НЕКОТОРЫЕ РЕКОМЕНДАЦИИ ПО ПОВЫШЕНИЮ СТОЙКОСТИ ШИФРА С МАЛЫМ РАЗМЕРОМ КЛЮЧА К МЕТОДУ ПОЛНОГО ОПРОБОВАНИЯ

Варфоломеев А.А.[1]

В работе содержатся рекомендации по повышению стойкости симметричного шифра к методу полного опробования ключей, при условии, что размер ключа не превышает 56 бит. Это условие соответствует требованию регулятора для безлицензионного использования средств криптографической защиты информации. Данные рекомендации существенно повышают сложность восстановления злоумышленником открытого текста указанным методом. Эффективность рекомендаций демонстрируется на примерах при различной вычислительной мощности злоумышленника и законных пользователей.

***Ключевые слова**: криптография, AON преобразование, асимметрия, ГОСТ 28147–89, ГОСТ Р 34.13–2015, открытый текст, шифрование.*

Ограничение размера ключа могут быть вызваны разными причинами. Одна из них связана с требованиями Постановления Правительства РФ от 16.04.2012 N 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, и др. Данное Положение требует от организации, осуществляющей определенные виды деятельности с использованием шифровальных (криптографических) средств получение лицензии на этот вид деятельности. А получение лицензии предполагает выполнение организацией целого ряда требований к персоналу, помещениям, технике и др. Это не всегда может быть выполнено по ряду причин. Однако согласно п. 3.6 данного Положения, оно не распространяется на деятельность с использованием: «*шифровальных (криптографических) средств, а также товаров, содержащих шифровальные (криптографические) средства, реализующих либо симметричный криптографический алгоритм, использующий криптографический ключ длиной, не превышающей 56 бит, либо асимметричный криптографический алгоритм, основанный либо на методе разложения на множители целых чисел, размер которых не превышает 512 бит, либо на методе вычисления дискретных логарифмов в мультипликативной группе конечного поля размера, не превышающего 512 бит, либо на методе вычисления дискретных логарифмов в иной группе размера, не превышающего 112 бит*».

Мы не рассматриваем другого исключительного случая, когда использование шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, «осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя» (п.1 Положения). То есть предполагается, что средства будут использоваться и для других целей без указанного ограничения.

Конечно, организации, не стремящиеся выполнять требования законодательства, могут игнорировать эти требования. Но хотелось бы выяснить, можно ли не нарушая требований законодательства и используя шифровальные (криптографические) средства с длиной ключа малого размера, что не требует получения лицензии, повысить стойкость этих средств. В данной работе приводятся такие рекомендации в отношении симметричных шифров, оценивается эта стойкость в условиях использования современной вычислительной техники.

Предлагаемые решения основаны на асимметрии трудозатрат различными законными участниками протокола обмена шифртекстами и нарушителем информационной безопасности(злоумышленником).

Рекомендация 1. Внести асимметрию в трудоемкость работы при зашифровании открытого текста и при расшифровании шифртекста

В статье Меркля [1] использовалась асимметрия в трудозатратах законных участников протокола (трудоемкость порядка n для каждого участника) и злоумышленника (трудоемкость порядка n^2). Для целей данной работы можно предложить внести асимметрию в трудозатраты при зашифровании и при расшифровании, именно повысив в 2^d раз трудоемкость расшифрования. Здесь d параметр метода, он определяется вычислительными ресурсами участника, выполняющего расшифрование, его терпением (то есть, при имеющихся у него ресурсах, сколько готов ждать результата расшифро-

1 Варфоломеев Александр Алексеевич, кандидат физико-математических наук, доцент, МГТУ им. Н.Э. Баумана, Москва, a.varfolomeev@mail.ru

вания – секунды, минуты, часы и др.).

Рассмотрим в качестве примера для определенности российский симметричный криптографический алгоритм ГОСТ 28147- 89. Разовый ключ k данного алгоритма задается двоичным вектором длины 256 бит, что больше 56 и не удовлетворяет ограничению Постановления. Представим этот вектор в виде конкатенации 3 векторов

k = (k1, …, k56, k57, …, k(56+d), k(56+d+1), …, k256).

