Московский Физико-технический Институт
(ГУ МФТИ)
Кафедра радиотехники
http://www.re.mipt.ru/infsec

Эссе по курсу "Защита информации"

Обзор криптографических алгоритмов претендентов AES

Выполнил студент гр 111 Лукин Дмитрий

Долгопрудный • 2005

Алгоритм DES (Data Encryption Standard), разработанный корпорацией IBM и являвшийся с 1977 федеральным стандартом шифрования данных США, использовался для шифрования не только правительством США, но и получил широкое распространение по всему миру среди частных пользователей. С ростом вычислительной мощности компьютеров стали возникать вопросы о криптостойкости DES'а перед вскрытием методом "грубой силы", но стандарт успешно проходил повторные сертификации, проводившиеся в 1983, 1988 и 1993. Хотя к середине 90х годов стало очевидным несоответствие общепринятого стандарта шифрования DES (Data Encryption Standard) современным требованиям. В первую очередь из-за недостаточной длины ключа всего в 56 бит. По данным Брюса Шнайера уже в 1993 году существовали устройства способные вскрыть DES за приемлемое время.

Процесс разработки нового федерального информационного стандарта (FIPS) для шифрования данных Advanced Encryption Standard (AES) был инициирован Национальным Институтом стандартов и технологий (NIST).

В начале января 1997 года NIST объявил о начале разработки AES, выпустив документ "Announcing development of a federal information processing standard for advanced encryption standard", содержащий первичные требования к алгоритму.[2]

1) Алгоритм шифрования AES должен быть открыто опубликован.
2) Алгоритм должен быть симметричным блочным шифром.
3) AES должен предусматривать возможность увеличения длины ключа.
4) AES должен быть легко реализуем и аппаратной и программно.
5) AES должен распространяться бесплатно или быть общедоступным в рамках патентов ANSI.

В сентябре 1997 года вышел уточняющий документ "Call for AES Candidate Algorithms", объявлявший о проведении конкурса на AES и содержащий официальные требования к кандидатам. В частности алгоритм должен поддерживать следующие комбинации длин блока и ключа 128-128, 128-192 и 128-256 битов. К 15 июню 1998 году был заявлен 21 криптографический алгоритм, но только 15 из которых удовлетворяли первоначальным требованиям. [3]

Страна происхождения	Алгоритм	Авторы
Australia	LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
Belgium	RIJNDAEL	Joan Daemen, Vincent Rijmen
Canada	CAST-256	Entrust Technologies, Inc
	DEAL	Richard Outerbridge, Lars Knudsen
Costa Rica	FROG	TecApro Internacional S.A.
France	DFC	Centre National pour la Recherche Scientifique
Germany	MAGENTA	Deutsche Telekom AG
Japan	E2	Nippon Telegraph and Telephone Corporation
Korea	CRYPTON	Future Systems, Inc
USA	HPC	Rich Schroeppel
	MARS	IBM
	RC6	RSA Laboratories
	SAFER+	Cylink Corporation
	TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
UK, Israel, Norway	SERPENT	Ross Anderson, Eli Biham, Lars Knudsen

В конце августа 1998 года в Калифорнии состоялась конференция, посвященная отбору кандидатов на AES, получившая название AES1. На конференции давались краткие описания алгоритмов шифрования, и были даны ответы на накопленные вопросы.

В качестве основных критериев оценки алгоритмов были [3]:

- Криптостойкость. Проводилось сравнение алгоритмов на степень независимости выходного блока от случайной перестановки битов входного блока, подверженность

известным криптоатакам. Каждый кандидат должен был представить оценочную криптостойкость алгоритма.
- Стоимость. Кандидат предоставлял информацию о лицензионных соглашениях и патентах на алгоритм. Также учитывалась производительность алгоритма (скорость шифрования), необходимый для шифрования размер памяти.
- Особенности алгоритма и его реализации. Гибкость, аппаратное и программное удобство реализации.

