УДК 004.056.55

ПРОБЛЕМАТИКА ПОПУЛЯРНЫХ АЛГОРИМТОВ ШИФРОВАНИЯ

Р.Ю. КАРАБАНОВ
(Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ)

Рассматриваются самые популярные алгоритмы шифрования и их проблемы в современном информационном мире. Приводятся примеры проблем алгоритмов, в частности опыт взлома и их анализ.

В современном мире приводятся множество требований к алгоритму шифрования, начиная от криптостойкости и заканчивая временем для шифрования/дешифрования данных. Однако самым главным критерием оценки проблемы будем считать факт взлома алгоритма до этого. В данной работе остановимся на трех самых популярных на данное время алгоритмах – AES, DES, RSA. Именно эти три алгоритма реализованы в стандартной библиотеке «javax.crypto» в языке программирования Java – самом популярном объектно-ориентированном языке программирования на 2016 год [1]. Также следует отметить, что данные алгоритмы были введены в общее пользование до нынешнего десятилетия [2–4], а следовательно, не могут, в эру быстро развивающихся информационных технологий называться современными.

1. **DES** (англ. dataencryptionstandard) – алгоритм для симметричного шифрования, разработанный фирмой IBM и утвержденный правительством США в 1977 году как официальный стандарт (FIPS 46-3). Размер блока для DES равен 64 бита. В основе алгоритма лежит сеть Фейстеля с 16 циклами (раундами) и ключом, имеющим длину 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований [4].

Основная проблема. Так как длина ключа равна 56 битам, существует 2^{56} возможных ключей. Сегодня такая длина ключа недостаточна, поскольку допускает успешное применение лобовых атак. Альтернативой DES можно считать тройной DES, IDEA, а также алгоритм Rijndael, принятый в качестве нового стандарта на алгоритмы симметричного шифрования.

Также без ответа пока остается вопрос, возможен ли криптоанализ с использованием существующих характеристик алгоритма DES. Основой алгоритма являются восемь таблиц подстановки, или S-boxes, которые применяются в каждой итерации. Имеет место опасность, что эти S-boxes конструировались таким образом, что криптоанализ возможен для взломщика, который знает слабые места S-boxes. В течение многих лет обсуждалось как стандартное, так и неожиданное поведение S-boxes, но все-таки никому не удалось обнаружить их фатально слабые места [5].

***Вывод*:** данный алгоритм можно легко взломать с помощью перебора.

2. **Advanced Encryption Standard (AES)** – симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES. Национальный институт стандартов и технологий США (англ. National Institute of Standards and Technology, NIST) опубликовал спецификацию AES 26 ноября 2001 года после пятилетнего периода, в ходе которого были созданы и оценены 15 кандидатур. 26 мая 2002 года AES был объявлен стандартом шифрования [3]. Суть AES в том, что любая «лобовая атака» на защищенные данные, то есть подбор всех возможных паролей, в перспективе очень сильно растягивается. Если представить, что взломщик располагает огромными ресурсами, то есть целой коллекцией суперкомпьютеров, то при усердном старании доступ к зашифрованным данным он мог бы получить через десятки лет. Если же в его распоряжении ничего этого нет, то взлом AES займет астрономически долгое время [6].

Основная проблема. Криптографы нашли метод взлома ключей AES-шифра ещё в 2011 году во время конференции по криптографии Crypto 2011, которая проходила в Санта Барбаре, США. Данный метод позволяет злоумышленникам получать секретные AES ключи в пять раз быстрее, чем это делалось ранее. Он же использует технику двудольного криптоанализа для удаления двух битов из 128-, 192- и 256-битных ключей. И эксперты поспешили успокоить общественность: «Данное исследование пошатнуло многие основы, так как мы получили первый метод взлома, AES-шифра с одним ключом, (немного) более быстрый, чем брут форс атака, – заявил Нейт Лаусон, криптограф и начальник отдела консультаций по безопасности компании Root Labs. – Однако с практической точки зрения, AES-шифр взломать пока невозможно» [7].

