УДК 681.3.06

В. О. Берников
Белорусский государственный технологический университет

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КРИПТОСТОЙКОСТИ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Проанализированы наиболее распространенные криптоаналитические атаки на блочные симметричные алгоритмы шифрования. Описаны основные методы, которые используются в атаках, выявлены преимущества и недостатки каждого метода. Рассмотрены и проанализированы наиболее известные в настоящее время симметричные криптосистемы на основе сравнения следующих характеристик: длина ключа должна составлять не менее 128 бит с возможностью быстрого расширения до 256 бит, длина обрабатываемого блока должна быть не менее 128 бит, структура каждого раунда алгоритма не должна иметь сложную математическую модель по причине продуктивности анализа в целом, а также данные алгоритмы шифрования должны быть устойчивыми к современным криптоаналитическим атакам. Приведена количественная оценка стойкости алгоритмов по следующим критериям: криптостойкость, запас криптостойкости, скорость расширения ключа, защита от атак по времени выполнения, реализация лавинного эффекта, возможность быстрого расширения ключа и возможность параллельных вычислений. Выявлены преимущества и недостатки каждого алгоритма шифрования. Выбран наиболее стойкий к взлому симметричный блочный алгоритм шифрования из рассмотренных.

Ключевые слова: симметричная криптосистема, криптостойкость, криптоаналитическая атака.

V. O. Bernikov
Belarusian State Technological University

COMPARATIVE ANALYSIS OF THE CRYPTOGRAPHIC RESISTANCE OF SYMMETRIC ALGORITHMS ENCRYPTION

The most common cryptanalytic attacks on block symmetric encryption algorithms are analyzed. The main methods that are used in attacks are described, the advantages and disadvantages of each method are identified. The most well-known symmetric cryptosystems are currently reviewed and analyzed based on a comparison of the following characteristics: the key length should be at least 128 bits with the ability to quickly expand to 256 bits, the length of the processed block should be at least 128 bits, the structure of each round of the algorithm should not have a complex mathematical model due to the productivity of the analysis as a whole, as well as these encryption algorithms must be resistant to modern cryptanalytic attacks. A quantitative assessment of the resistance of the algorithms is given according to the following criteria: cryptographic resistance, cryptographic strength margin, key expansion speed, protection against attacks at runtime, realization of an avalanche effect, the ability to quickly expand the key, and the possibility of parallel computing. The advantages and disadvantages of each encryption algorithm are revealed. The most resistant to cracking symmetric block encryption algorithm is selected from those considered.

Key words: symmetric cryptosystem, cryptographic resistance, cryptanalytic attack.

Введение. Задача обеспечения требуемой криптографической стойкости алгоритмов шифрования приобретает все большую актуальность в связи с развитием информационных технологий. Как известно, при помощи шифрования должны обеспечиваться следующие состояния безопасности: конфиденциальность, целостность и идентифицируемость передаваемой информации. Одним из наиболее продуктивных средств решения поставленной задачи является применение эффективных методов шифрования.

Для выбора соответствующего криптоалгоритма необходимо владеть математическим аппаратом, положенным в основу алгоритма, а также проанализировать возможность того или иного метода шифрования противостоять современным криптоаналитическим атакам. Далее важно выбрать критерии для оценки и анализа криптостойкости алгоритмов шифрования. Например, запас криптостойкости, скорость расширения ключа, защита от атак по времени выполнения, возможность быстрого расширения ключа и др.

В статье дана количественная оценка стойкости симметричных алгоритмов шифрования, а также выявлены их преимущества и недостатки. Данные криптосистемы были выбраны по причине того, что в настоящее время их ма-

тематический аппарат анализа и оценки стойкости лучше исследован по сравнению с асимметричными алгоритмами шифрования.

Основная часть. Как известно, симметричное шифрование – способ преобразования, в котором для зашифрования и расшифрования секретной информации используется один и тот же ключ [1]. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Криптостойкость – важнейшая характеристика для алгоритмов шифрования, которая обычно измеряется временем, необходимым для вскрытия того или иного метода шифрования при неких фиксированных ресурсах, имеющихся у злоумышленника. Нарушитель ставит перед собой следующие цели: нахождение открытого текста (при этом у него имеется криптограмма, но нет секретного ключа) или самого тайного ключа.

