Московский Физико-Технический Институт
Факультет Радиотехники и Кибернетики

Обзор кандидатов на стандарт AES

Липатьев Р.С., студент 013 гр.

Общие сведения о конкурсе AES

В 80-х годах в США был принят стандарт симметричного криптоалгоритма для внутреннего применения DES (Data Encryption Standard), который получил достаточно широкое распространение в свое время. Однако на текущий момент этот стандарт полностью неприемлем для использования по двум причинам : 1) основной – длина его ключа составляет 56 бит, что чрезвычайно мало на современном этапе развития ЭВМ, 2) второстепенной – при разработке алгоритм был ориентирован на аппаратную реализацию, то есть содержал операции, выполняемые на микропроцессорах за неприемлемо большое время (например, такие как перестановка бит внутри машинного слова по определенной схеме).

Все это сподвигло Американский институт стандартизации NIST - National Institute of Standards & Technology на объявление в 1997 году конкурса на новый стандарт симметричного криптоалгоритма. На сей раз уже были учтены основные промахи шифра-предшественника, а к разработке были подключены самые крупные центры по криптологии со всего мира. Тем самым, победитель этого соревнования, названного AES – Advanced Encryption Standard, становится де-факто мировым криптостандартом на ближайшие 10-20 лет.

Требования, предъявленные к кандидатам на AES, были предельно просты :

- алгоритм должен быть симметричным,
- алгоритм должен быть блочным шифром,
- алгоритм должен иметь длину блока 128 бит, и поддерживать три длины ключа: 128, 192 и 256 бит.

Дополнительно кандидатам рекомендовалось:

- использовать операции, легко реализуемые как аппаратно (в микрочипах), так и программно (на персональных компьютерах и серверах),
- ориентироваться на 32-разрядные процессоры,
- не усложнять без необходимости структуру шифра для того, чтобы все заинтересованные стороны были в состоянии самостоятельно провести независимый криптоанализ алгоритма и убедиться, что в нем не заложено каких-либо недокументированных возможностей.

В августе 1998 г. были объявлены 15 принятых на конкурс алгоритмов, разработанных криптографами из 12 стран. В течение 2 лет специалисты комитета, исследуя самостоятельно, и изучая публикации других исследователей, выбрали 5 финалистов первого этапа конкурса. Ими стали MARS, RC6, Rijndael, Serpent и Twofish. Все эти алгоритмы были признаны достаточно стойкими и успешно противостоящими всем широко известным методам криптоанализа. Проведя дальнейший анализ каждого из алгоритмов-финалистов, 2 октября 2000 года NIST объявил о своем выборе – победителем конкурса стал бельгийский алгоритм RIJNDAEL. С этого момента с алгоритма-победителя сняты все патентные ограничения – его можно будет использовать в любой криптопрограмме без отчисления каких-либо средств создателю.

Обзор шифров-кандидатов на AES

CAST-256 (Канада)

Криптоалгоритм от канадской фирмы Entrust Technologies. Карлайл Эдамс, разработавший концепцию семейства шифров CAST вместе со Стэффордом Таваресом в начале 1990-х годов, говорит о новом шифре следующее: "Алгоритм CAST-256 в своей конструкции всецело опирается на идеи, которые уже очень хорошо проанализированы и проверены. Многие другие предложенные

шифры являются довольно новыми, в том смысле, что новыми являются конструктивные аспекты этих шифров, в нашем же случае мы попытались опереться на вещи, уже доказанные".

Предыдущий шифр этого семейства - CAST-128 - является неофициальным канадским стандартом шифрования, и респектабельная теоретическая база данной архитектуры в сочетании с успешным противостоянием криптоанализу могли бы дать алгоритму CAST-256 весьма реальные шансы на победу в конкурсе. Однако, среди явных минусов шифра называют такие немаловажные факторы, как более медленную по сравнению с другими кандидатами производительность (следствие "консервативного дизайна"), а также необходимость хранения достаточно больших табличных массивов (4 килобайта), что затрудняет реализацию алгоритма в некоторых приложениях.

