Безопасность данных: так ли надёжна криптография?

Криптографические приложения, в связи с расширением объёмов виртуальной экономики, увеличения числа безналичных расчётов (в т.ч. разнообразные "электронные деньги") и т.п., применяются всё шире и поэтому проблемы, связанные с информационной безопасностью, будут привлекать всё большее внимание. Reuters пишет, что U.S. National Security Agency (NSA) заплатило 10 млн. долларов за возможность облегченного доступа к данным, зашифрованным с использованием стандартизированного в США алгоритма Dual EC DRBG, разработанного хорошо известной компанией RSA.

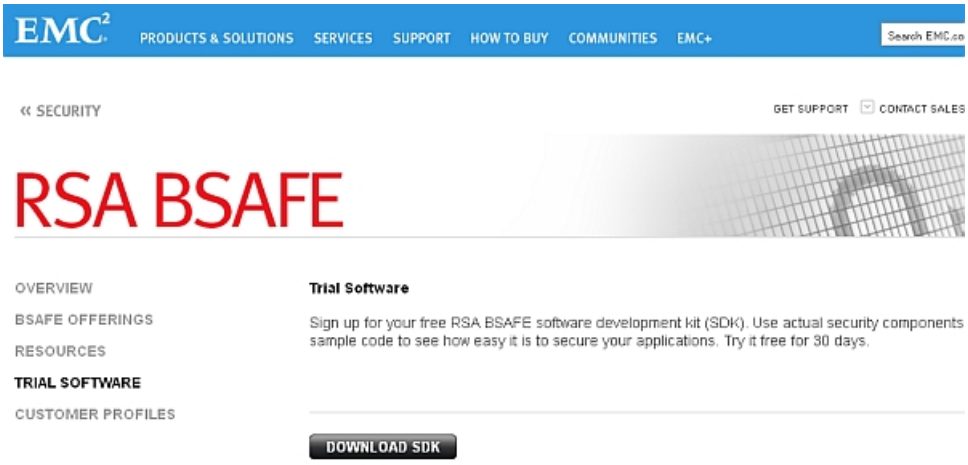
"Никому нельзя верить!" — в очередной раз можно воскликнуть, ознакомившись с информацией в этом материале. Можно вспомнить и другое утверждение — "всё имеет свою цену!". Ну и в очередной раз подтверждается, что "слабое звено" в любой суперсистеме — это человек — существо, иногда действующее иррационально, иногда с ошибками. А ещё есть человеческие пороки...

Почти всё изложенное ниже касается событий в США — реальность такова, что многое в интернет-технологиях формально и неформально связано с Америкой. "Вдруг" выяснилось, что американцы сумели использовать эту ситуацию в своих целях. Международное сообщество возмутилось бесцеремонностью и широкими возможностями американских спецслужб, но эти успехи не были бы возможны без соответствующей технологической подготовки на разных уровнях и в разных сферах. Теперь "руку" агентов NSA уже ищут в IETF: их деятельность (в свою пользу) может сказаться на безопасности будущих интернет-технологий. Пока же можем обсудить то, что уже стало известно на сегодняшний день.

RSA Security продала NSA "back door"

О возможности лёгкого доступа американских спецслужб к данным, которые были предварительно, казалось бы, надёжно зашифрованы, писала газета New York Times (и несколько других изданий, например, The Guardian) в сентябре 2013 года. И Reuters и New York Times сообщают об этих проблемах в безопасности, опираясь на информацию из материалов, которые когда-то предоставил журналистам Эдвард Сноуден (Edward Snowden). В новой статье Reuters пишет, что компания RSA получила 10 млн. долларов от Агентства Национальной Безопасности (National Security Agency) и предполагает, что это оплата за возможность доступа к приложениям, разработанным с применением Dual EC_DRBG (этот алгоритм используется в ПО RSA BSAFE). То есть у спецслужб есть информация, позволяющая упростить дешифрацию и последующий мониторинг информации любого рода. Этот факт вновь привлёк внимание.