Симметричные криптосистемы обладают следующими достоинствами по сравнению с асимметричными криптосистемами:

1) скорость;

2) простота реализации (благодаря более простым операциям);

3) меньшая требуемая длина ключа для сопоставимой стойкости;

4) изученность (за счет большего возраста).

Необходимо также отметить и недостатки данных криптосистем:

– сложность управления ключами в большой сети. Означает квадратичное возрастание числа пар ключей, которые надо генерировать, передавать, хранить и уничтожать в сети;

– сложность обмена ключами. Для применения следует решить проблему надежной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам.

Существует следующая классификация атак на симметричные алгоритмы шифрования [2]:

1) атака с известным открытым текстом. Предполагает у криптоаналитика некоторого количества пар текстов, каждая из которых представляет собой открытый текст и соответствующий ему шифртекст;

2) атака с выбранным открытым текстом. У криптоаналитика есть возможность выбора открытых текстов для получения соответствующих им шифртекстов;

3) адаптивная атака с выбором открытого текста. Криптоаналитик может не просто выбирать открытые тексты для зашифрования, но и делать это многократно с учетом результатов анализа ранее полученных данных;

4) атака с выбором шифртекста. Криптоаналитик может выбирать шифртексты и получать соответствующие им открытые тексты;

5) адаптивная атака с выбором шифртекста. Криптоаналитик может многократно выбирать шифртексты для их расшифрования с учетом предыдущих результатов.

Далее рассмотрим криптоаналитические методы, которые используются в атаках [3].

Метод «грубой силы» предполагает перебор всех возможных комбинаций ключа шифрования для нахождения искомого ключа. Защита от атак этого метода проста: увеличение размера ключа на 1 бит увеличит возможное количество ключей. Современная техника не позволяет в «лоб» атаковать 128-битный ключ полным перебором, однако данный метод можно использовать в контексте других методов криптоанализа.

Метод встречи посередине. Любые методы, способные вскрыть алгоритм шифрования быстрее, чем полный перебор всех возможных вариантов ключа шифрования, как правило, оперируют недостатками реализации того или иного метода шифрования. Примером данной атаки является вскрытие любого алгоритма шифрования, представляющего собой двойное шифрование данных с помощью какого-либо одного алгоритма. Во многих литературных источниках данный метод показан для взлома алгоритма Double DES, который в настоящее время не используется.

Дифференциальный криптоанализ. Данный метод основывается на анализе пар открытых текстов, между которыми существует определенная разность. При помощи этого метода вскрывается одноraундовый DES, а также сокращается количество комбинаций подбора секретного ключа для трехраундового DES с определенной вероятностью.

Линейный криптоанализ. Суть данного метода состоит в нахождении соотношений между открытым текстом, шифртекстом и ключом соответственно. Как и в дифференциальном криптоанализе, криптоаналитик находит некое одноraундовое соотношение и пытается распространить его на большее количество раундов. Во многих литературных источниках данный метод показан также на примере выявления закономерностей в работе алгоритма DES для поиска определенного количества начальных бит ключа, что по итогу заметно сокращает перебор оставшихся возможных комбинаций секретного ключа. Стоит отметить, что данный метод криптоанализа также продуктивен против алгоритмов RC5, NUSH и Noekeon.

Метод бумеранга является усилением дифференциального криптоанализа и состоит в использовании квартета (четырех вместо двух открытых текстов). Он представляет собой атаку с адаптивным выбором открытых текстов и

шифртекстов, которая на практике сложно применима. Данный метод был использован против CAST-256, MARS и SERPENT. Последние два алгоритма вскрываются только в вариантах с уменьшенным количеством раундов.