Тем не менее уже меньше, чем через год, Сергей Скоробогатов, который до этого недавно обнаружил бэкдор в китайском чипе FPGA, произвел успешное извлечение ключа AES, который отмечен как «высокозащищенный» и «практически неломаемый», на FPGA военного уровня Actel/Microsemi ProASIC3 за 0,01 секунду. Использовался способ анализа сторонних каналов, который назвается Pipe-

line Emission Analysis (PEA). Это не новый способ сам по себе, а значительно улучшенный метод волнового анализа. Данный способ используется для атаки на реализацию AES на FPGA, используя наводки и помехи [8].

Вывод: данный алгоритм оказался тоже взламываемым при помощи метода волнового анализа. Также существует вероятность, что при помощи квантовых компьютеров в будущем это будет сделать достаточно быстро, чем это предполагали, когда создавали алгоритм.

3. **RSA** (аббревиатура от фамилий Rivest, Shamir и Adleman) – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других [2].

Основная проблема. Была обнаружена уязвимость в реализации алгоритма RSA, позволившая исследователям взломать 1024-битное шифрование. Но для реализации взлома необходим физический доступ к держателю «секретного ключа», так что на крупных компаниях это вряд ли отразится.

Что же касается обычных гаджетов, то достаточно не упускать их из виду. Докторант Мичиганского университета Андреа Пелегрини (Andrea Pellegrini) завтра представит отчет о проделанной работе на конференции «Design, Automation and Test in Europe» (DATE) в Дрездене.

Но перейдем к сути. Атака на алгоритм проводилась путем искусственного вызова ошибок при помощи изменения напряжения на процессоре. В результате появлялись ошибки в коммуникации с другими клиентами, и удавалось получить небольшую часть ключа, а как только было собрано достаточно частей, ключ был восстановлен в режиме офлайн. На все про все ушло 104 часа работы 81 процессора Pentium 4. Техника не пострадала, следов взлома не осталось. Несмотря на то, что в статье описывается только уязвимость, ученые из университета заявили, что они предлагают довольно простое решение проблемы. Для этого, по их словам, достаточно применить «соль», позволяющую изменять порядок цифр случайным образом при каждом запросе ключа [9].

Таким образом, RSA также был взломан, а алгоритм до сих пор не изменен, следовательно, если бы ученые стремились заново его взломать, то потратили даже меньше 104 часов, потому что вычислительная мощность компьютеров увеличилась.

Заключение

Распространенность алгоритмов шифрования часто служит им плохую службу, потому что все больше злоумышленников и не только пытаются их взломать. Однако стоит отметить, что для своего времени каждый был прорывом в шифровании. И новое время требует новое откровение в среде шифрования данных.

ЛИТЕРАТУРА

7. The 9 Most In-Demand Programming Languages of 2016 [Electronic resource]. – 2016. – Mode of access: http://www.codingdojo.com/blog/9-most-in-demand-programming-languages-of-2016/ . – Date of access: 23.09.2017.
8. RSA [Электронный ресурс]. – 2017. – Режим доступа: https://ru.wikipedia.org/wiki/RSA/. – Дата доступа: 23.09.2017.
9. AdvancedEncryptionStandard [Электронный ресурс]. – 2017. – Режим доступа: https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard. – Дата доступа: 23.09.2017.
10. DES [Электронный источник]. – 2017. – Режим доступа: https://ru.wikipedia.org/wiki/DES. – Дата доступа: 23.09.2017.
11. Криптографические основы безопасности [Электронный ресурс]. – 2017. – Режим доступа: http://www.intuit.ru/studies/courses/28/28/lecture/20412?page=4#sect17. – Дата доступа: 23.09.2017.
12. Алгоритм шифрования AES [Электронный ресурс]. – 2017. – Режим доступа: https://www. opengsm.ru/blog/algoritm-shifrovaniya-aes/. – Дата доступа: 23.09.2017.
13. Криптографы нашли способ взлома ключей AES-шифра [Электронный ресурс]. – 2011. – Режим доступа: http://www.securitylab.ru/news/406880.php . – Дата доступа: 23.09.2017
14. Извлечение AES ключа в мгновение ока [Электронный ресурс]. – 2012. – Режим доступа: https://habrahabr.ru/post/145775/. – Дата доступа: 23.09.2017
15. Взломано 1024-битное шифрование RSA[Электронный источник]. – 2010. – Режим доступа: https: //habrahabr.ru/post/86841/. – Дата доступа: 23.09.2017.