УДК 003.26

РАЗРАБОТКА И АНАЛИЗ СКОРОСТИ РАБОТЫ БЛОЧНОГО СИММЕТРИЧНОГО АЛГОРИТМА ШИФРОВАНИЯ AES С ИСПОЛЬЗОВАНИЕМ РАЗЛИЧНЫХ ЯЗЫКОВ ПРОГРАММИРОВАНИЯ

А. А. Стариков, А. В. Лысенко, А. А. Клевцов
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Изучен и проанализирован уже существующий алгоритм шифрования AES, его достоинства и недостатки. Представлена концепция самостоятельно разработанного алгоритма на трех различных языках. Результатом данной статьи является анализ алгоритма AES, его применение в криптографии, а также созданный работающий алгоритм шифрования AES и его временные характеристики, соответствующие каждому используемому языку, показывающие за какую единицу времени обрабатывается исследуемый алгоритм.

Ключевые слова: шифрование, расшифрование, криптостойкость, блок данных, расписание ключей, производительность, алгоритм, программирование.

DEVELOPMENT AND ANALYSIS OF THE OPERATION SPEED OF A BLOCK SYMMETRIC AES ENCRYPTION ALGORITHM USING VARIOUS PROGRAMMING LANGUAGES

A. A. Starikov, A. V. Lysenko, A. A. Klevtsov
Don State Technical University (Rostov-on-Don, Russian Federation)

In this article, the already existing AES encryption algorithm, its advantages and disadvantages have been studied and analyzed. The concept of a self-developed algorithm in three different languages is presented. The result of this article is the analysis of the AES algorithm, its application in cryptography, as well as the created working AES encryption algorithm and its temporal characteristics corresponding to each language used, and showing in what unit of time the algorithm under study is processed.

Keywords: encryption, decryption, cryptographic strength, data block, key schedule, performance, algorithm, programming.

Введение. На сегодняшний день криптография развивается намного стремительнее, чем раньше. Злоумышленники находят всё больше уязвимостей и способов для взлома различных алгоритмов шифрования. Сегодня представить себе мир без алгоритмов шифрования не представляется возможным. Любая передача, хранение конфиденциальных данных, выполнение транзакций, отправка электронных писем, IP-телефония — это далеко не полный список того, что должно в обязательном порядке подвергаться шифрованию для минимизирования количества атак злоумышленников и сохранения конфиденциальных данных. Именно для обеспечения безопасности информации разработчики совместно с математиками постоянно трудятся над разработками новых или усовершенствованием существующих алгоритмов и всевозможных средств шифрования.

Основная часть. Все существующие алгоритмы шифрования делятся на симметричные и ассиметричные, блочные и поточные. Симметричные алгоритмы используют один ключ как для шифрования, так и для расшифрования информации. Достоинствами симметричных алгоритмов шифрования является высокая скорость работы и небольшая длина ключа. К недостаткам данного типа алгоритмов можно отнести сложность управления ключами в большой сети, необходимость

использования защищенного или секретного канала связи, шифрования ключа для исключения риска его компрометации [1]. В отличии от симметричных, ассиметричные алгоритмы используют два ключа — открытый и закрытый. Шифрование происходит с использованием открытого ключа, который можно передавать по незащищенному каналу связи. При расшифровании используется закрытый ключ, который хранится у получателя информации [1]. К достоинствам можно отнести отсутствие необходимости в использовании защищенного канала связи при передаче открытого ключа, а также необходимость в дополнительном шифровании данного ключа. Главными недостатками таких алгоритмов является низкая скорость шифрования и расшифрования, в сравнении с симметричными алгоритмами из-за большой длины ключа и сложных математических вычислений, а также их высокая ресурсоемкость [2].

Целью данной статьи являлась реализация алгоритма шифрования AES (Advanced Encryption Standard) на разных языках программирования и анализ времени, затрачиваемого на его работу.

Описание алгоритма. Рейндал (Rijndael) — победитель конкурса AES, является блочным симметричным алгоритмом шифрования, использующим в своей основе SP сеть, сменивший название на AES, под которым в настоящее время он всемирно известен [1]. Данный алгоритм имеет постоянную размерность блока в 128 бит и возможность работы с тремя размерностями ключей: 128, 192, 256 бит. Количество раундов зависит от длины выбранного ключа: 10, 12, 14 соответственно. Внутри алгоритма используется четыре основные функции: SubBytes, ShiftRows, MixColumns и AddRoundKey [3].

– SubBytes — обрабатывает каждый байт состояния, производя нелинейную замену байтов, используя стандартизированные таблицы замен, именуемые как S-box.

– ShiftRows — обрабатывает строки состояния, выполняя трансформацию, посредством которой строки циклически сдвигаются на n-байт, в зависимости от номера строки по горизонтали.

– MixColumns — выполняет смешивания четырех байт каждой колонки состояния с помощью обратимой линейной трансформации, обрабатывая каждую колонку. Функция представляет их как полином третьей степени и производя над ними умножения в поле Галуа (GF) 2^8 по модулю x^4+1 на многочлен $3x^3+x^2+x+2$.

