Дружкова Ирина Викторовна,
студент кафедры информационно-телекоммуникационных
систем и технологий,
НИУ «БелГУ»,
(Белгород, Россия)
Игрунова Светлана Васильевна,
доцент кафедры информационных систем,
НИУ «БелГУ»,
(Белгород, Россия)
Нестерова Елена Викторовна,
старший преподаватель кафедры информационных систем,
НИУ «БелГУ»,
(Белгород, Россия)

МОДЕЛИРОВАНИЕ РАБОТЫ АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ AES НА ЯЗЫКЕ C++

Аннотация

Для современной криптографии характерно использование открытых алгоритмов шифрования, предполагающих использование вычислительных средств. В данной статье речь пойдет о шифре AES - Advanced Encryption Standard 128-bit version (так же известный как Rijndael), принятый в качестве ныне действующего стандарта шифрования правительством США. Этот алгоритм в настоящее время широко используется в различных информационных системах и технологиях.

Ключевые слова

Криптография; стандарты шифрования; AES.

В современном мире защита информации является одной из самых актуальных проблем. Это связано с тем, что с каждым годом компьютерная информация играет все более важную роль в нашей жизни. Информации угрожает множество самых разнообразных опасностей, начиная от сугубо технических неполадок и заканчивая действиями злоумышленников.

Шифрование представляет собой сокрытие информации от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней [2]. Пользователи называются авторизованными, если у них есть соответствующий ключ для расшифрования информации.

Для усиления защищённости данных и облегчения работы с шифрованием и расшифрованием со стороны человека используются криптосистемы - это завершенные комплексные модели, способные производить двусторонние криптопреобразования над данными произвольного объема [3].

Чтобы обеспечить полную защиту информации, необходимо учитывать возможные причины ненадежности криптосистем:

1. Невозможность применения стойких криптоалгоритмов.
2. Ошибки в реализации криптоалгоритмов.

3. Неправильное применение криптоалгоритмов.
4. Человеческий фактор.

Целью любой системы шифрования является максимальное усложнение получения доступа к информации неавторизованными лицами, даже если у них есть зашифрованный текст и известен алгоритм, использованный для шифрования. Пока неавторизованный пользователь не обладает ключом, секретность и целостность информации не нарушается.

Рассматриваемый алгоритм относится к симметричным криптосистемам, где для шифрования и расшифрования информации используется один и тот же ключ (секретный ключ)[4].

Данные для шифрования разбиваются на блоки по 128 бит. AES является байтовым алгоритмом, таким образом полученный блок представляется в формате матрицы 4×4, каждый элемент которой занимает 1 байт (8 бит) [1]. Матрицы заполняются шестнадцатеричными числами, каждое из которых представляет собой символ по таблице ASCII. То же самое происходит и с ключом длинной 128 бит.

Алгоритм имеет четыре трансформации, каждая из которых своим образом влияет на состояние блока: SubBytes (подстановка), ShiftRows (циклический сдвиг строк), MixColumns (смешивание) и AddRoundKey (добавление раундового ключа). Все итерации можно представить в виде схемы (рис. 1).