CRYPTON (Южная Корея)

Шифр Crypton представлен южнокорейской компанией Future Systems, с конца 1980-х годов работающей на рынке сетевого обеспечения и защиты информации. Автор алгоритма Че Хун Лим признает, что конструкция его шифра во многом опирается на идеи шифра SQUARE бельгийских криптографов Дамена и Рэмена (также участвующих в конкурсе). Здесь нет традиционной для многих блочных шифров "структуры Фейстела", оперирующей в каждом цикле шифрования половиной блока данных (например, как в DES или CAST). Основу данного шифра составляет другая стандартная конструкция - так называемая SP-сеть, т.е. повторяющаяся цикловая функция из замен-перестановок, ориентированная на распараллеленную нелинейную обработку всего блока данных. Помимо высокой скорости, к преимуществам такой конструкции относят и то, что она облегчает исследование стойкости шифра к методам дифференциального и линейного криптоанализа, являющимся на сегодня основными инструментами вскрытия блочных шифров.

Шифр Crypton, как и Square, эффективно реализуется на разнообразных платформах, и признано, что в корейском алгоритме присутствуют талантливые конструктивные идеи.

DEAL (Норвегия, Канада)

Самый первый из предложенных кандидатов на AES, появившийся летом 1997 года, шифр разработан датчанином Ларсом Кнудсеном, одним из наиболее блестящих криптоаналитиков в области блочного шифрования, и его канадским коллегой Ричардом Аутебриджем. Собственно говоря, DEAL нельзя называть самостоятельной разработкой, поскольку, по сути дела, это остроумная схема использования старого знакомого DES в новой, более стойкой конфигурации. Проще говоря, это DES с увеличенными длинами блока данных и ключа, соответствующими требованиям AES. Главный недостаток такого подхода - сохраняются неудобства реализации, присущие DES, а это серьезно сказывается на производительности шифра. Учитывая, что у пользователей уже имеется и достаточно широко применяется надежный (и медленный) тройной-DES, можно было уверенно констатировать минимальные шансы DEAL на победу.

DFC или Decorrelated Fast Cipher (Франция)

Французский алгоритм DFC или "декоррелированный быстрый шифр" - совместная разработка криптографов парижской Высшей нормальной школы и Национального центра научных исследований (CNRS). Шифр создан большим коллективом из 8 человек и базируется на фундаменте недавно созданной технологии конструирования блочных шифров с доказуемой стойкостью к известным криптоаналитическим атакам. Однако нельзя не отметить, что уже появились аналитические результаты, несколько скомпрометировавшие эту достаточно красивую теорию.

Конструктивно архитектура шифра DFC представляет собой традиционную сеть Фейстела с цикловой функцией, построенной специфическим образом, обеспечивающим высокую стойкость при удивительно малом количестве циклов шифрования. Алгоритм характеризуется хорошей, но не слишком высокой производительностью. Авторами декларируется эффективная реализация на разнообразных платформах, хотя сторонние наблюдатели отмечают, что 64-битные перемножения - это все же довольно дорогая операция для большинства вычислительных платформ.

E2 (Япония)

Шифр представлен на конкурс японской национальной телекоммуникационной компанией NTT. Название "E2" обозначает "Efficient Encryption" или "эффективное шифрование", а в остальном - это как бы японский близнец французского шифра DFC. Различие шифров заключается лишь в использовании разных методик конструирования доказуемо стойких шифров.

Представленная разработчиками обстоятельная аналитическая документация получила самые высокие отзывы специалистов, свидетельствующие, что в NTT создали весьма серьезный сильный шифр.

FROG (Коста-Рика)

Шифр FROG выставила на конкурс международная компания TecApro Internacional, зарегистрированная в Коста-Рике. Авторы криптоалгоритма - Д. Георгудис, Д. Леру и Б. Шаве – малоизвестные люди в криптографическом мире. Согласно характеристике разработчиков, FROG - это "новый шифр с неортодоксальной структурой".