На статью откликнулась только одна компания из упомянутых. По поводу сотрудничества с АНБ, в RSA пояснили, что этот факт не скрывается, про деньги не сказали ничего, а относительно всего остального: "RSA always acts in the best interest of its customers and under no circumstances does RSA design or enable any back doors in our products", — заявила RSA Security. Позже, 22 декабря, даже вышел отдельный пресс-релиз RSA. Вторая сторона "сделки" — Агентство Национальной Безопасности отказалось от комментариев, сообщает Reuters.



С сентября внешне ничего не изменилось. По-прежнему, на сайте EMC Corp, которой и принадлежит компания RSA, в одном из разделов желающие могут скачать и в течение месяца попробовать программное обеспечение RSA BSAFE ("Sign up for your free RSA BSAFE software development kit (SDK). Use actual security components and embed sample code to see how easy it is to secure your applications"). Хотя вроде бы сама RSA косвенно признала наличие проблемы, рекомендовав перестать пользоваться некоторыми своими программными продуктами, об этом будет сказано чуть позже.

Причина шумихи

Дело в том, что ещё в 2007 году была публикация "On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng (Dan Shumow, Niels Ferguson из Microsoft)", где было высказано предположение о возможности взлома этого алгоритма только из-за того, что в NIST странным образом его реализовали при стандартизации, фактически ослабив. Специалисты своё дело сделали — предупредили.

[Безопасность данных: так ли надёжна криптография?]

Из презентации "On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng"

Появление дополнительной информации — о "контракте" и о "деньгах" — взволновала и пользователей, и экспертов. Шум поднялся по нескольким причинам: пользователи продуктов RSA не предполагали, что сам разработчик средств безопасности окажется в роли этакого хакера, пытающегося легко получить (или в данном случае помочь получить третьей стороне) доступ к непубличной информации. Дополнительное возмущение связано с тем, что на этом компания RSA ещё и заработала (Reuters ссылается на двух источников, знающих о наличии контракта). Ну и наконец, RSA заработала и на компаниях, выбравших её решения, и вот теперь после всего этого они должны что-то предпринимать и думать о дальнейших своих действиях. Довериться, заплатить деньги и оказаться в дураках? Ситуация на букву "х"...

Как я уже писал выше, на "пропущенную" (намеренно или случайно — это неважно) слабость в Dual EC_DRBG обратили внимание впервые в 2007 году. Потом в наличие такой "возможности" убеждались (теоретически и практически) другие исследователи и эксперты по безопасности.

Волна упрёков, теперь уже со стороны профессионального сообщества, вызвана как раз тем, что RSA, зная о наличии "изъяна" в этом криптографическом методе, более 5 лет, до сентября 2013 года, практически ничего не делала для повышения качества своего продукта.

И вот только осенью, после появления статей в нескольких известных газетах, в RSA озвучили: "To ensure a high level of assurance in their application, RSA strongly recommends that customers discontinue use of Dual EC DRBG and move to a different PRNG". Рекомендация была адресована клиентам, которые пользуются BSAFE toolkit и Data Protection Manager от RSA. Но, так как в виде библиотек, алгоритм мог использоваться и в продуктах, разработанных другими компаниями, то "масштаб бедствия" может оказаться намного шире.

Далее. Доверие можно легко разрушить. Если в стандарте так беспечно (случайно или за деньги) отнеслись к наличию "back door" в одном алгоритме, можно ли быть уверенными на 100% в безгрешности других рекомендованных способов?

В 2006 году Американский Институт стандартизации и технологий (National Institutes of Standards and Technology, NIST) стандартизировал "Dual Elliptic Curve Deterministic Random Bit Generator", наряду с Hash_Based DRBG, CTR_DRBG и HMAC_Based DRBG, для применения в различных информационных системах США. Поэтому Dual EC DRBG используется, например, в McAfee Firewall Enterprise Control Center, который предназначен для американских госучреждений.