Последние 256 – 56-d бит положим фиксированными, например, нулями. Значимыми ключевыми битами, известными обоим законным участникам протокола, будем считать первые 56 бит. Ключевые таблицы на передающем и приемном концах шифрованной связи будут содержать двоичные векторы размера в 56 бит. Напомним, что согласно международному стандарту ИСО/МЭК 18033-1 и другим, «ключ(key) – изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование». Двоичный вектор (v1, …, v56) определяет преобразование алгоритма ГОСТ 28147-89 следующим образом. Ему равны первые 56 координат (k1, …, k56) ключа k, следующие d координат (k57, …, k(56+d)) выбираются на передающем конце случайно, остальные – нулевые. Далее вектор k используется как в стандартном алгоритме ГОСТ 28147-89 (См., например, [4]).

На приемном конце для расшифрования придется перебрать 2^d бит вектора (k57, …, k(56+d)) и определить те, которые были использованы отправителем методом отбраковки, например, по критерию на открытый текст. Последние биты – нулевые. Процесс использования ключей считается известным злоумышленнику, и он знает о нулевых битах и строении вектора k. Но при атаке методом полного перебора ключей ему придется определить (56+d) бит, то есть выполнить работу порядка 2^(56+d) операций, в то время как законный участник протокола выполнит работу порядка 2^d операций. Определим параметр d.

Будем исходить, например, из данных статьи [8], где приведены данные по перебору ключей разной длины с использованием персонального компьютера, с использованием технологии FPGA и технологии ASIC. Исходя из оценки в 10^3 операций на опробование одного ключа, получим следующие скорости опробования:

PC: 1,6 * 10^9 опер/ сек.; FPGA: 5,5 * 10^10 опер/ сек.; ASIC: 2,7 * 10^14 опер/ сек.

Отсюда, например, при 1 минуте на расшифрование законным участником, параметр d будет равен 20 битам для расшифрования/дешифрования на PC. Соответственно злоумышленнику придется опробовать 2^76 ключей. (Предполагаем, что именно этот способ дешифрования возможен для злоумышленника для данного симметричного алгоритма).

Рекомендация 2. Сделать параметр d переменным

В зависимости от степени секретности открытого текста можно выбирать и параметр d, увеличивая время по расшифрованию законным получателем, но увеличивая время дешифрования нарушителем. Для рассматриваемого примера и даже при d<20 получим увеличение времени опробования порядка в 2^3 раза.

Рекомендация 3. Выполнять предварительное преобразование открытого текста

Впервые в работе Райвеста [3], а также в работах Бойко[5] и Стинсона [7] были предложены реализации так называемого преобразования AONT (All-Or-Nothing Transform). AONT не является преобразованием шифрования. В качестве AONT рассматривались также известное преобразование OAEP (Optimal Asymmetric Encryption Padding) [2] и другие.

AONT является взаимно-однозначным преобразованием блоков открытого текста в блоки псевдотекста. При этом прямое и обратное AONT являются полиномиальными, то есть эффективно вычисляемыми. Главное свойство этого преобразования в том, что без знания всех блоков псевдотекста нельзя эффективно (в полиномиальное время) восстановить исходный открытый текст. Далее псевдотекст шифруется одним из режимов симметричного шифрования. Трудоемкость зашифрования может несколько увеличиться в зависимости от реализации AONT. Например, в реализации Райвеста трудоемкость увеличивается в 3 раза по сравнению с обычным режимом шифрования. Но в методе полного опробования ключей приходится сначала восстанавливать все блоки псевдотекста, чтобы восстановить открытый текст и только после этого применять критерий на открытый текст. Чем длиннее открытый текст, тем длиннее псевдотекст и тем больше трудоемкость опробования каждого ключа.

Рекомендация 4. Выбирать режим шифрования

Размер блоков открытого текста в ГОСТ 28147-89 равен 64 битам, что приводит к общему увеличению длины открытого текста при желании увеличить число блоков открытого текста и псевдотекста. Раньше до появления новых ГОСТов режимы работы ГОСТ 28147-89 не позволяли сократить этот множитель. Существует ГОСТ Р ИСО/МЭК 10116-93, в котором есть режим с обратной связью по выходу (OFB – Output Feedback), позволяющий шифровать блоками длины от 1 до 64 бит. Но этот ГОСТ на практике редко реализовывался, так как в нем не был определен базовый блочный алгоритм шифрования. В настоящее время

приняты новые российские стандарты шифрования, в частности ГОСТ Р 34.13 -2015 (Режимы работы блочных шифров). Одним из режимов является «Режим гаммирования с обратной связью по шифртексту», позволяющий шифровать блоками длины от 1 до 64 бит. Сравнивая режимы шифрования при фиксированной длине открытого текста при использовании AONT, например, из работы [3], можно сделать вывод, что наиболее стойким будет указанный выше режим при длине блоков текста в один бит, ввиду необходимости применять базовый блочный алгоритм на каждый бит текста, а не на группу бит. Уменьшение размера блока открытого текста увеличивает время зашифрования, но увеличивает и стойкость.