Сдвиговая атака. Уникальность атаки состоит в том, что ее успешность не зависит от количества раундов атакуемого алгоритма. Однако с помощью данной атаки можно вскрыть только те алгоритмы, раунды которых являются идентичными. Благодаря данной сдвиговой атаке был полностью раскрыт алгоритм шифрования TREYFER. Эта атака также применима к модифицированным симметричным алгоритмам DES и Blowfish, но не распространима на их полные версии. Стоит отметить, что несколько позже сдвиговая атака была усилена и применена на алгоритмы, в которых функции раундов не совсем идентичны, но имеют существенные сходства. Усиленная атака была использована для взлома нескольких вариантов алгоритма DES, а также 20-раундового стандарта шифрования ГОСТ.

Метод интерполяции применим к таким алгоритмам шифрования, которые используют достаточно простые алгебраические операции, в результате чего криптоаналитик может построить некий полином, который определяет взаимосвязь между шифртекстом и открытым текстом.

Невозможные дифференциалы. Основное отличие данного метода по сравнению с классическим дифференциальным анализом заключается в том, что тут используются дифференциалы с нулевой или минимальной вероятностью для того, чтобы сократить подмножество возможных ключей для выполнения дальнейшего перебора и нахождения секретного ключа. Этот метод нашел свое применение для вскрытия усеченных версий симметричных блочных алгоритмов шифрования, таких как IDEA.

Отметим, что это самые известные криптоаналитические атаки, которые предназначены для вскрытия или частичного взлома большинства симметричных криптосистем.

В данной статье рассмотрим следующие симметричные блочные алгоритмы шифрования, которые были участниками конкурса AES для выбора стандарта шифрования в США. Определим следующие критерии для отбора:

– 128-битный размер блока шифруемых данных;

– не менее трех поддерживаемых алгоритмом размеров ключей шифрования: 128, 192 и 256 бит;

– алгоритм должен быть стойким против современных криптоаналитических атак;

– структура и математическая модель алгоритма должны быть ясными и простыми, что облегчало изучение криптографической системы;

– должны отсутствовать слабые и эквивалентные ключи;

– скорость шифрования должна быть высокой;

– алгоритм должен предъявлять минимальные требования к оперативной памяти.

Многие симметричные системы шифрования были исключены из анализа по причине сложной математической модели и операций, которые были положены в основу структуры алгоритма, невозможности противостояния криптоаналитическим атакам, медленной скорости шифрования данных, а также невозможности реализации на разных платформах.

Для анализа криптостойкости были выбраны следующие симметричные блочные криптосистемы: AES, RC6, SERPENT и Twofish. Было обращено особое внимание на следующие компоненты каждого из алгоритмов: сложность структуры метода шифрования, способность быстрого расширения секретного ключа до 128, 192 и 256 бит.

В табл. 1 приведен результат сравнительного анализа эффективности данных криптосистем по выбранным критериям.

Таблица 1

Сравнительный анализ эффективности симметричных блочных криптосистем

Критерий	AES	RC6	SERPENT	Twofish
Криптостойкость	1	1	1	1
Запас криптостойкости	1	1	1	1
Скорость расширения ключа	1	0,5	0,5	0
Защита от атак по времени выполнения	1	0	1	0,5
Реализация лавинного эффекта	1	1	1	1
Возможность быстрого расширения ключа	0,5	0,5	1	1
Возможность параллельных вычислений	1	0,5	0,5	0,5
Результат	6,5	4,5	6	5

Анализ данных криптосистем производился по следующему принципу: если критерий не реализуем в определенном алгоритме, то выдвигается количественная единица для его оценки, равная 0; если критерий частично реализован в криптосистеме, то количественная единица принимает значение 0,5; следовательно, если критерий реализуем в методе шифрования без каких-либо ограничений, то коэффициент принимает значение 1.

Криптостойкость рассматриваемых симметричных шифров является достаточной. На ос-

новании многих литературных источников было выявлено, что для данных методов шифрования сложно реализуемы криптоаналитические атаки на полноценные или усеченные версии алгоритмов.