Уже через месяц после публикации алгоритма появились криптоаналитические результаты, свидетельствующие, что FROG - явно недостаточно сильный шифр для AES. Было показано, что ключ шифра Frog можно вскрывать при трудозатратах около 2^{57}. Для DES, к примеру, с его 56-битным ключом это было бы прекрасным показателем стойкости (поскольку на лобовое вскрытие ключа тотальным перебором требуется 2^{56} опробований), однако, для шифра с длиной ключа по меньшей мере 128 бит этого уже слишком мало.

HPC или Hasty Pudding Cipher (США)

Шифр с игривым названием "заварной пудинг" - самая "темная лошадка" в начавшихся состязаниях. Его разработчик - авторитетный американский математик Рич Шреппель - специализируется, главным образом, в области теории чисел и криптографии с открытым ключом, так что его выход с собственным симметричным шифром оказался достаточно неожиданным. По признанию самого разработчика, криптоалгоритм создавался по сути дела экспромтом и чрезвычайно перегружен всевозможными "хитрыми" числовыми преобразованиями. В связи с этим шансы на победу у HPC были минимальны.

LOKI97 (Австралия)

Новый представитель достаточно широко известного ряда шифров LOKI, разрабатываемых в стенах Академии министерства обороны Австралии с 1989 года. Авторы криптоалгоритма: Лори Браун (по сути дела, шифр LOKI - это основа его докторской диссертации), Йозеф Пьепшик (польский криптограф, перебравшийся в Австралию в конце 80-х годов) и Дженифер Себери.

Шифр LOKI97 основан на традиционной сети Фейстела, предыдущий представитель этого семейства - LOKI91 - был признан достаточно стойким шифром для своего класса, хотя и с некоторыми оговорками. Практически сразу же после публикации LOKI97 криптоаналитиками, уже хорошо знакомыми с данной конструкцией, были выявлены две существенные слабости в цикловой функции шифра, что, естественно, отдалило данный алгоритм от группы лидеров.

MAGENTA (Германия)

Шифр, представленный немецкой телекоммуникационной компанией Deutsche Telekom AG. Авторы алгоритма - Клаус Хубер и Михаэль Якобсон. MAGENTA - это аббревиатура от развернутого названия шифра, звучащего как "Многофункциональный алгоритм для шифрования общего назначения и сетевых телекоммуникаций". В настоящее время этот шифр используется внутри Deutsche Telekom для защиты важных данных компании. Криптоалгоритм изначально разрабатывался для работы на высоких скоростях (порядка гигабит в секунду). В основе его конструкции лежит традиционная сеть Фейстела, а в качестве цикловой нелинейной функции выбрано быстрое адамарово преобразование. На конференции AES1 в ходе сессии вопросов-ответов криптосхема MAGENTA была, по сути дела, завалена искушенными в криптоанализе слушателями.

MARS (США)

Шифр MARS выставлен на конкурс корпорацией IBM. Эта компания с 60-х годов занимается самостоятельными криптографическими исследованиями, и нелишне напомнить, что алгоритм DES родился именно в стенах IBM, а Хорст Фейстел - автор "сети Фейстела" - был первым руководителем криптографического подразделения корпорации.

Среди большого коллектива соавторов нового шифра MARS можно найти имя Дона Копперсмита, участника разработки DES и человека с репутацией "одного из самых проницательных криптоаналитиков". По заявлению IBM, в алгоритм MARS вложен 25-летний криптоаналитический опыт фирмы, и наряду с высокой криптографической стойкостью шифр допускает эффективную реализацию даже в таких ограниченных рамках, какие характерны для смарт-карт. Понятно, что MARS считался одним из реальных кандидатов на победу.

RC6 (США)

Как говорится в рекламных анонсах к RC6 - новейшему алгоритму Рональда Райвиста - это "быстрый, гибкий и необычно компактный алгоритм - сочетание мощи и элегантности простоты". Райвист - это "R" в знаменитом алгоритме RSA, он один из сооснователей криптофирмы RSA Data Security и изобретатель широко используемых шифров RC2 и RC4, а также хеш-функций MD2, MD4 и MD5. Своими соавторами при создании нового криптоалгоритма Райвист называет Мэтта Робшоу, Рэя Сидни и Лайсу Йин - криптографов исследовательского центра RSA Laboratories.