– AddRoundKey — выполняет побитовый XOR каждого байта состояния с байтом раунд ключа, предварительно получив раундовый ключ с помощью функции расширения ключа KeyExpansion.

При шифровании функции используются в следующем порядке: SubBytes, ShiftRows, MixColumns, AddRoundKey. Кроме последнего раунда, в нем не используется функция MixColumns. Для расшифрования применяются обратные преобразования, используемые в следующих функциях InvShiftRows, InvSubBytes, AddRoundKey и InvMixColumns [3].

Программная реализация. Данный алгоритм шифрования представлен на трех языках программирования. Выбранные языки сильно отличаются по скорости работы за счет используемых ими программ, выполняющих обработку и выполнение исходного кода, компилятора или интерпретатора. Компилятор переводит исходный код программы в машинный набор кодов, сразу анализируя весь текст программы. Интерпретатор, в свою очередь, — программа, которая построчно анализирует, обрабатывает и выполняет исходный код языка программирования, что снижает скорость работы, в сравнении с компилируемыми языками. Стоит заметить, что интерпретаторы активно развиваются и скорость интерпретации постоянно растет.

PHP — си-подобный язык, использующий интерпретатор, является самым популярным языком в сфере web-программирования, на php работает около 70 % всех сайтов [4].

GO — компилируемый многопоточный язык от компании Google, молодой язык программирования, целью которого стать современной альтернативой C/C++ [5].

Python — интерпретируемый язык программирования, на данный момент является самым популярным языком. Однако если сравнивать с вышеперечисленными языками, он является менее производительным [6].

Исходя имеющихся данных можно предположить, что самой быстрой будет реализация, написанная на языке программирования Golang. Проведя тестирование написанного алгоритма, можно будет подтвердить данный результат и понять, насколько будет значимая разница в скорости шифрования и расшифрования исходного текста.

Оценка времени выполнения. Для выполнения оценки временных характеристик шифрования и расшифрования использовались функции Microtime. Тестирование проводилось 15 раз на трех устройствах, 5 лучших результатов усреднялись, сравнивалось время выполнения как и отдельных функций, так и алгоритма целиком и с разной длиной ключа. Для тестирования использовались следующие устройства:

- Apple macbook, apple m1 chip, 16gb unified memory;
- HP, ryzen 5 4500u, 16 gb ram;
- Lenovo, intel core i3 6006u, 8gb ram.

Лучшие усредненные результаты представлены в таблице 1.

Таблица 1

Время работы алгоритма AES на различных языках

Язык программирования	Лучшие усредненные результаты		
	Устройство 1	Устройство 2	Устройство 3
PHP	00,0048	00,0035	00,0048
Python	00,0435	00,0230	00,0250
GO	00,0040	00,0035	00,0038

Опираясь на данные тестирования, можно заключить, что лучшим языком для программирования является Golang, чуть хуже Python. Стоит отметить, что язык PHP, хоть и не является самым быстрым среди выбранных, показал очень хороший результат. Таким образом лучшим выбором для реализации алгоритма шифрования AES оказался Golang и компилируемые языки соответственно. При этом PHP последних версий, которые используют современный интерпретатор, тоже возможно использовать, так как это достаточно популярный, хоть и не такой молодой как Go, но стремительно развивающийся язык.

Заключение. Реализован алгоритм шифрования и расшифрования AES на трех языках программирования: PHP, Python, GO. Каждая реализация отображает время обработки данного алгоритма, на основе которого был сделан вывод, что на языке Golang и PHP время, затрачиваемое на шифрование и расшифрование, является наименьшим по сравнению с Python.

Библиографический список

1. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа : учебное пособие для студентов вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Гелиос АРВ, 2006. — 376 с. — ISBN 5-85438-149-4.

2. Панасенко, С. П. Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. — Санкт Петербург: БХВ-Петербург, 2009. — 576 с.

3. Habr. Как устроен AES / habr.com : [сайт]. — URL : https://habr.com/ru/post/112733/ (дата обращения : 02.05.2022).

4. PHP. Справочная информация / php.net : [сайт]. — URL : https://www.php.net/ (дата обращения 01.05.2022)

5. Golang. Справочная информация / go.dev : [сайт]. — URL : https://go.dev/ (дата обращения : 01.05.2022).

6. Python. Справочная информация / docs-python.ru : [сайт]. — URL : https://docs-python.ru (дата обращения :01.05.2022).

Об авторах:

Стариков Александр Александрович, студент кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1) starik0v2000@yandex.ru

Лысенко Андрей Владимирович, студент кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1) andrikgod1312@mail.ru

Клевцов Алексей Алексеевич, студент кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1) klevtsov.leha@mail.ru

About the Authors:

Starikov, Aleksandr A., Student of the Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF) starik0v2000@yandex.ru

Lysenko, Andrey V., Student of the Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF) andrikgod1312@mail.ru

Klevtsov, Aleksey A., Student of the Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF) klevtsov.leha@mail.ru