УДК 004.056.55

Студ. А.О. Николаенков, И.С. Денисюк
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КРИПТОСТОЙКОСТИ AES И DES

Стандарт шифрования данных DES за 20 лет стал стандартом мирового уровня. Так как DES является одним из первых алгоритмов симметричного блочного шифрования, и в свое время был очень популярен, он хорошо изучен и известно множество вариантов атак на него. К основным недостаткам DES можно отнести: проблему слабых и полуслабых ключей, ориентацию на аппаратную реализацию. Как альтернатива, был разработан стандарт AES [1]. Сравнение обоих стандартов приведено в табл. 1.

Таблица 1 – Сравнение параметров стандартов

Критерий оценки	**AES**	**DES**
Длина блока в битах	128	64
Длина ключа в битах	128/192/256	56 (+ 8 контрольных бит)
Принцип работы	SP – сеть	Сеть Фейстеля
Число раунда	10/12/14 (зависит от длины ключа)	16

Изучив табл. 1, несложно сделать вывод об очевидных преимуществах AES перед DES. Проведем исследование быстродействия работы двух шифров с большим по размеру исходным текстом (рис.1).

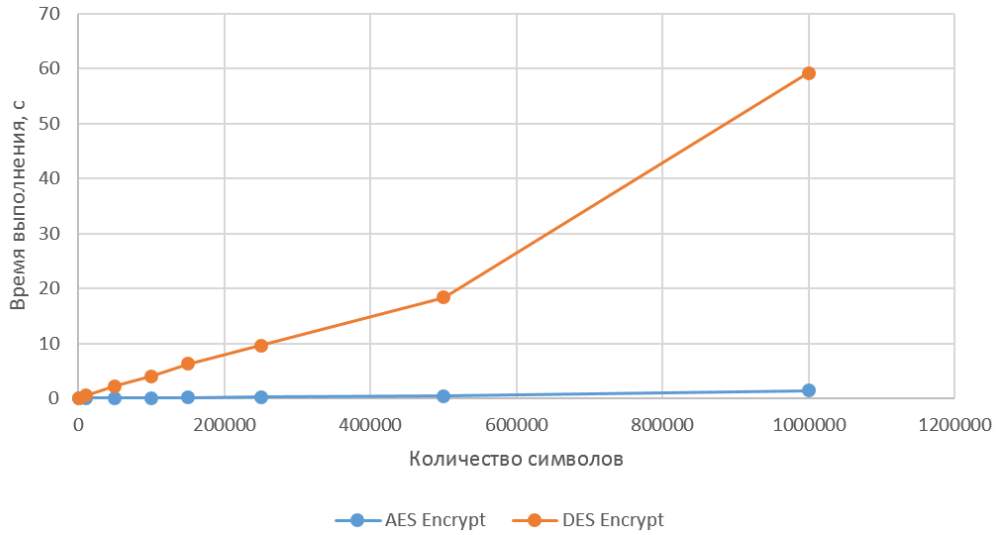

Рисунок 1 — График зависимости времени выполнения от длины сообщения

Программные реализации были написаны нами собственноручно, и не стоит исключать влияние недостатков оптимизации алгоритма.

В основе криптостойкости блочных шифров лежит идея К. Шеннона о представлении составного шифра таким образом, чтобы он обладал двумя важными свойствами: рассеиванием и перемешиванием. Рассеивание должно скрыть отношения между зашифрованным текстом и исходным текстом. С понятием рассеивания тесно связано понятие “лавинный эффект”. Лавинный эффект – важное криптографическое свойство для шифрования, которое означает, что изменение значения малого количества битов во входном тексте или в ключе ведет к «лавинному» изменению значений выходных битов шифротекста [2].

Благодаря постоянным перестановкам в DES, изменение одного бита в ключе или сообщении повлияет на каждый бит спустя 5 раундов.

В AES лавинный эффект появляется следующим образом: в первом раунде операция перемешивания колонок распространяет изменения одного байта на все 4 байта колонки, после чего во втором раунде применение операций перемещение строк и перемешивание колонок распространяет изменения на всю таблицу.

В 1990 г. исследователи, используя метод дифференциального криптоанализа, нашли способ вскрытия DES, более эффективный, чем вскрытие методом грубой силы. Базовый метод дифференциального криптоанализа – это атака на основе подобранных открытых текстов. Для проведения атаки используются пары открытых текстов, связанных определенной разницей (табл. 2). Так как единственные нелинейные элементы в схеме – это S-блоки, то данный метод хорошо подходит для взлома DES.

Таблица 2 – Атаки на DES

Методы атак	Известные открытые тексты	Количество операций
Полный поиск	1	2^{55}
Линейный криптоанализ	2^{43}(85%)	2^{43}
Линейный криптоанализ	2^{38}(10%)	2^{50}
Дифференциальный криптоанализ	2^{55}	2^{55}

Так как классический DES уже изжил свое и не является криптостойким, существуют и его модификации, например, 3DES, который заключается в тройном преобразовании входного сообщения тремя разными ключами. При таком условии длина сообщения очевидно

не меняется, а длина ключа становится равной 168 бит, а в сумме с битами четности 192. При таком подходе суммарное число раундов увеличивается в 3 раза.

Многие исследователи проверяли AES на прочность, однако серьезных уязвимостей у него обнаружено не было. Настоящая атака применима ко всем версиям AES. Количество итераций для поиска ключа к AES-128 выражается числом 8*1037; у 1 трлн компьютеров, способных проверять по 1 млрд ключей в секунду, на поиск ключа уйдет 2 млрд лет (табл. 3).

Таблица 3 – Методы атак на AES

Метод атак	Количество раундов	Известные открытые текста	Количество операций
Встреча посередине	2	2	2^{32}
Частичные суммы	6	2^{32}	2^{42}
Биклик	10	2^{128}	2^{125}

Большинство атак на AES-128 основывается на нескольких идеях и свойствах шифра, описанных в том числе ещё в исходной работе 1998 г., представляющей алгоритм Rijndael. Наиболее сильные атаки практической трудоёмкости используют метод «Квадрат», а наиболее сильные атаки теоретического понижения стойкости большого числа раундов AES основаны на методах «встреча посередине» и «Биклик» и их комбинациях.

Максимальное количество раундов AES-128, которое удаётся атаковать с практической трудоёмкостью, равно шести. Такое количество раундов достигается с помощью метода частичных сумм, поэтому для атаки необходимо 2^{33} подобранных открытых текстов.

ЛИТЕРАТУРА

1. National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard, 2001, URL: http://csrc.nist.gov/ publications/fips/fips197/fips-1, доступ: 20.04.2021.

2. Урбанович, П. П. Лабораторный практикум по дисциплинам «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации». В 2 ч. Ч. 1. Кодирование информации: учеб.-метод. пособие для студентов учреждений высшего образования / П. П. Урбанович, Д. В. Шиман, Н. П. Шутько. – Минск: БГТУ, 2019. – 116 с.