В апреле 1999 года в Риме состоялась конференция AES2, в рамках которой проводились сравнение производительности программных реализаций алгоритмов с оптимизациями под языки C и Java. Наибольшую скорость шифрования/дешифрования показал алгоритм Crypton (40 Мбайт/с), наименьшую Magenta и HPC (2Мбайт/с). Хотя при проведении тестов на разных платформах и с различными компиляторами, полученные результаты довольно сильно различались.

Все блочные алгоритмы можно разбить на две основные группы:

1) использующие сети Фейстеля
2) сети перестановок-подстановок (SP-сети) основанные на последовательных перестановках и подстановках, зависящих от ключа.

Среди алгоритмов-претендентов к первым относятся CAST-256, DEAL, DFC, E2, LOKI97, MAGENTA, MARS, RC6, TWOFISH, ко вторым CRYPTON, Rijndael, SAFER+ и SERPENT. Алгоритмы FROG и HPC не подпадали ни под одну из категорий, но входе обсуждения кандидатов не выявлено каких-либо выдающихся качеств данных алгоритмов.

В результате первичного обсуждения была выявлена слабая криптостойкость алгоритма MAGENTA, вскоре появились данные по криптоанализу алгоритмов FROG, LOKI, показывающие слабости алгоритмов относительно других алгоритмов. Также часть алгоритмов имели низкие шансы на успех из-за крайне малой скорости шифрования/дешифрования.

Отбор финалистов по названным критериям продолжался до начала августа 1999г.

9 августа NIST выпустила пресс-релиз **“**Announces AES Finalists”, в котором объявлялось о пяти финалистах: MARS, RC6, Rijndael, Serpent, TwoFish.