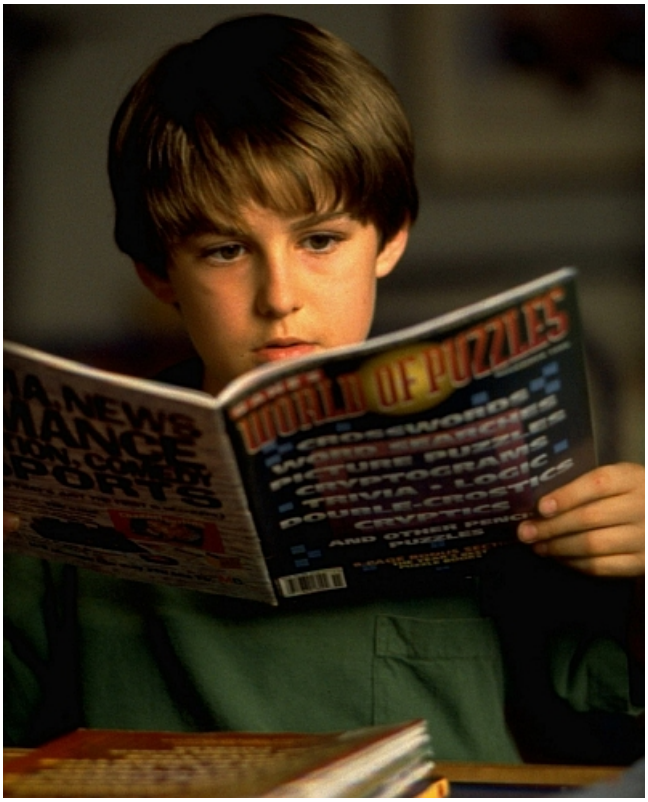
Согласно данным в "DRBG Validation List", который ведёт NIST, в общей сложности, на 20 декабря 2013 года этот институт сертифицировал применение указанных четырёх алгоритмов реализации Deterministic Random Bit Generator (DRBG) в 462 продуктах (чисто программных или в виде "прошивок", как у Utimaco для чипа Texas Instruments TMS320C6416T) таких компаний, как Symantec, Cisco, Blue Coat, Brocade, McAfee и так далее.

Внимание (без паники): именно Dual EC DRBG применяют не все и не везде. Используют, как минимум: Mocana Corporation, сама RSA, Cisco в "CiscoSSL FIPS Object Module"*, BlackBerry в "BlackBerry Cryptographic Algorithm Library", Certicom Corp., Juniper Networks в "Juniper Networks Pulse Cryptographic Module"**, OpenPeak Inc. в OpenPeak Cryptographic Security Library и так далее. Тут понятно беспокоиться нужно пользователям только этих продуктов.

Но, как в New York Times, так в других СМИ, большую тревогу вызвало то, что Dual EC DRBG (правда не на эксклюзивной основе, задействованы и другие три метода) используется, например, OpenSSL Software Foundation, Inc. в виде "OpenSSL FIPS Object Module", а это может иметь уже более повсеместное распространение (в газетах написали об угрозах всему шифрованному интернет-трафику). Ещё вспомнили и об уязвимости данных в сотовых сетях с учётом того, что трафик в сетях 3G/4G преимущественно не голосовой.

Часть обсуждающих проблему наличия "back door" в криптографических приложениях высказали опасение, что эти "тайные ходы" могут быть использованы против отдельных учреждений и, против безопасности США в целом, в случае, если станут известны "недружественным силам". То есть применение спецслужбами таких способов "облегчения" своей работы может сыграть в обратную сторону и тогда доступ к информации, в том числе и к частной (электронная переписка, онлайн-банкинг, медицинские данные), может получить некая "третья сторона".