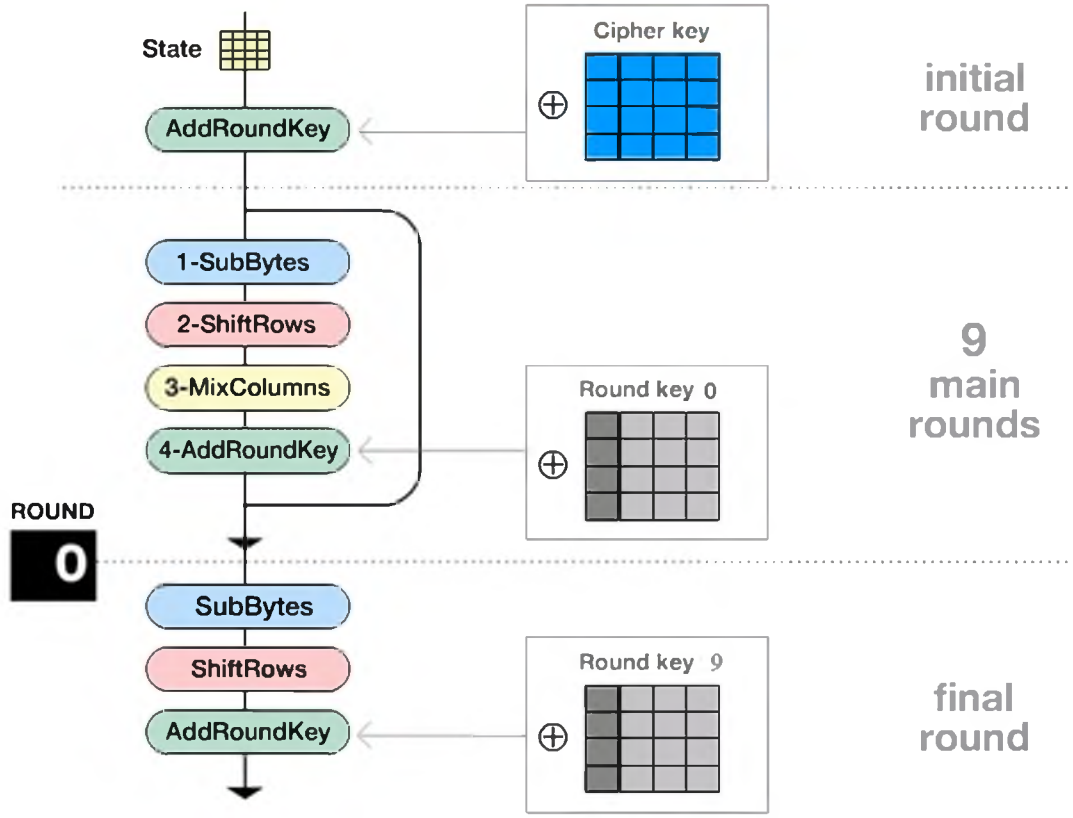

Рисунок 1. **Процесс шифрования блока**

Реализация алгоритма осуществлялась на программном языке C++. С помощью полученной программы был проведен анализ алгоритма на криптостойкость.

Порядок использования данной криптосистемы будет следующим:

1. Безопасно создается, распространяется и сохраняется симметричный секретный ключ.

2. Отправитель использует алгоритм AES, используя секретный симметричный ключ, для открытого текста. Неявно производится аутентификация, так как только отправитель знает секретный ключ и может зашифровать открытый текст, и только получатель знает тот же ключ и может расшифровать полученный шифротекст.

3. Отправитель передает зашифрованный текст. Симметричный секретный ключ никогда не передается по незащищенным каналам связи.

4. Получатель использует тот же самый алгоритм с тем же секретным ключом к зашифрованному тексту для восстановления исходного текста. Его успешное восстановление также аутентифицирует того, кто знает секретный ключ.

Первым тестом послужит сравнение полученных зашифрованных сообщений из одного и того же открытого текста, но измененного на один символ. Исходный текст для шифрования использован следующий: «Hello, world!», для удобства состоящий из 16 символов (1 блок). Полученный результат отображен в таблице 1.

Таблица 1**. Результат тестирования при изменении 1 символа исходных данных**

Исходный текст	«Hello, world!»	«Mello, world!»
Шифроблок	10 3f ea 40 bb a3 20 15 b1 c6 2b b8 d4 53 88 76	4d b9 1f d5 ed fc a1 11 bd 2c 9c f 3c 7b bd 2

Из полученной таблицы можно сделать вывод, что при изменении одного символа блока, меняется весь блок. Это говорит о наличии потери соответствия битов между блоками открытых и зашифрованных данных.

Были так же проведены тесты на случайность псевдослучайной последовательности (зашифрованного текста). Для исследования было зашифровано 20000 бит. Результаты представлены на рисунке 2. В результате полученный зашифрованный текст был признан случайной последовательностью.

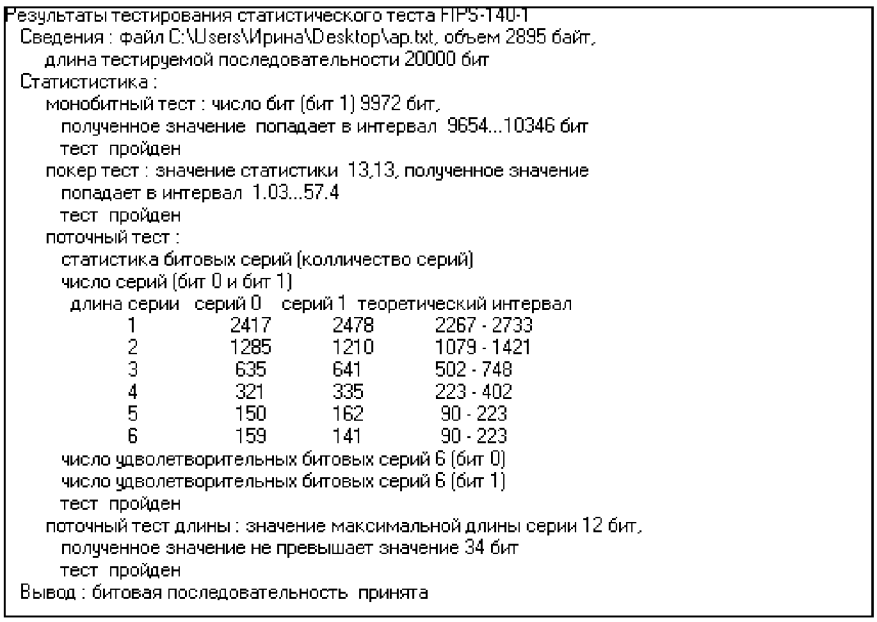

Рисунок 2. **Статический тест шифроблока**

В ходе исследования можно сделать следующие выводы:

1. Зашифрованный текст является случайной последовательностью.
2. В ходе шифрования теряется зависимость между битами открытого и зашифрованного текста.
3. Длина ключа алгоритма является приемлемой для надежной стойкости.
4. Простота алгебраического представления является большим преимуществом, что важно для реализации и быстродействия алгоритма.

Список использованных источников:

1. Стоякин Е. В., Хрусталев В. И. Принцип пошагового преобразования данных в алгоритмах шифрования ГОСТ28147-89 и AES //Новые задачи технических наук и пути их решения. – 2015. – С. 133-136.

2. Лапонина, О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействияю. – 2005. – 608 с.

3. Алексеев Д. М., Кутняк Н. А. Программная реализация алгоритма шифрования AES //Инновационная наука. – 2016. – №. 4-3 (16).

4. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. – 2001. – 176 с.