RC6, возможно, самый быстрый шифр из всех кандидатов на AES в условиях платформ Pentium Pro/II, но он не очень хорошо ложится на 8-битные процессоры смарт-карт. По всеобщему признанию, шифр RC6 - это прямое эволюционное развитие предыдущего криптоалгоритм Райвиста под названием RC5, появившегося в 1995 году. Как сообщил автор, внесенные в конструкцию новшества прежде всего обусловлены результатами криптоанализа RC5 в кругах криптографической общественности. По признанию специалистов, RC6 - превосходный кандидат.

RIJNDAEL (Бельгия)

Шифр разработали известные бельгийские криптографы Йон Дамен и Винсент Рэмен из Лувенского католического университета, являющегося одним из признанных центров академической криптографии не только Бельгии, но и всей Европы. Конструкция нового шифра в значительной степени опирается на сильные идеи, воплощенные и проверенные в архитектуре шифра SQUARE, предыдущего детища этих же авторов, представленного в начале 1997 года.

Шифр реализует совершенно нетрадиционную криптографическую парадигму, полностью отказавшись от сети Фейстела. К достоинствам алгоритма относят: очень хорошее быстродействие на всех платформах от 8-битных до 64-битных, самый высокий потенциальный параллелизм среди претендентов, минимальные требования к ресурсам оперативной и постоянной памяти в реализации без кеширования некоторых операций, устойчивость к подавляющему большинству атак по времени исполнения и потребляемой мощности, структура шифра позволяет использовать любые комбинации размеров блока и длин ключа, кратные 32 бит (при достижении размером блока определенных границ требуется только увеличение числа раундов). При этом процедуры шифрования/дешифрования и операции расширения ключей различаются между собой достаточно сильно по сравнению с простым изменением порядка ключей либо операцией наложения, характерных для сети Фейстела, что увеличивает суммарный объем кода алгоритма.

Как показали предварительные исследования, Rijndael может быть очень эффективно реализован на самых разных процессорах и чрезвычайно успешно противостоит известным криптоаналитическим атакам.

SAFER+ (США)

Новая реинкарнация достаточно широко известного сильного шифра SAFER, впервые представленного в 1993 году патриархом академической криптографии Джеймсом Мэсси из швейцарского политехникума ETH (Цюрих). Шифр SAFER был разработан им по заказу американской криптофирмы Cylink, одним из основателей которой в начале 80-х годов был и сам Дж. Мэсси. Поэтому неудивительно, что новый шифр SAFER+ выдвинут на конкурс AES

корпорацией Cylink, а главный криптограф Cylink Лили Чен названа корпорацией как соавтор криптоалгоритма.

Чтобы дать представление об авторитете Мэсси как криптографа, достаточно упомянуть, что он является одним из двух авторов очень сильного блочного шифра IDEA - криптографической основы знаменитой программы PGP (Pretty Good Privacy). Говоря же о минусах новой схемы, следует отметить, что шифр SAFER+ разрабатывался под 8-битные микропроцессоры и довольно медленно работает на 32-битных машинах.

SERPENT (Великобритания, Израиль, Норвегия)

Главная изюминка шифра SERPENT в том, что все три его автора - это "асы криптоанализа", наиболее известные вскрытием шифров других криптографов. Израильский исследователь Эли Бихам - один из создателей дифференциального криптоанализа - техники, лежащей в основе большинства современных методов вскрытия блочных шифров. Датчанин Ларс Кнудсен уже упоминался в данном обзоре в связи с шифром DEAL (Кнудсен - единственный криптограф, фигурирующий сразу в двух проектах). Англичанин Росс Андерсон из Кембриджского университета с начала 90-х годов известен своими неординарными криптоаналитическими работами.

Требования алгоритма к ресурсам оперативной и постоянной памяти достаточно малы. Алгоритм устойчив практически ко всем атакам по времени исполнения и потребляемой мощности. Использованная в шифре схема поддерживает генерацию материала ключа «на лету» в обоих направлениях. Недостатком является очень маленькая возможность распараллеливания на 32-разрядных платформах. Несмотря на это специалисты рассматривают SERPENT как очень сильный криптоалгоритм.