Jeffrey Carr, chief executive of Taia Globa, так озаглавил свой пост "Who's Defending U.S. Military Networks if the NSA and FIS are Breaking Them?", в котором он упоминает про хороший уровень подготовки российских и китайских специалистов по информационной безопасности, и что наличие "backdoors" NSA на самом деле ослабляет защиту данных в сетях американских госучреждений, включая военные ведомства.



Фильм "Меркурий в опасности" (Mercury Rising) вышел в 1998 г (источник фото: сайт КиноПоиск)

А американцы всегда стремились к защите личной информации: пару десятилетий назад широкое распространение получил, так называемый "Clipper chip" — аппаратная реализация стойкого шифрования, рекомендованная в США для применения телефонными компаниями. Широко применялось это решение в том виде не очень долго. Одной из причин стали деньги — возникли опасения, что телефонное оборудование не будут покупать иностранные компании именно из-за наличия проприетарной реализации и опять же из-за наличия "back door" — можно почитать (есть статья в New York Times — "Battle of the Clipper Chip") о протестах в США в 1994 году, когда это выяснилось. И вот опять в одном ряду: данные, безопасность, деньги...

Месяц назад Deutsche Telekom объявил о запуске в следующем году новой услуги "clean pipe" для среднего и малого бизнеса. Основная ценность этой услуги, которую сформулировал немецкий телеком-гигант — это защита от хакеров и от иностранных разведок. В подтверждение актуальности своего предложения Deutsche Telekom привел данные, что лишь 13 процентов немецких компаний не испытали кибератаки, а около трети из более чем 200 компаний с числом работников более 1000 пережили несколько атак в неделю. Тестирование услуги будет проходить до конца года, партнёром Deutsche Telekom является ... RSA. Странно, неужели в Германии нет собственных реализаций криптографических алгоритмов? Впрочем, это их дело.

Из последних новостей

- Похоже, что в отличие от сентябрьских сообщений, в этот раз, на статью в Reuters обратили внимание большее количество людей. И даже перешли к более активным действиям. Так, например, от возмущения бездействием и игнорированием со стороны RSA основ бизнеса в сфере безопасности, например, Mikko Hypponen*** — руководитель исследовательского направления в финской компании F-Secure, занимающейся антивирусными и т.п. продуктами публично отказался ехать с запланированным выступлением на RSA Conference USA 2014, которая должна пройти в феврале 2014 года. Возможно, кто-то ещё из коллег последует его примеру.

  Update (09.01.2013): Mikko Hypponen уже не единственный, кто отказался от участия в февральском мероприятии RSA. Статья была написана в конце декабря 2013 года, а в январе этого года стало известно, что, как минимум, шесть человек изменили свои планы и не намерены быть участниками RSA Conference USA 2014. The Wall Street Journal сообщает о бойкоте

- Вроде как, OpenSSL Software Foundation прореагировало в этот раз и готово заново сертифицировать "OpenSSL FIPS Object Module" с учётом сомнений в качестве Dual EC DRBG.
- На уровне администрации американского президента также зашевелились. В начале декабря Консультативный комитет, после анализа появления информации от Сноудена о многообъемлющей и географически распространенной прослушки телефонных переговоров, изложил 46 рекомендаций по "наведению порядка" в сфере безопасности (308-страничный отчёт был подготовлен в соответствии с меморандумом президента Обамы от 27 августа 2013 года). Есть там и про недопущение ухудшения бизнеса американских компаний, которые предлагают коммерческие продукты в сфере безопасности. Также рекомендуется правительству США полностью поддерживать, а не разрушать, усилия по созданию стандартов шифрования, а также стремиться увеличить использование шифрования. Кроме этого, американским компаниям нужно сделать всё, чтобы как можно лучше защитить данные при передаче информации, при её хранении, при нахождении её в "облаке" или в любом другом хранилище данных.



