1693

Таблица 2. Сводная таблица для алгоритма RSA, длина ключа 256 бит

	Время выполнения, с
Шифрование	0,135
Расшифрование	2,003

Сравнивания таблицы 1 и 2 можно отметить, что цикл шифрования данных алгоритмом RSA при длине ключа 1024 бита равен практически 698 мс. Такое время считается долгим для микроконтроллерной системы, поэтому алгоритм RSA с длиной ключа 1024 бита далее рассматриваться не будет.

Сравнительная информация для алгоритма AES для длины ключа 256 бит представлена в таблице 3.

Таблица 3. Сводная таблица для алгоритма AES

	Время выполнения, с
Шифрование	0,0495
Расшифрование	1,9193

По данным, представленным в таблице 3 можно сказать, что операция шифрования алгоритмом AES выполняется быстрее примерно в 3 раза, чем алгоритмом RSA при аналогичной длине ключа.

Сравнительная информация для алгоритма ГОСТ 28147-89 для длины ключа 256 бит представлена в таблице 4.

Таблица 4. Сводная таблица для алгоритма ГОСТ 28147-89

	Время выполнения, с
Шифрование	0,045
Расшифрование	0,1755

По полученным данным построим временную диаграмму для одного цикла работы системы для всех представленных алгоритмов. Она представлена на рисунке 1.

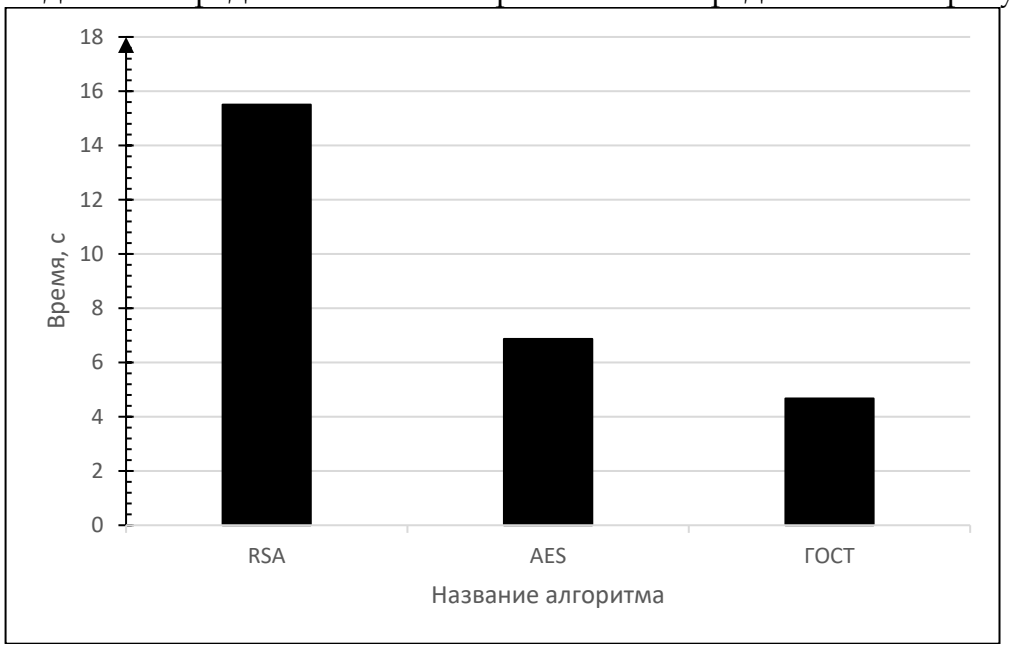

Рисунок 1. Время работы 1 цикла системы

Помимо затрат процессорного времени, для разработки этих алгоритмов на микроконтроллере представляет интерес объем кода, необходимый для реализации. Для упомянутых выше алгоритмов приведем диаграмму значений объема занимаемого кода. Она представлена на рисунке 2.