Под запасом стойкости понимается соотношение полного количества раундов и максимального из тех вариантов, против которого действуют какие-либо криптоаналитические атаки. Например, при помощи дифференциально-линейного криптоанализа вскрывается 11-раундовый SERPENT, тогда как в оригинальном алгоритме используется 32 раунда.

Защита от атак по времени выполнения заключалась в том, что скорость шифрования или расширения ключа не должна выходить за определенные установленные границы времени, в противном случае данный алгоритм будет подвержен данным атакам.

Лавинный эффект в указанных симметричных криптосистемах реализован в полной мере, поэтому все алгоритмы шифрования получили 1 количественную единицу за этот критерий.

На основании различных источников было установлено, что все данные симметричные криптосистемы поддерживают возможность быстрого расширения ключа, однако только SERPENT и Twofish реализуют такую возможность без каких-либо ограничений [4, 5]. Выявлено, что только алгоритм AES позволяет производить параллельные вычисления без ограничений, под которыми понимается одновременное выполнение операций внутри раунда и расширение ключа.

В ходе анализа было установлено, что алгоритм AES является наиболее стойким к взлому из рассмотренных с результатом 6,5 количественной единицы.

Проанализируем достоинства и недостатки данных алгоритмов шифрования, которые в итоге уступили алгоритму AES.

Алгоритм Twofish. Из преимуществ алгоритма можно выделить следующие:

1) процессы шифрования и дешифрования в алгоритме практически идентичны;

2) лучший из алгоритмов с точки зрения быстрого расширения ключа.

Отметим недостатки рассматриваемой криптосистемы:

– сложность структуры алгоритма затрудняет его анализ;

– сложная процедура расширения ключа;

– распараллеливание вычислений реализуемо с ограничениями.

Алгоритм SERPENT. Из достоинств алгоритма шифрования можно выделить следующие:

1) простая структура алгоритма, что значительно облегчает его анализ с целью нахождения возможных уязвимостей;

2) легко модифицируется для защиты от атак по времени выполнения, однако при этом снижается скорость.

Среди недостатков отметим следующие:

– самый медленный алгоритм в программных реализациях;

– процедуры шифрования и дешифрования различны, поэтому требуют различной реализации;

– распараллеливание вычислений реализуемо с ограничениями.

Алгоритм RC6. Из преимуществ данной симметричной криптографической системы можно выделить следующие:

1) простая структура алгоритма, что в итоге облегчает его анализ;

2) как и в алгоритме Twofish, процессы шифрования и дешифрования в алгоритме практически идентичны.

Отметим также недостатки рассматриваемого алгоритма:

– скорость шифрования зависит от того, поддерживает ли платформа 32-битное умножение и вращение на переменное число бит;

– достаточно сложно защищается от атак по времени выполнения;

– частично поддерживается быстрое расширение ключа;

– распараллеливание вычислений реализуемо с ограничениями.

Далее проанализируем симметричные криптосистемы AES и DES. Алгоритмы Twofish, SERPENT и RC6 не участвовали в данном сравнении по причине того, что эти криптосистемы имеют длину обрабатываемого блока и длину ключа такие же, как и у алгоритма AES. Стоит отметить, что рассмотренные в статье криптоалгоритмы отличаются между собой только типом архитектуры, количеством раундов и схемой генерации ключа.

В табл. 2 приведен сравнительный анализ алгоритма предшественника DES и нынешнего стандарта шифрования в США – AES.

Таблица 2

Сравнительный анализ алгоритмов AES и DES

Критерий	AES	DES
Длина блока, бит	128/192/256 в зависимости от длины ключа	64
Длина ключа, бит	128/192/256	56
Архитектура	SP – сеть «Квадрат»	Сеть Фейстеля
Число раундов	10/12/14 в зависимости от длины ключа	16
Схема генерации ключа	Умеренно сложная	Сложная

Анализ данных блочных симметричных алгоритмов шифрования показал, что нынешний

стандарт шифрования в США на основе алгоритма AES значительно превосходит своего предшественника и по длине обрабатываемого блока, и по длине ключа, что значительно повышает его криптостойкость. Отметим, что алгоритм DES не устойчив к различным криптоаналитическим атакам. Алгоритм Double DES взламывается за счет метода встречи посередине. Определенное количество раундов DES вскрывается на основе сдвиговой атаки, а также при помощи линейного и дифференциального криптоанализа [6].