В заключение (переводить не стал, не вижу смысла) процитирую информацию из приложения, которое "обнаружилось" в "Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies", информацию для которого предоставила NSA. Так сказать, для справки и для демонстрации как в США исторически продвигались в этой сфере деятельности, в том числе опираясь на международный опыт, а потом старались реализовать всё это, уже как независимые разработки, защищенные на уровне IP-законодательства и национальных стандартов. Заголовок про "роль" тоже оттуда.

US Government Role in Current Encryption Standards

... Most of the standards described below are approved by NIST for protecting unclassified US Government information and by NSA for protecting classified US Government information. AES, SHA-2, EC-DSA, and EC-DH make up the core of "Suite B," NSA's mandated set of public standard algorithms, approved in 2006, for protecting classified information. Each algorithm discussed below is currently in use in National Security Systems, although NSA is pursuing the transition from SHA-1 to SHA-2. For further information on all but SHA-1 (see https://www.cnss.gov/policies.html) and references contained there. In general, NSA applies the deep cryptanalytic tradecraft and mathematical expertise developed over decades of making and breaking codes, to ensure that cryptography standardized by the US Government is strong enough to protect its own sensitive communications.

AES – The Advanced Encryption Standard – FIPS 197
NSA did not contribute to nor modify the design of the Advanced Encryption Standard (AES). It was designed by two European cryptographers: Joan Daemen and Vincent Rijmen. It was published and submitted in 1998 for NIST's AES competition and selected in 2001 as the Advanced Encryption Standard. NSA extensively examined the algorithms in the competition and provided technical guidance to NIST during the competition to make sure that NIST's final selection was a secure algorithm. NIST made the final algorithm choice under its own authority, independent of NSA. Both NSA and the academic cryptography community have thoroughly analyzed the AES.

RSA – The Rivest, Shamir, Adelman Public Key Algorithm – FIPS 186, NIST SP 800-56B
NSA did not contribute to, nor modify, the design of RSA, but it did provide input on RSA usage in standards. It was designed in 1977 by three cryptographers working at MIT: Americans Ron Rivest, and Leonard Adelman, and Israeli Adi Shamir. The algorithm was independently designed earlier by Cliff Cocks of UK GCHQ in 1973 but was not published, and was only declassified in 1997. Both NSA and the academic cryptography community have thoroughly analyzed the RSA algorithm both as a digital signature (FIPS-186)

and as an encryption algorithm for keys (SP 800-56B).

Diffie-Hellman/Elliptic Curve Diffie-Hellman – The Diffie-Hellman Key Exchange Algorithm – NIST SP 800-56A
NSA did not contribute to, nor modify, the design of Diffie-Hellman. The Diffie-Hellman Key Exchange Algorithm was designed by American cryptographer Whitfield Diffie and Martin Hellman at Stanford University in 1976. It was invented by Malcolm Williamson of GCHQ a few years earlier, but never published. The elliptic curve variant of the Diffie-Hellman key exchange was invented independently by American cryptographers Victor Miller and Neal Koblitz in 1985. NSA ensured that a class of potentially weak elliptic curve parameters was not included in the NIST standard. Both NSA and the academic cryptography community have thoroughly analyzed both the Diffie-Hellman Key Exchange algorithm and its elliptic curve variant (both found in NIST SP 800-56A).

DSA/ECDSA—The Digital Signature Algorithm/Elliptic Curve DSA —FIPS 186
NSA designed the algorithm known as DSA as the original signature algorithm in FIPS 186 initially in 1991-1993, then contributed advice on later versions of the standard. NSA also designed a variant of DSA that uses the mathematics of elliptic curves and is known as the “Elliptic Curve DSA” or ECDSA. Both NSA and the academic cryptography community have thoroughly analyzed the DSA (FIPS 186).

