УДК 004.056.55

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМА ШИФРОВАНИЯ НА ОСНОВЕ АЛГОРИТМА КУБИКА РУБИКА И AES

И.Е. ИВАНЕНКО
(Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ)

Рассматривается сравнение алгоритмов AES и алгоритма на основе алгоритмов кубика Рубика. Проведён анализ общих характеристик и работы алгоритмов.

Введение. AES – аббревиатура от Advanced Encryption Standard (перевод с англ. усовершенствованный стандарт шифрования).

После открытия в 1997 г. Национальным Институтом Стандартов и Технологии США (NIST) программы по разработке AES состоялись 3 этапа международного конкурса. Новый стандарт должен был иметь:

- стойкость не меньше, чем у 3DES.
- скорость шифрования больше скорости 3DES.
- прозрачную структуру.
- эффективную реализацию на платформе Pentium Pro.
- эффективную аппаратную реализацию.

Победителем конкурса стали бельгийцы Йоан Дамен и Винсент Реймен с алгоритмом RIJNDAEL (читается Рейн-дал от первых букв авторов). Стандарт начал действовать с 2002 г.

Алгоритм шифрования на основе кубика Рубика является шифром перестановки. Метод перестановки заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов, т.е. преобразования приводят к изменению только порядка следования символов исходного сообщения.

Данный алгоритм шифрования на основе алгоритма кубика Рубика был изменен для работы не с символами шифруемого текста, а с массивом байт, который получается путем преобразования шифруемого текста. Данный алгоритм является симметричным алгоритмом шифрования.

Сравнительный анализ алгоритмов.

Таблица 1. – Сравнение общих характеристик

Критерий сравнения	**AES**	**Алгоритм шифрования на основе алгоритма кубика Рубика**
1. Размер блока шифрования	AES зашифровывает и расшифровывает 128-битовые блоки данных	Данный алгоритм зашифровывает и расшифровывает 48-битовые блоки данных
2. Длина ключей шифрования	AES позволяет использовать три различных ключа длиной 128, 192 или 256 бит	Для работы алгоритма могут быть использованы ключи 128 бит, 256 бит, 512 бит, 1024 бита и 2048 бит
3. Число раундов	От размера ключа зависит число раундов шифрования: длина 128 бит – 10 раундов; длина 192 бита – 12 раундов; длина 256 бит – 14 раундов.	От размера ключа зависит число раундов шифрования: длина 128 бит – 12 раундов; длина 256 бит – 16 раундов; длина 512 бит – 20 раундов; длина 1024 бита – 24 раунда; длина 2048 бит – 32 раунда.

Исходя из данный таблицы 1, алгоритмы отличаются размером блока шифрования. Алгоритм шифрования на основе алгоритма кубика Рубика охватывает больший диапазон ключей, однако при одинаковом размере ключа имеет большее количество раундов, что может увеличить время работы алгоритма. Сравнение времени работы алгоритмов не имеет смысла без дальнейшей оптимизации алгоритма на основе алгоритма кубика Рубика, так ка встроенные реализации алгоритма AES являются оптимизированными и выполняется в многопоточном режиме, тогда алгоритм на основе алгоритма кубика Рубика работает в однопоточном режиме и нуждается в дальнейшей оптимизации.

В таблице 2 представлены результаты работы AES и алгоритма на основе алгоритмов кубика Рубика на различных данных. Для работы алгоритмов был использован один и тот же ключе длинной 256 бит.