TWOFISH (США)

Еще один потенциальный финалист. Шифр основан на хорошо известном, популярном и широко используемом в Интернете криптоалгоритме Blowfish, разработанном в 1993 году Брюсом Шнайером, автором книги-бестселлера "Прикладная криптография". За прошедшие годы в открытой литературе не появилось ни одной работы о сколь-нибудь успешном вскрытии Blowfish. В команду создателей нового шифра Twofish почти в полном составе входит консалтинговая криптофирма Шнайера Counterpane Systems (сам Шнайер, Джон Келси, Крис Холл и Нильс Фергюсон), а также шеф по технологиям фирмы Hi/fn Дуг Уайтинг и Дэвид Вагнер, исследователь из калифорнийского университета Беркли, известный по ряду заметных криптоаналитических работ.

По оценкам специалистов, новый алгоритм Twofish эффективно реализуется на 32-битных микропроцессорах, 8-битных смарт-картах и ожидаемых в будущем 64-битных архитектурах, предложенных фирмами Intel и Motorola. Дабы подчеркнуть криптостойкость своего творения, создатели Twofish объявили об учреждении приза в 10 тысяч долларов за лучшую криптоаналитическую атаку против Twofish.

Cipher	Type	Rounds
CAST-256	Ext. Feistel	48
Crypton	Square	12
Deal	Feistel	6, 8, 8
DFC	Feistel	8
E2	Feistel	12
Frog	Special	8
HPC	Omni	8
LOKI97	Feistel	16
Magenta	Feistel	6, 6, 8
Mars	Ext. Feistel	32
RC6	Feistel	20
Rijndael	Square	10, 12, 14
Safer+	SP network	8, 12, 16
Serpent	SP network	32
Twofish	Feistel	16

Общая структура алгоритмов

В таблице слева приводится краткое описание структуры алгоритмов-кандидатов на AES, а именно - типы шифров и количество раундов шифрования. Как можно видеть большинство шифров имеет в своей основе схему Фейстела.

Итоги первого этапа испытаний

Предварительные испытания эффективности алгоритмов-кандидатов провел сам NIST. Под эффективностью шифра понимаются два основных показателя: скорость шифрования/расшифрования и скорость формирования криптографических ключей.

В качестве первой тестовой платформы был выбран IBM-совместимый ПК с процессором Intel-Pentium Pro 200 МГц, с 64 Мб RAM и ОС Windows 95. Тестирование проводилось с оптимизированными кодами на языке ANSI C, представленными самими разработчиками алгоритмов.

Испытания на скорость шифрования/расшифрования (компилятор Borland) выявили 6 более-менее очевидных лидеров, продемонстрировавших скорость свыше 25 Мбит/сек: Crypton (40 Мбит/сек); Rijndael; RC6; E2; Twofish и Mars (26 Мбит/сек). На последних местах оказались Magenta и HPC со скоростью около 2 Мбит/сек, остальные алгоритмы показали результаты от 6 до 10 Мбит/сек. Сразу же было отмечено, что при других компиляторах показатели могут сильно отличаться. Что же касается скорости формирования ключей, то здесь разброс оказался значительно шире: от 500 000 кл/мсек (Crypton) до 100 кл/мсек (HPC и FROG). Среди лидеров в этом разряде можно отметить алгоритмы Magenta, E2, Safer+, RC6, Rijndael, Mars, Serpent, Twofish.

Тестирование шифров-кандидатов производилось также на множестве других платформ и при использовании разных компиляторов. Ниже для справки приведена таблица результатов испытаний 13 шифров на скорость шифрования при использовании различных платформ: Pentium II фирмы Intel, UltraSPARC фирмы Sun and Alpha AXP 21164 фирмы Compaq. Числа в таблице – количество машинных тактов требуемых для шифрования 128-битного блока.