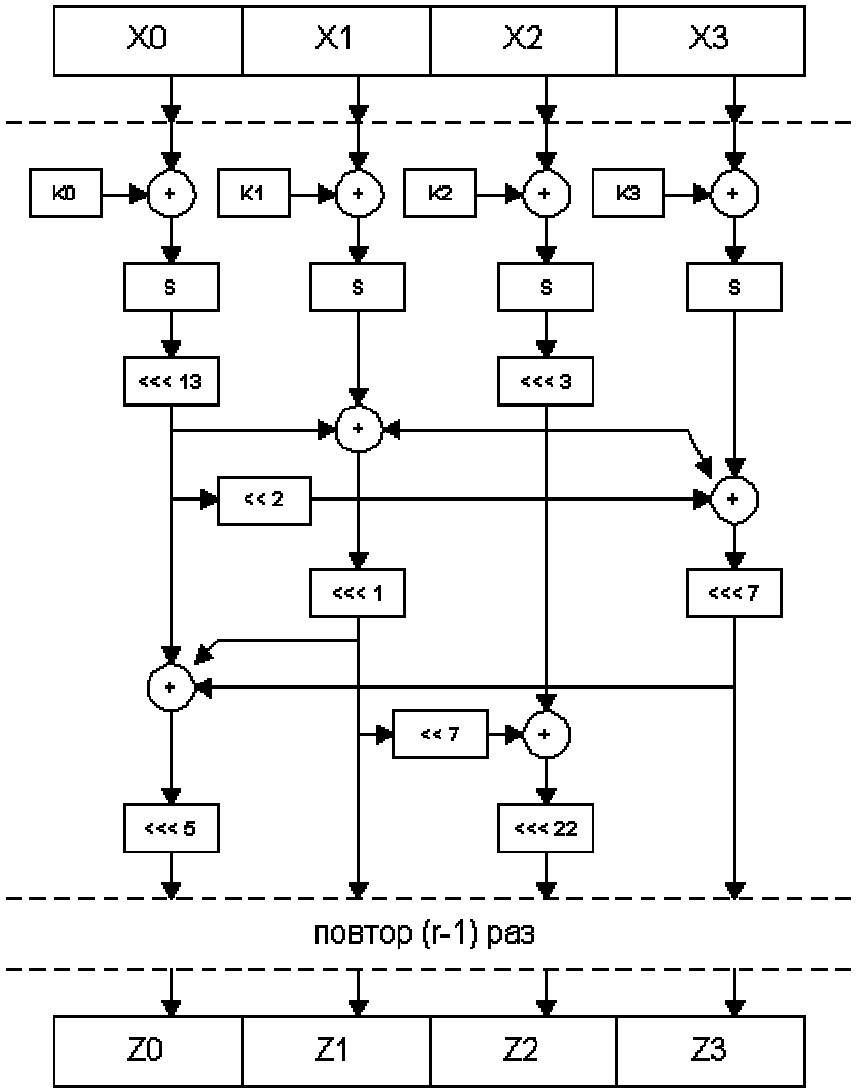
Serpent

Создателями алгоритма являются трое известных криптоаналитиков: Эли Бихам (один из создателей дифференциального криптоанализа), Росс Андерс, Ларс Кнудсен (также принимал участие в создании алгоритма DEAL). Профессионалам криптоанализа действительно удалось создать алгоритм криптостойкий ко всем известным атакам, и до сих пор слабых сторон данного алгоритма не обнаружено.

Алгоритм представляет собой 32 раундовую сеть перестановок-подстановок (SP-сеть). В алгоритме используются комбинации S-box’ов и линейных преобразований, похожие на преобразования в DES, что упрощает анализ криптостойкости алгоритма, а для увеличения стойкости алгоритма количество раундов удвоенно.

Над входным 128 битным блоком производится начальная перестановка IP, далее в каждом из 32 раундов производится XOR раундовых ключей с выходом предыдущего раунда, прохождение S-box’ов и линейных преобразований, затем производится конечная перестановка IP^{-1}. Начальная и конечная перестановка не влияют на криптостойкость алгоритма, они предназначены для увеличения быстродействия алгоритма.

Удвоение количества раундов уменьшило скорость шифрования, и для увеличения скорости Бихам применил оптимизированную версию алгоритма (так называемый “bitslicing” применявшийся раннее при шифровании DES). Метод основан на том, что для шифрования DES можно использовать 1 битный процессор, со специальной аппаратной реализацией алгоритма, позволяющей эмуллировать все логический элементы.



Поэтому, используя 32 битный процессор, можно параллельно шифровать 32 блока, что является гораздо более эффективным решением, чем шифрование одного блока 32 битным процессором, который большинство времени простаивает, выполняя операции всего лишь с несколькими битами. Серпент разработан таким образом, чтобы все операции при шифровании и дешифровании использовали 32 битный параллелизм.
На каждом раунде производятся следующие действия:

1) исключающее “ИЛИ” ключа и выхода предыдущего раунда.
2) результат поступают на вход S-box’ов.

Для шифрования Серпентом используют 8 Sbox’ов, S_0 используется в 0,8,16,24 раундах, S_1 в 1,9,17,25 и т.д. В течение одного раунда используется один Sbox, который представляетс собой 4 битовую перестановку. 128 битов, логически представимых 4 слова по 32 бита, поступают на вход 32 Sbox’ов, каждый из которых является копией раундового S-box’а.
Итак, каждый Sbox используется в течение четырех раундов, в каждом из которых он используется параллельно 32 раза.

3) линейные преобразования 32 битных слов.

