Конкурс на новый криптостандарт AES

В 1972 и 1974 годах Национальным бюро стандартов США (сегодня НИСТ, или Национальный институт стандартов и технологий) был объявлен первый открытый конкурс на федеральный стандарт шифрования данных. Результатом этого начинания стал DES (Data Encryption Standard) - возможно, самый широко используемый и самый успешный криптоалгоритм в мире. После 1977 года НИСТ каждые пять лет вновь утверждал DES в качестве национального стандарта шифрования. Делалось это не очень охотно, но более современного эквивалента DES не виделось. Однако, вместе с развитием технологической базы и ростом вычислительной мощности процессоров, все более остро стала ощущаться и потребность в новом криптостандарте. К середине 1990-х годов было уже совершенно очевидно, что DES стал архаикой: 56 бит ключа - это слишком мало, шифр весьма медленно работает в программных реализациях, да и аппаратная реализация изначально была сориентирована на 4-битные процессоры 1970-х. С учетом всех этих обстоятельств, в январе 1997 г. НИСТ объявил о запуске программы по принятию нового криптостандарта AES. Согласно целям новой программы "AES будет определять незасекреченный алгоритм шифрования, способный защищать важную информацию правительственного уровня в следующем столетии". Исходные минимальные требования к новому криптоалгоритму были следующими:

- AES должен быть открыто опубликован;
- AES должен быть симметричным блочным шифром;
- AES должен быть разработан так, чтобы длину ключа можно было при необходимости увеличить;
- AES должен допускать как аппаратную, так и программную реализацию;
- AES должен быть бесплатным, то есть либо незапатентованным, либо с аннулированными патентными правами;

Алгоритмы-кандидаты, отвечающие перечисленным требованиям, подлежат исследованиям по следующим параметрам: стойкость (т.е. усилия, требуемые при криптоанализе); вычислительная эффективность; требования к памяти; удобство аппаратной и программной реализации; простота; гибкость.

Естественно, данная инициатива НИСТ вызвала живой интерес не только в американских правительственных кругах и промышленности, выполняющей государственные заказы. Хотя стандарты НИСТ являются обязательными только для правительственных структур США, тем не менее, ими охотно пользуются и во всем остальном мире, в частности, банковская сфера, телекоммуникационные компании, компьютерная индустрия и т.д. Собственно говоря, именно поэтому федеральный криптостандарт DES и стал самым распространенным на планете шифром. В апреле 1997 года, после обсуждения проблемы со всеми заинтересованными сторонами, НИСТ сформулировал более конкретные требования к новому криптостандарту и их разъяснения. По убеждению НИСТ, AES должен быть симметричным блочным, а не поточным шифром. При разъяснении позиции НИСТ было сказано, что, во-первых, блочный шифр AES станет прямым преемником концептуально такого же шифра DES, и, во-вторых, уже имеющиеся утвержденные стандарты режимов функционирования криптоалгоритма ориентированы на блочное шифрование. Излагая взгляд НИСТ на новый шифр в самой краткой форме, можно сказать, что AES должен существенно превосходить по эффективности "тройной DES" и при этом не уступать ему в стойкости.

В окончательной формулировке требования к AES стали выглядеть так. Шифр должен иметь размер блока 128 бит (существенно, что это требование сразу же вывело из игры почти все применяющиеся ныне алгоритмы, традиционно ориентированные на 64-битный блок), и допускать размеры ключей в 128, 192 и 256 бит. На сегодняшний день вполне достаточной длиной ключа считают 80 бит, однако, учитывая, что AES принимается на 20-30 лет, длина ключа выбрана с солидным запасом.

В сентябре 1997 года НИСТ опубликовал приглашение выдвигать кандидатов на AES,

призвав принять участие в конкурсе желающих из всех стран. Высказывались также мнения, что в конкурсе должно принять участие и АНБ США, как наиболее компетентное в криптографии национальное ведомство. Однако, Агентство национальной безопасности, занимающееся разработкой шифров для защиты секретов американского правительства и вскрытием шифров иностранных, объявило, что не будет выставлять своего кандидата на AES. Как сказали в АНБ, об этом их попросил сам НИСТ, поскольку в такой ситуации они смогут быть беспристрастным участником процесса выбора победителя, а не участвующей в конкурсе стороной. В августе 1998 г. в калифорнийском городе Вентура прошла AES1 - "Первая конференция кандидатов на AES", где были объявлены 15 принятых на конкурс алгоритмов, разработанных криптографами из 12 стран. Мировая криптографическая общественность более чем доброжелательно отреагировала на стремление НИСТ к открытому и интернациональному процессу принятия и обсуждения шифров-кандидатов.

Принятые на конкурс алгоритмы

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). Другими словами, здесь нет традиционной для многих блочных шифров так называемой "структуры Фейстела", оперирующей в каждом цикле шифрования половиной блока данных (как в DES или CAST, к примеру). 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. Однако, автор шифра не придерживается общепринятых правил: он уже неоднократно вносил модификации в конструкцию алгоритма после всех контрольных сроков. Это обстоятельство существенно понижает шансы данного кандидата на вхождение в группу лидеров.