Cipher	Pentium II	Alpha	SPARC	$\overline{x}$
Rijndael	284	490	328	367.3
Twofish	258	490	487	411.7
Crypton	390	499	477	455.3
DFC	480	323	802	535.0
E2	415	587	711	571.0
MARS	376	507	840	574.3
RC6	243	559	1161	654.3
CAST-256	668	749	694	703.3
HPC	1468	$\approx$ 420	450	779.3
Serpent	992	998	992	994.0
Safer+	$\approx$ 775	1502	3002	1759.7
Frog	2572	2752	2337	2553.7
DEAL	2339	2752	2781	2624.0

Что же касается стойкости шифров, то этот показатель проверить значительно сложнее. В ходе этапа предварительной оценки первого круга на web-сайте НИСТ и непосредственно на конференции AES2 было представлено значительное количество криптоаналитических результатов, так или иначе испортивших репутацию практически всех шифров-кандидатов. Однако, если не говорить о явных аутсайдерах LOKI, Frog, Magenta и HPC, то никаких очевидных слабостей в алгоритмах не обнаружено.

Таким образом в завершении первого этапа конкурса на основе многочисленных испытаний предложенных алгоритмов NIST отобрал пять сильнейших кандидатов - MARS, RC6, Rijndael, Serpent и Twofish.

Второй этап конкурса.

После того как были объявлены победители первого этапа, на них более тщательно сконцентрировалось внимание специалистов комитета. Было получено огромное количество информации, касающейся скорости работы шифров при различных программных и аппаратных

реализациях. Ниже приведены таблицы, отражающие производительность алгоритмов-финалистов на некоторых базовых программных платформах. В таблицах римская цифра "I" соответствует наибольшей производительности.

Скорость шифрования/расшифрования на различных платформах

	32-bit (C)	32-bit (Java)	64-bit (C and assembler)	8-bit (C and assembler)	32-bit smartcard (ARM)	Digital Signal Processors
MARS	II	II	II	II	II	II
RC6	I	I	II	II	I	II
Rijndael	II	II	I	I	I	I
Serpent	III	III	III	III	III	III
Twofish	II	III	I	II	III	I

Скорость формирования ключей на различных платформах

	32-bit (C)	32-bit (Java)	64-bit (C and assembler)	8-bit (C and assembler)	Digital Signal Processors
MARS	II	II	III	II	II
RC6	II	II	II	III	II
Rijndael	I	I	I	I	I
Serpent	III	II	II	III	I
Twofish	III	III	III	II	III

Скорость, усредненная по всем платформам

	Enc/Dec	Key Setup
MARS	II	II
RC6	I	II
Rijndael	I	I
Serpent	III	II
Twofish	II	III

Что касается стойкости криптографических алгоритмов, то ни к одному из претендентов по этому аспекту претензий не предъявлялось. Запас стойкости был несколько завышен у алгоритмов MARS, Serpent, Twofish (что проявляется в избыточном времени шифрования) и оптимален у алгоритмов RC6 и Rijndael.

По приведенным выше результатам исследования шифров уже можно судить, кто мог стать победителем конкурса на AES. Из пяти финалистов выделился сильный лидер - Rijndael. В его пользу говорил также огромный потенциал по распараллеливанию вычислений. Немаловажным было и то, что алгоритм Square, на котором по сути базировался Rijndael, уже два года успешно сопротивлялся криптографическим атакам. Ко всему прочему из-за своей простоты (Rijndael не использует какие-либо специфические 32- или 64-битные операции) алгоритм подходит для широкого круга архитектур и очень эффективен при аппаратной реализации.

Все эти причины причины заставили NIST сделать свой выбор в сторону бельгийского шифра RIJNDAEL, а затем начать подготовку плана Федерального Стандарта Обработки Информации (Federal Information Processing Standard) для AES.

Литература:

[1] Б. Киви. *Конкурс на новый криптостандарт AES.*
[2] Helger Lipmaa. *AES Candidates: A Survey of Implementations.*
[3] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback. *Report on the Development of the Advanced Encryption Standard (AES).*
[4] *Общие сведения о конкурсе AES*. http://kiev-security.org.ua/box/1/56.shtml