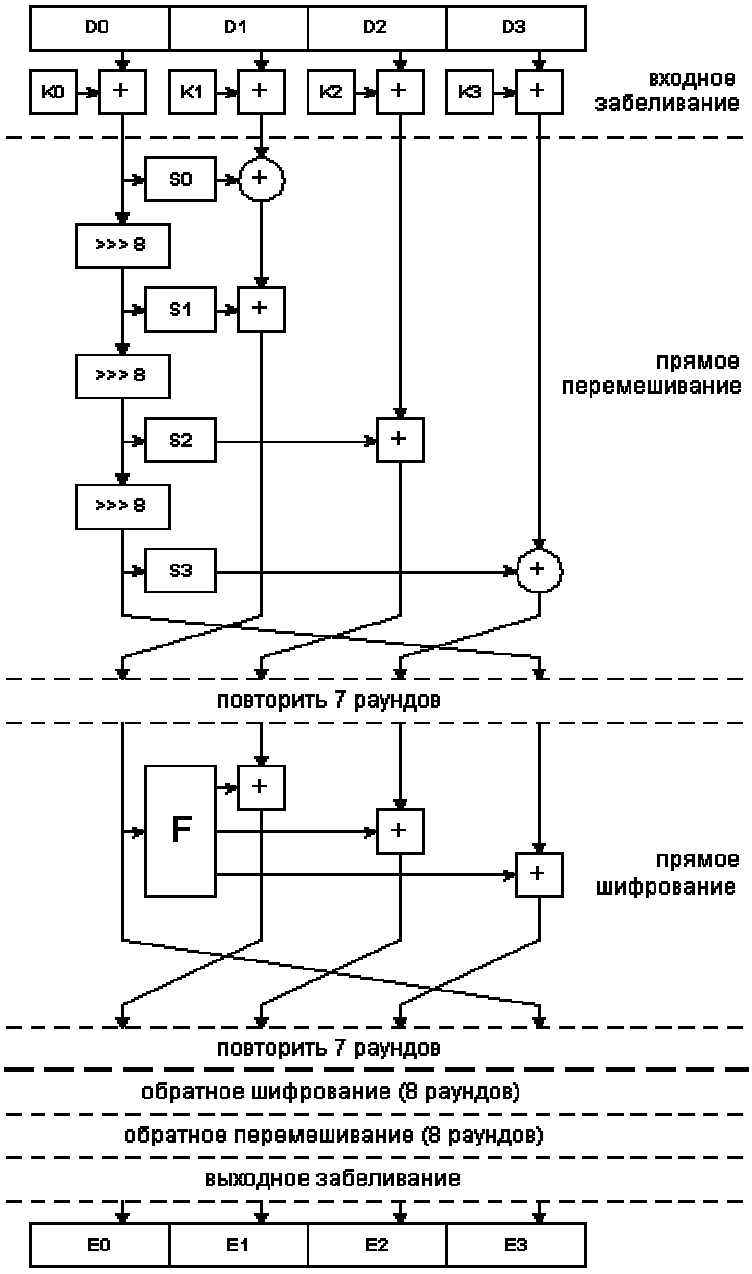
$X0;X1;X2;X3 := S_i(B_i + K_i)$
$X0 := X0 <<< 13$
$X2 := X2 <<< 3$
$X1 := X1 + X0 + X2$

X3 := X3 + X2 + (X0 << 3)
X1 := X1 <<< 1
X3 := X3 <<< 7
X0 := X0 + X1 +X3
X2 := X2 + X3 +(X1 << 7)
X0 := X0 <<< 5
X2 := X2 <<< 22
B_{i+1} := X0;X1;X2;X3

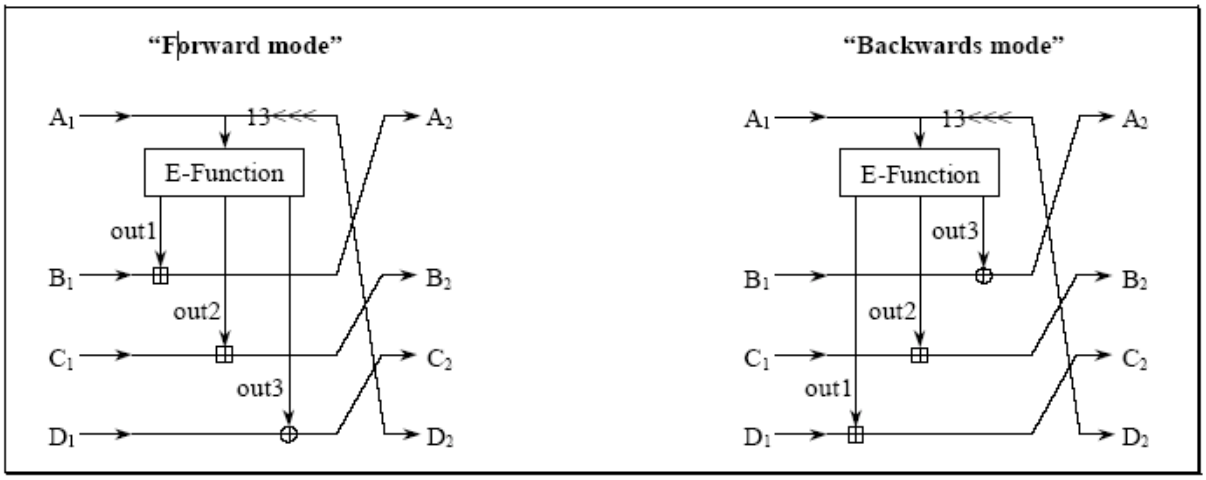
Согласно данным, представленным создателями протокола, 16 раундовый Серпент по криптостойкости аналогичен 3DES, а по быстодействию оптимизированный алгоритм в два раза быстрее DES. Хотя относительно других кандидатов скорость шифрования явно ниже. Согласно тестам, проводившимся на Intel-Pentium 200 МГц, алгоритмы Rijndael, RC6, E2, Mars показали скорость около 10 Мбайт/с, а Serpent только 14.7 Мбит/с.