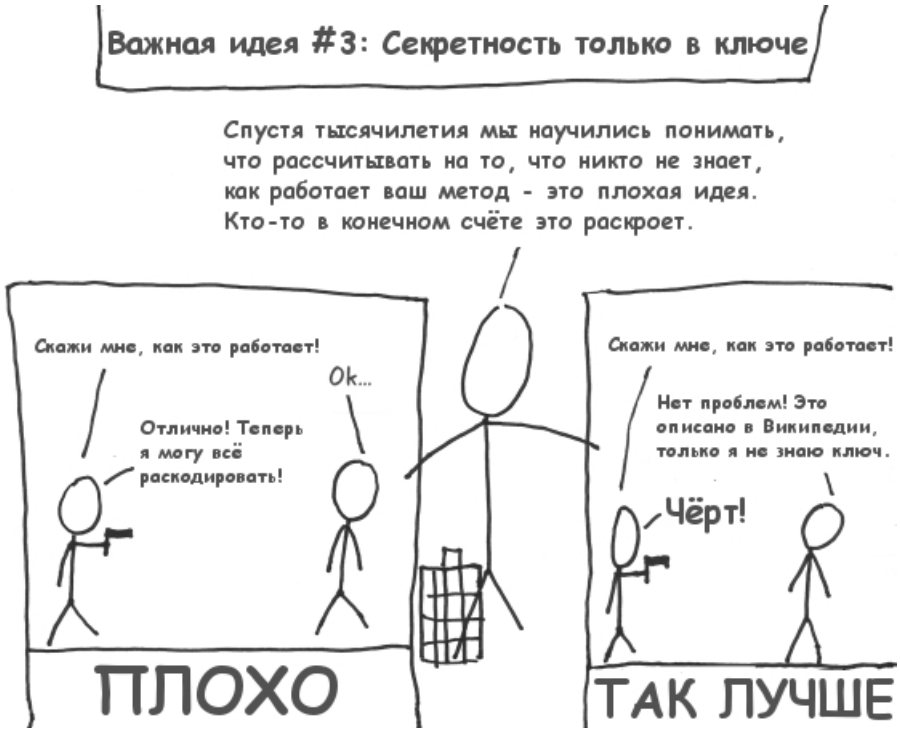
SHA-1 – The Secure Hash Algorithm Variant 1 – FIPS 180-1
NSA designed the SHA-1 algorithm as a correction to the SHA-0 algorithm, a longer (160-bit) variant of the MD5 algorithm designed by Ron Rivest. SHA-0 was an NSA design standardized in 1993. In 1994, NSA acted quickly to replace SHA-0 with SHA-1 as a NIST standard when NSA cryptanalysts discovered a problem with the SHA-0 design that reduced its security. Both NSA and the academic cryptography community have thoroughly analyzed the SHA-1 (FIPS 180). For many years NIST and NSA have recommended that people stop using SHA-1 and start using the SHA-2 hash algorithms.

SHA-2 – The Secure Hash Algorithm Variant 2 – FIPS 180-2
NSA designed the four different-length hash algorithms contained in FIPS-180-2 and collectively known as SHA-2. Because of their longer hash lengths (224, 256, 384, and 512 bits), the SHA-2 hash lengths provide greater security than SHA-1. SHA-2 also blocks some algorithm weaknesses in the SHA-1 design. These algorithms were standardized in 2002. Both NSA and the academic cryptography community have thoroughly analyzed the SHA-2 hash algorithms (FIPS 180).

РОССИЯ

Немного придётся потратить время, чтобы найти, что в настоящее время действует "свеженький" (введён с 1 января 2013 года) измененный вариант отечественного криптографического стандарта — "ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования". Сказано, что он заменяет ГОСТ Р 34.11-94 (причина выделена болдом): "Стандарт разработан взамен ГОСТ Р 34.11-94. Необходимость разработки настоящего стандарта **вызвана потребностью в создании хэш-функции, соответствующей современным требованиям к криптографической стойкости** и требованиям стандарта ГОСТ Р 34.10-2012 к электронной цифровой подписи".