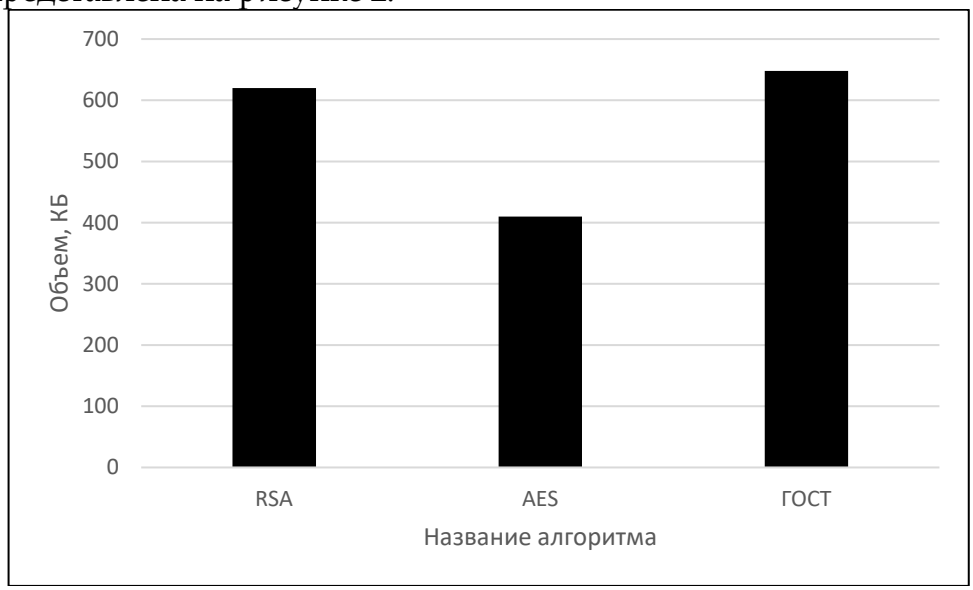

Рисунок 2. Объем, занимаемый алгоритмами

На диаграмме показан такой параметр, как ресурсоемкость. Как видно по рисунку, наиболее ресурсоемкий алгоритм – ГОСТ, наименее – AES.

По результатам сравнительного анализа можно выделить алгоритмы AES – как относительно производительный, но наименее ресурсоемкий, и алгоритм ГОСТ 28147-89 –

как наиболее производительный, но также и наиболее ресурсоемкий. Конкретный алгоритм стоит выбирать из условий решаемой задачи, а также производительности системы на которой она решается. Для наиболее быстрого шифрования и дешифрования данных стоит отметить алгоритм ГОСТ, если же скорость выполнения не критична, то алгоритм AES вероятнее лучше подойдет, в связи с его меньшей ресурсоемкостью.

Список литературы:

1. Мишкин А.Е., Чухраев И.В. Анализ методов обработки информации в микропроцессорных системах // Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в ВУЗе. Материалы Всероссийской научно-технической конференции. Москва, 2022, с. 91-95.
2. Макаров Д.Е. Человеко-машинный интерфейс (ЧМИ). Использование облачного ЧМИ и его сравнение с другими ЧМИ // Научные аспекты глобализационных процессов. Сборник статей международной научно-практической конференции, Уфа, 2014, с.13-14.
3. Абдикаликов К. А. Криптографическая система шифрования данных RSA // Наука и мир, 2019, №10-1(74), с. 8-11.
4. Нурмухамедов Д.А. Исследование стандартов шифрования AES-128 и AES-256 // Научное сообщество студентов. Междисциплинарные исследования (Новосибирск, 04 ноября 2021), Новосибирск, 2021, с.37-42.
5. Бабенко Л.К., Ищукова Е.А., Маро Е.А. Исследование стойкости алгоритма шифрования ГОСТ 28147-89 // XII Международная научно-практическая конференция «ИБ-2012» (Таганрог, 25-29 июня 2012), Таганрог, 2012, с. 309-316.

References:

1. Mishkin A.E., Chukhraev I.V. Analysis of information processing methods in microprocessor systems // Science-intensive technologies in instrumentation and mechanical engineering and the development of innovative activities in universities. Materials of the All-Russian Scientific and Technical Conference. Moscow, 2022, p. 91-95.
2. Makarov D.E. Human-machine interface (HMI). The use of cloud HMI and its comparison with other HMIs // Scientific aspects of globalization processes. Collection of articles of the international scientific and practical conference, Ufa, 2014, pp. 13-14.
3. Abdikalikov K. A. Cryptographic data encryption system RSA // Science and World, 2019, No. 10-1(74), p. 8-11.
4. Nurmukhamedov D.A. Study of encryption standards AES-128 and AES-256 // Scientific community of students. Interdisciplinary research (Novosibirsk, November 04, 2021), Novosibirsk, 2021, pp.37-42.
5. Babenko L.K., Ishchukova E.A., Maro E.A. Research on the strength of the GOST 28147-89 encryption algorithm // XII International Scientific and Practical Conference “IB-2012” (Taganrog, June 25-29, 2012), Taganrog, 2012, p. 309-316.