MARS

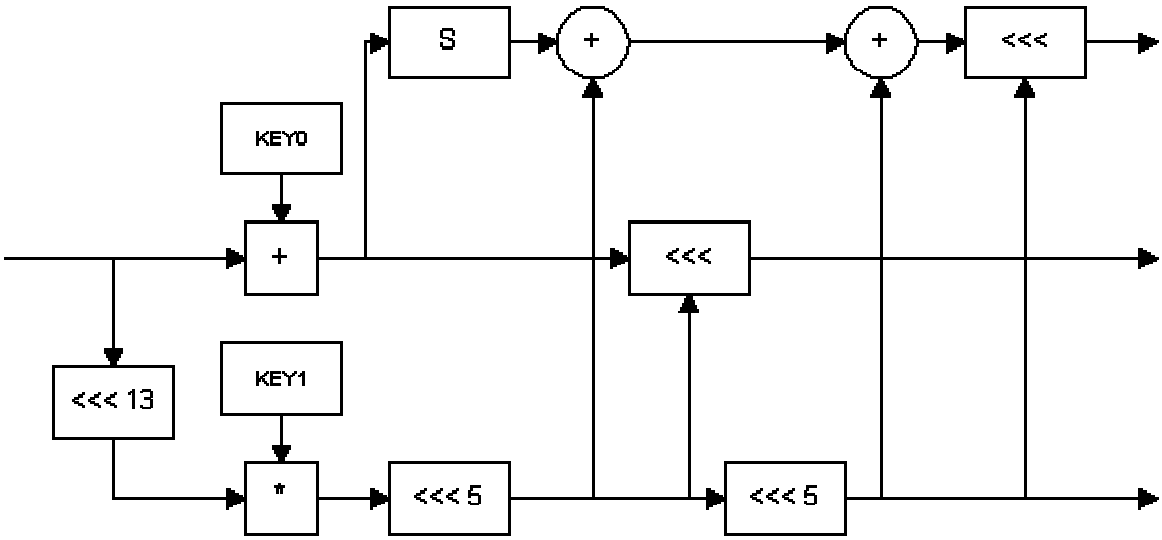
Коропорация IBM, создавшая DES, представила алгоритм MARS, обладающий как хорошей криптостойкостью так и высокой скоростью шифрования.



Процесс шифрования состоит из трех стадий: прямого и обратного перемешивания, которые оборачивают шифрование и состоят из 8 раундов, и 16 раундового шифрования. Обратное перемешивание производят для более быстрого достижение лавинного эффекта и нарушения симметричности при перемешивании. Стадии прямого и обратного перемешивания инвертированы относительно друг друга.
Перед прямым перемешиванием происходит входное забеливание (добавление к входному блоку ключей). Далее в течение 8 раундов производится перемешивание без использования ключа. На стадии перемешивания используются операции битового сдвига, исключающего “ИЛИ”, сложения и Sbox’ы.
Непосредственное шифрование представляет собой сеть Фейстеля с 4 ветвями. От первой ветви вычисляется функция F. На вход функции F подается 32 битное слово, функция выдает на выход три 32 битных слова. Полученные слова складываются с тремя оставшимися ветвями, далее выполняется перестановка ветвей. Структура функции представлена на рис.