В свою очередь, алгоритм AES устойчив к известным алгоритмам криптоанализа. Подчеркнем, что структура генерации ключа стала умеренно сложной по сравнению с алгоритмом DES.

Заключение. После проведения сравнительного анализа симметричных блочных алгоритмов шифрования по выбранным критериям было установлено, что AES является наиболее криптостойким алгоритмом с результатом в 6,5 количественной единицы. Единственный недостаток данного криптоалгоритма заключается в возможности расширения ключа лишь с некоторыми ограничениями.

Алгоритм Twofish был оценен в 5 количественных единиц из-за медленной скорости расширения ключа, а также частичной возможности быстрого расширения ключа и возможности параллельных вычислений.

Алгоритм RC6 получил 4,5 количественной единицы по причине невозможности защиты от атак по времени выполнения. Возможность быстрого расширения ключа и возможность параллельных вычислений реализуемы с ограничениями.

В свою очередь, алгоритм SERPENT был наиболее близок к показателям AES с результатом в 6 количественных единиц. Скорость расширения ключа относительно медленная, а возможность быстрого расширения ключа и возможность параллельных вычислений реализуемы в данной криптосистеме с ограничениями.

Литература

1. Урбанович П. П. Защита информации методами криптографии, стеганографии и обфускации. Минск: БГТУ, 2016. 220 с.

2. Брассар Ж. Современная криптология. М.: Полимед, 1999. 176 с.

3. Панасенко С. П. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. 576 с.

4. Аграновский А. В., Хади Р. А. Практическая криптография: Алгоритмы и их программирование. М.: СОЛОН-Р, 2002. 257 с.

5. Грушо А. А., Тимошина Е. Е., Применко Э. А. Анализ и синтез криптоалгоритмов. Курс лекций. Йошкар-Ола: Изд-во МФ МОУ, 2000. 110 с.

6. Бабенко Л. К., Ищукова Е. А. Современные алгоритмы блочного шифрования и методы их анализа. М.: Гелиос АРВ, 2006. 258 с.

References

1. Urbanovich P. P. *Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii* [The protection of information based on the methods by cryptography, steganography and obfuscation]. Minsk, BGTU Publ., 2016. 220 p.

2. Brassar Zh. *Sovremennaya kriptologiya* [Modern cryptology]. Moscow, Polimed Publ., 1999. 176 p.

3. Panasenko S. P. *Algoritmy shifrovaniya. Spetsial'nyy spravochnik* [Encryption Algorithms. Special reference]. St. Petersburg, BKhV-Peterburg Publ., 2009. 576 p.

4. Agranovsky A. V., Hadi R. A. *Prakticheskaya kriptografiya: Algoritmy i ikh programmirovaniye* [Practical cryptography: Algorithms and their programming]. Moscow, SOLON-R Publ., 2002. 257 p.

5. Grusho A. A., Timoshina E. E., Primenko E. A. *Analiz i sintez kriptoalgoritmov. Kurs lektsiy* [Analysis and synthesis of cryptographic algorithms. Lecture course]. Yoshkar-Ola, Izdatel'stvo MF MOU Publ., 2000. 110 p.

6. Babenko L. K., Ishchukova E. A. *Sovremennyye algoritmy blochnogo shifrovaniya i metody ikh analiza* [Modern block cipher algorithms and methods for their analysis]. Moscow, Gelios ARV Publ., 2006. 258 p.

Информация об авторе

Берников Владислав Олегович – аспирант, ассистент кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: vladbernikovronaldo@gmail.com

Information about the author

Bernikov Vladislav Olegovich – PhD student, assistant lecturer, the Department of Information Systems and Technology. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: vladbernikovronaldo@gmail.com

Поступила после доработки 14.11.2019