Таблица 2. – Результаты работы алгоритмов

Входной текст	**Зашифрованный текст AES**	**Зашифрованный текст алгоритма на основе алгоритмов кубика Рубика**
11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11	cc cf e 4 f 83 69 e2 a7 49 b9 2f d5 c0 6f d7 17 bc d1 ef dc 23 22 6c ac c1 49 c0 f7 e6 72 7c 63 34 26 d1 27 40 65 91 b7 ce 28 61 8b c da c7	a2 40 50 12 49 f2 12 f0 28 94 8b ef c8 ce c7 81 97 ab ae fe 65 c9 19 55 39 a7 42 84 72 40 85 78 f6 5 d 4b 99 c2 80 66 b1 a9 19 3b f 72 86 e
11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 10	49 3a 55 c4 df 86 8f 1f b 5b 90 40 d6 5 a9 49 a4 33 67 a 1f de ad a9 be f3 c6 ee 6a 1d 71 72 74 99 aa 5d 3 4a d1 a5 3d 4e f5 39 b2 24 da dd	6f 71 b9 1f c3 4b 54 ef 55 fc 39 c1 60 56 9a de a3 a7 b3 54 55 14 ed d9 2e 9f 4b 9a 8d 72 5 cf 4c 29 be 72 8f c3 46 2f f0 74 69 d5 a8 7b b3 a6
11 22 33 66 55 44 55 44 77 88 99 66 44 45 36 12	67 35 e5 1e 22 62 14 ca 7c 3e 57 3b c0 c7 59 7e e7 af 22 ed f4 b9 29 37 91 d2 17 e6 c6 23 0 c0 23 73 8 9c 8c c8 b9 98 5c f5 a3 ba e0 9 dc 7d	bd f8 5f f4 d7 49 6a 62 92 54 75 f2 3c e0 31 15 36 fc 3f ed 78 ce bf c8 a2 ad 25 4f 7e 57 2 cf 1c 60 e8 c9 bc e3 36 fc b8 ed c4 24 3d a 5f d5
11 22 33 66 55 44 55 44 77 88 99 66 44 45 36 11	5 fa c0 bb 6a 61 81 f3 2b 34 f6 2a dd 38 5 59 a8 b8 85 eb 2f ed 6d 96 44 38 25 d5 eb a2 d0 79 14 14 d6 b6 f8 38 73 70 57 21 99 b7 1e fe f1 5e	cd e4 96 2a 5 1e 4 11 1e c7 de 13 9d 7a 6d ed a8 38 5f 80 7a 6 3e 15 e6 a9 fc 44 43 54 f4 3d 9 11 16 91 f 35 f4 ed 2e 48 bd c5 6a 8c f0 cb
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	2 97 6c 34 50 fd 7a 19 5e a7 9d ae 98 19 f3 1b 83 ea 5f 6a 2f db 28 67 bb bc dd 11 11 f3 e8 c6 78 7a 88 2d b9 ff f5 69 94 3d f1 89 9c dd 5 5b	2e 24 28 fb 9a 5e 84 c0 7b 84 c2 74 68 d6 1f ce 81 fd e6 fa 3a 44 e0 79 db f7 23 23 f7 3 91 12 ae ec 92 42 23 8c 65 e0 7 e3 17 a8 1c eb ff 7b
10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0 57 be 43 5e 52 6d 71 b1 bb 57 10 19 bc f8 e5 a7 b9 40 b 9e 8 28 82 fd 8c 49 a9 1a 5b ba 9d 24 55 d4 74 1e 71 4 68 9c ff 33 8 eb 6e 3b b4	6a 77 73 88 ae 6a 3 ad 3e 23 1f 70 37 3c 1b 56 75 e5 d 37 b9 63 64 9d 2e 89 6f a0 93 97 b6 bd e0 f9 a9 da d4 ff a0 39 f7 5f 73 59 8a 87 e4 c4

Исходя из данных таблицы 2 можно сделать вывод, что оба алгоритма обладают так называемым «лавинным эффектом» и зашифрованные данные обладают свойством нелинейности. «Лавинный эффект» означает, что изменения в одном бите входных данных должны распространяться по всем битам выходных данных. В свою очередь нелинейность означает невозможность подобрать линейную функцию, хорошо аппроксимирующую данное преобразование.

Заключение. В ходе данного исследования были получены результаты, исходя из которых можно сделать вывод, что алгоритм на основе алгоритмов кубика Рубика обладает некоторыми преимуществами, такими как больший диапазон ключей для шифрования по сравнению с алгоритмом AES. Так же исходя из результатов данный алгоритм обладает рядом существенных недостатков, такими как скорость работы алгоритма, по сравнению с алгоритмом AES, небольшой размер блока шифрования равный 48 бита, что негативно сказывается на скорости работы и при больших объемах данных может быть нарушен «лавинный эффект».

ЛИТЕРАТУРА

1. Материал из StudFiles — файловый архив студентов. Шифры перестановки [Электронный ресурс]. Режим доступа: https://studfiles.net/preview/5470123/page:8/. Дата доступа: 20.09.2018.
2. Н. Птицын. Приложение теории детерминированного хаоса в криптографии / Н. Птицын; доцент(к.н.) к.т.н. – Москва: МГТУ им. Н.Э. Баумана, 2002. 80 с.
3. Ю.А.Гатчин, А. Г. Коробейников. Основы криптографических алгоритмов. Учебное пособие / Ю.А.Гатчин; доктор технических наук, профессор кафедры проектирования и безопасности компьютерных систем. – СПб: ГИТМО (ТУ), 2002. 29 с.
4. Жданов О.Н., Актуальные проблемы безопасности информационных технологий/ Жданов О.Н. кандидат физико-математических наук, Профессор Российской Академии Естествознания - Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2009. – 144 с.
5. Общее описание криптоалгоритма AES [Электронный ресурс]. – Режим доступа: http://bit.nmu.org.ua/ua/student/metod/cryptology/лекция%209.pdf – Дата доступа: 20.09.2018.