В первых восьми раундах производится прямое шифрование, в следующих восьми раундах обратное. Прямое и обратное шифрование отличаются порядком функций, выполняемых над выходами функции F.

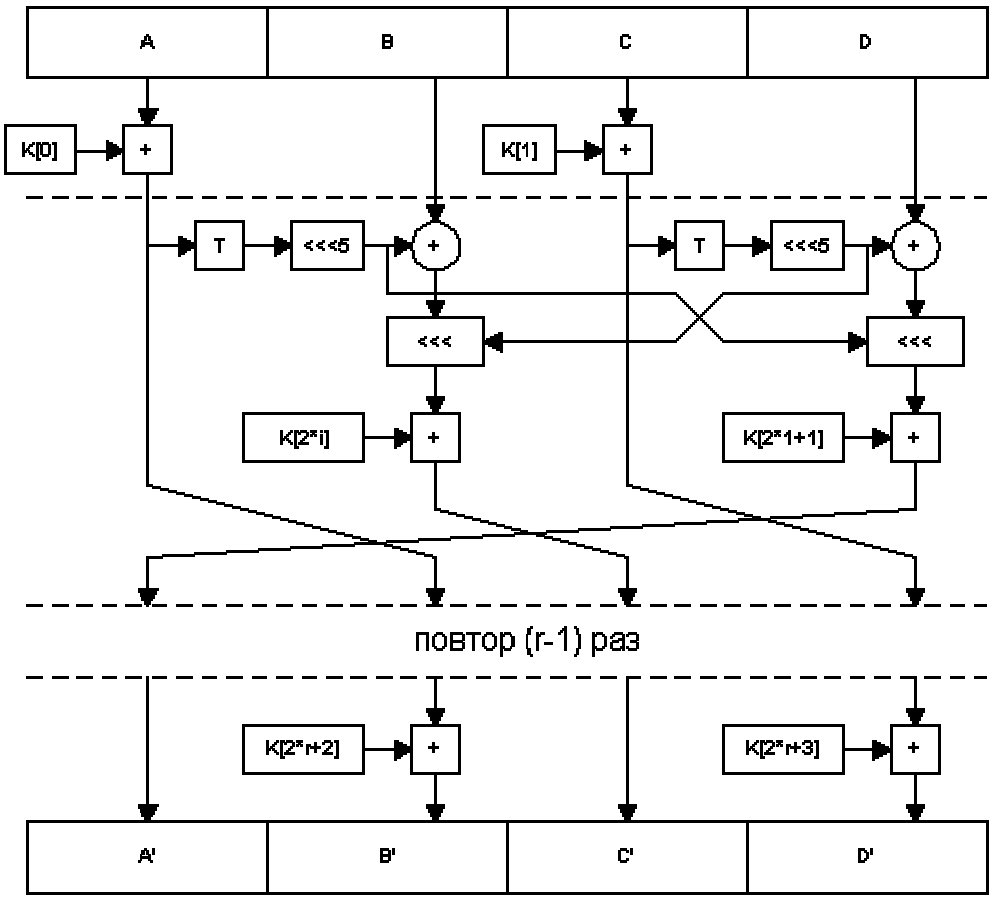


MARS поддерживает переменную длину ключа от 128 до 448 битов, используя процедуру расширения входного ключа до 40 32-битовых слов, которые используются при шифровании и дешифровании.

Одним из недостатков алгоритма является сложность его криптоанализа из-за использования двойного перемешивания. Алгоритм показал хорошую скорость шифрования. Скорость шифрования на Intel-Pentium 200 МГц достигала 65 Мбит/с, скорость выполнения блока прямого и обратного шифрования достигала 100 Мбит/с.