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 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. Эта методика разработана, главным образом, одним из соавторов DFC Сержем Водене. Водене имеет репутацию превосходного криптографа, его теоретические идеи встречены с большим интересом, но нельзя не отметить, что уже появились аналитические результаты, несколько скомпрометировавшие 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. Имеется в виду, что для описания конструкции E2 применимы практически те же самые слова, но с одним национальным нюансом - методика конструирования доказуемо стойких шифров здесь своя, японская. 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 - люди, мягко говоря, малоизвестные в криптографическом мире. Согласно характеристике разработчиков, FROG - это "новый шифр с неортодоксальной структурой". Но "неортодоксальность" - это не всегда хорошо, особенно в криптографии. Уже через месяц после публикации алгоритма появились криптоаналитические результаты, свидетельствующие, что FROG - явно недостаточно сильный шифр для AES. Команда "Twofish" (Вагнер, Фергюсон и Шнайер) нанесла мощный удар по команде "Frog". 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.

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 - одна из немногих женщин-криптографов "с именем". 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 вслед за публикацией в Интернете описания шифра LOKI97, появились и результаты его криптоанализа, выполненного Ларсом Кнудсеном и Винсентом Рэменом (из команд "Serpent" и "Rijndael", соответственно). Из этих результатов следовало, что цикловая функция шифра не обладает достаточной криптографической стойкостью, и с довольно высокой вероятностью можно подбирать криптоаналитические методы вскрытия шифра.

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. Немцы предпочли не публиковать заранее свой алгоритм в Интернете. Тем большее разочарование, надо полагать, постигло их непосредственно на самой конференции AES1, когда в ходе сессии вопросов-ответов криптосхема MAGENTA была "на лету", 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 той самой "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 считается 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". 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 (генерация материала ключа по ходу алгоритма возможна только в прямой процедуре — шифровании (при этом требуется только около 100 байт временных переменных), для дешифрования приходится создавать все 768 байт материала ключа — это является достаточно большими требованиями для чипов пластиковых карт.). Алгоритм требует минимальные ресурсы неизменяемой памяти для хранения своего кода и чрезвычайно прост, что является преимуществом как в плане реализации, так и в плане более тщательного криптоанализа.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. К недостаткам алгоритма относят нестойкость шифра к атакам по скорости исполнения и потребляемой мощности, кроме того алгоритм достаточно слабо распараллеливаем. Тем не менее, 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 неизменяемой 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. Генерация материала ключа по ходу алгоритма возможна только в прямой процедуре — шифровании, для дешифрования приходится создавать все байты материала ключа.

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. (Правда, сам Джеймс Мэсси почему-то считает, что его соавторами являются Гурген Хачатрян и Мелсик Курегян из Академии наук Армении, известной своими многолетними связями с Cylink.) 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. Бытует распространенное мнение, что по-настоящему хороший шифр может создать только тот, кто до этого добился серьезных успехов в криптоанализе. Требования алгоритма к ресурсам оперативной и постоянной памяти достаточно малы. Из-за применения только указанных выше примитивов 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.

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". 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.

Итоги первого раунда

Одна из самых больших проблем при сравнении разнообразных алгоритмов - это два конфликтующих между собой требования к конструкции шифра: стойкость и скорость. Упор на усиление одного из этих параметров неминуемо ослабляет другой. Поскольку разработчики разных шифров вольно или невольно отдавали предпочтение одному из этих показателей, задача сравнения получившиеся в итоге конструкций оказывается достаточно нетривиальной.

Предварительные испытания эффективности алгоритмов-кандидатов провел сам НИСТ. 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. (Сразу же было подчеркнуто, что предусмотрены и другие тесты на различных платформах и с различными компиляторами.) 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. Например, при компиляторе DJGPP алгоритм MARS демонстрирует скорость свыше 60 Мбит/сек, а лидер Crypton - менее 30 Мбит/сек. 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.

В течение 2 лет специалисты комитета, исследуя самостоятельно, и изучая публикации других исследователей, выбрали 5 лучших представителей, прошедших в «финал» соревнования. Ими стали: MARS, RC6, Rijndael, Serpent, TwoFish.

Ключевые моменты итогового заявления NIST в отношении финалистов сводятся к следующему:

- ни к одному из претендентов нет претензий к криптографической стойкости; запас стойкости несколько завышен у алгоритмов MARS, Serpent, Twofish (что сказывается на избыточном времени шифрования) и оптимален у алгоритмов RC6 и Rijndael
- по быстродействию в программной реализации первые места занимают RC6 и Rijndael, причем первый уверенно лидирует на 32-разрядных платформах, а второй — на всех остальных архитектурах
- процедура расширения ключа выполняется за наименьшее время у алгоритма Rijndael
- при реализации на архитектурах, ограниченных в ресурсах, вне конкуренции в плане требований является Rijndael
- по быстродействию в аппаратной реализации первые места занимают Rijndael и Serpent
- к атакам, связанным с особенностями сред исполнения команд, наиболее устойчивы Rijndael и Serpent
- в отношении объема дополнительных ресурсов памяти для реализации дешифрования в предпочтительном положении находятся Twofish, MARS и RC6
- наименее ресурсоемкой схемой генерации ключей «на лету» обладает алгоритм Twofish
- в плане возможности распараллеливания вычислений с отрывом в несколько раз лидирует алгоритм Rijndael

Комплексный анализ всех описанных выше достоинств и недостатков привел к тому, что новым стандартом блочного шифрования объявлен алгоритм RIJNDAEL. 2 октября 2000 года многолетний и трудный проект был завершен. С алгоритма Rijndael по условиям конкурса сняты все патентные ограничения — его использование в различных продуктах на территории США теперь контролируется только государственными нормативными актами этой страны. Сам алгоритм получил почетное второе наименование: Advanced Encryption Standard — AES.

Использованная литератра:

http://csrc.nist.gov/CryptoToolkit/aes/

http://electronica.finestreet.ru/5/index.shtml

http://kiev-security.org.ua