То есть сейчас для России актуальны: "ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи" и только что упомянутый "ГОСТ Р 34.11-2012".



Источник: Jeff Moser http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

Не буду пересказывать Википедию, где сказано, что "*ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001 основаны на эллиптических кривых. Стойкость этих алгоритмов основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости хэш-функции. Для ГОСТ Р 34.10-2012 используется хэш-функция по ГОСТ Р 34.11-2012. Для ГОСТ Р 34.10-2001 - ГОСТ Р 34.11-94.*

Стандарт ГОСТ Р 34.10-2012 использует ту же схему формирования электронной цифровой подписи, что и ГОСТ Р 34.10-2001. Новый стандарт отличается наличием дополнительного варианта параметров схем (соответствующего длине секретного ключа порядка 512 бит) и требованием использования функций хэширования ГОСТ Р 34.11-2012: первый вариант требований к параметрам (такой же, как в ГОСТ Р 34.10-2001, соответствующий длине секретного ключа порядка 256 бит) предусматривает использование хэш-функции с длиной хэш-кода 256 бит, дополнительный вариант требований к параметрам предусматривает использование хэш-функции с длиной хэш-кода 512 бит."

Таким образом, перейдя в ГОСТе 2001 года к применению эллиптических кривых, в государственном стандарте, введённом в 2013 году, сложность вычислений решили повысить увеличением хэш-хода.

[Безопасность данных: так ли надёжна криптография?]
Если обобщить всю информацию, связанную с претензиями к RSA, то получается, что "Dual Elliptic Curve Deterministic Random Bit Generator" не очень-то "random generator"

Несмотря на предложенные и уже введенные законодательные изменения в виде ГОСТов, сейчас на сайте одного из разработчиков — ОАО "Информационные технологии и коммуникационные системы" (ОАО "ИнфоТеКС") можно узнать, что проходит "Открытый конкурс научно-исследовательских работ, посвященных анализу криптографических качеств хэш-функции ГОСТ Р 34.11-2012". Сроки: с 21 октября 2013 года по 15 декабря 2014 года, проводится Российским Техническим комитетом по стандартизации "Криптографическая защита информации" (ТК 26) при участии Академии криптографии Российской Федерации и при организационной и финансовой поддержке ОАО "ИнфоТеКС".



Не знаю причин проведения конкурса (кроме "лежащего на поверхности" желания найти талантливых и увлечённых новых сотрудников, а победитель ещё и неплохие "разовые" деньги получит), но объявление конкурса примерно через год после введения в действие требований безопасности на уровне отечественного стандарта, немного странно. Вторая особенность — сроки, совпавшие с шумихой в США вокруг использования в алгоритме эллиптических кривых. Конечно, нельзя и исключать и случайность и несвязанность этих событий, но тем не менее...

Подытожим: с одной стороны, использование "эллиптических кривых" годится для криптографических целей, а с другой — в процессе написания статьи наткнулся пару раз на утверждения, что нет строгого доказательства надёжности в области несимметричной криптографии. "На сегодняшний день нет доказательства существования или несуществования полиномиального алгоритма дискретного логарифмирования в простом поле", — утверждает автор статьи, посвященной цифровой подписи и эллиптическим кривым.

---
* "The Cisco FIPS Object Module is a software library that provides cryptographic services to a vast array of Cisco''s networking and collaboration products." — примечание на сайте NIST.
** "The Juniper Networks Pulse Cryptographic Module provides secure cryptographic services. It enables dynamic SSL VPN, NAC, mobile security, online meetings and collaboration, and application acceleration while removing the complexities of device type and security state, location, identity, and adherence to policies." — примечание на сайте NIST.
*** Mikko Hypponen неоднократно выступал на таких мероприятиях, как Black Hat, Defcon, Hack in the Box