RC6

Алгоритм, разработанный RSA Laboratories, является видоизменным алгоритмом RC5 для соответствия требованиям AES. Алгоритм построен на сети Фейстеля с четырьмя ветвями и имеет 20 раундов. Входная последовательность разбивается на 4 32-битных слова. Нечетные блоки используются для изменения четных блоков, процессы изменения второго и четвертого блоков идут параллельно.



Характерной особенностью алгоритма является отказ от привычных Sbox'ов и введение операция квадратичной трансформации. Простота и высокая скорость шифрования являются его основными достоинствами, к тому же RC6 имеет наибольшую скорость среди финалистов (12.6 Мбайт/с)

TwoFish

Алгоритм, разработанный Шнайером, является модификацией алгоритма BlowFish, созданного в 1993г. Алгоритм TwoFish основан на 16 раундовой сети Фейстеля. В алгоритме используются преобразование PHT (Pseudo-Hadamard Transforms), MDS матрицы, зависимые от ключа Sbox'ы, по сравнению с другими алгоритмами TwoFish имеет довольно сложную структуру.

В середине апреля 2000 года в Нью-Йорке состоялась конфренция AES3, в которой приняли участие более 250 криптографов. На конференции подводились итоги по криптоанализу финалистов. Одним из интересных полученных результатов является максимальное количество раундов, при котором наилучшая из известных криптографических атак на данный алгоритм более эффективна, чем взлом методом грубой силы 256 битного ключа. [7]

Алгоритм	MARS	RC6	Rijndael	Serpent	TwoFish
Количество раундов	9 из 16	15 из 20	8 из 14	9 из 32	6 из 16

2 октября 2000 NIST объявил, что алгоритм Rijndael выбран в качестве Advanced Encryption Standard. По замечанию авторов алгоритма, главная проблема с данным шифром - это как читать его название, составленное из фамилий криптографов. В соответствии с фламандскими традициями, "ij" читается как "э", а "ae" - как открытое "a". Так что "Rijndael" - это просто "Рэндал"... [9]

Литература:

1. Advanced Encryption Standard
   a) AES - The Early Years (1997-98)
      http://csrc.nist.gov/CryptoToolkit/aes/pre-round1/earlyaes.htm
   b) AES Round 1 Information
      http://csrc.nist.gov/CryptoToolkit/aes/round1/round1.htm
   c) AES Round 2 Information
      http://csrc.nist.gov/CryptoToolkit/aes/round2/round2.htm
2. Announcing development of a federal information processing standard for advanced encryption standard
   http://csrc.nist.gov/CryptoToolkit/aes/pre-round1/aes_9709.htm
3. CONFERENCE REPORT. FIRST ADVANCED ENCRYPTION STANDARD (AES) CANDIDATE CONFERENCE Ventura, CA August 20-22, 1998
   http://csrc.nist.gov/CryptoToolkit/aes/round1/conf1/j41ce-rob.pdf
4. Serpent: A Proposal for the Advanced Encryption Standard. R.Anderson, E. Biham, L.Knudsen
   http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/serpent.pdf
5. The MARS Encryption Algorithm C. Burwick, D. Coppersmith, E. D'Avignon
   http://www.research.ibm.com/security/mars-short.ps
6. The RC6 Block Cipher. Ronald L. Rivest, M.J.B. Robshaw, R. Sidney
   http://theory.lcs.mit.edu/~rivest/rc6.pdf
7. A Performance Comparison of the Five AES Finalists. B.Schneier, D. Whiting.
   http://csrc.nist.gov/CryptoToolkit/aes/round2/conf3/papers/17-bschneier.pdf
8. О процессе принятия AES. Б. Киви
   http://byrd.narod.ru/aes/aes2.htm
9. Конкурс на новый криптостандарт AES. Б. Киви
   http://kiwibyrd.chat.ru/ru/aes1.htm
10. Общие сведения о конкурсе AES
    http://www.citforum.ru/internet/infsecure/its2000_21.shtml