Таким образом, использование AONT может давать увеличение трудоемкости метода полного опробования ключей в t раз, где t длина открытого текста. Например, при зашифровании статьи из трудов конференции CRYPTO среднего размера это дает увеличение трудоемкости в 2^21 раз, то есть увеличивает эффективный размер ключа еще на 21 бит. В рассмотренных выше примерах трудоемкость метода полного опробования увеличивается с порядка 2^56 до порядка 2^97 операций.

Рецензент: Велигура Александр Николаевич, кандидат физико-математических наук, доцент, vg_2000@mail.ru

Литература:

1. Mercle R. C. Secure Communications Over Insecure Channels, Comm. of the ACM, 1978, v.21, N 4, pp. 294-299.
2. Bellare M., Rogaway P. Optimal Asymmetric Encryption - How to encrypt with RSA. Eurocrypt '94, LNCS, 950, 1995.
3. Rivest R. All-Or-Nothing Encryption and the Package Transformation, 1997, Fast Software Encryption, LNCS, 267, pp. 210–218.
4. Варфоломеев А.А., Жуков А.Е., Мельников А.Б., Устюжанин Д.Д. Блочные криптосистемы. Основные свойства и методы анализа стойкости. М.: МИФИ, 1998. 198 с.
5. Boyko V. On the Security Properties of OAEP as an All-or-nothing Transform. 1999, CRYPTO 99, LNCS, 1666, pp. 503–518.
6. Canetti R., Dodis Y., Halevi S., Kushilevitz E., Sahai A. Exposure-Resilient Functions and All-or-nothing Transforms, Eurocrypt`2000, pp.453-469.
7. Stinson, D. R. Something About All or Nothing (Transforms). Designs, Codes and Cryptography, 2001, 22 (2), pp. 133–138.
8. Лукацкий А., Атаки на VPN // КомпьютерПресс. 2002. № 3. С.56-59.
9. Чмора А.Л. Современная прикладная криптография. М.: Гелиос АРВ, 2002. 256 с.
10. Resch J., Plank J. AONT-RS: Blending Security and Performance in Dispersed Storage Systems. Usenix FAST'11. URL: https://www.usenix.org/legacy/event/fast11/tech/full_papers/Resch.pdf.
11. Ключарев П. Г., Жуков Д. А. Введение в теорию алгоритмов: учеб. пособие. М.: Изд-во МГТУ им. Н. Э. Баумана, 2012. 37 с.

SOME RECOMMENDATIONS FOR IMPROVING SECURITY OF THE CIPHER WITH SMALL KEYAGAINST BRUTE FORCE ATTACK

***Varfolomeev A.A.*[2]**

The paper contains recommendations for improving the resistance of a symmetric cipher to brute force attack, provided that the key size is less than 56 bits. This condition corresponds to the regulatory requirements for unlicensed use of cryptographic protection means of information. These guidelines significantly increase the complexity of the plaintext recovery by this method for attacker. The effectiveness of the recommendations is demonstrated by examples with different computing power of an attacker and legitimate users.

***Keywords**: cryptography, all–or–nothing transform, asymmetry, standards GOST 28147–89, GOST R 34.13:2015, plain text, encryption*

References:

1. Mercle R. C. Secure Communications Over Insecure Channels, Comm. of the ACM, 1978, v.21, N 4, pp. 294-299.
2. Bellare M., Rogaway P. Optimal Asymmetric Encryption - How to encrypt with RSA. Eurocrypt '94, LNCS, 950, 1995.
3. Rivest R. All-Or-Nothing Encryption and the Package Transformation, 1997, Fast Software Encryption, LNCS, 267, pp. 210–218.
4. Varfolomeev A.A., Zhukov A.E., Mel'nikov A.B., Ustyuzhanin D.D. Blochnye kriptosistemy. Osnovnye svoystva i metody analiza stoykosti. M.: MIFI, 1998. 198 p.
5. Boyko V. On the Security Properties of OAEP as an All-or-nothing Transform. 1999, CRYPTO 99, LNCS, 1666, pp. 503–518.
6. Canetti R., Dodis Y., Halevi S., Kushilevitz E., Sahai A. Exposure-Resilient Functions and All-or-nothing Transforms, Eurocrypt`2000, pp. 453-469.
7. Stinson, D. R. Something About All or Nothing (Transforms). Designs, Codes and Cryptography, 2001, 22 (2), pp 133–138.
8. Lukatskiy A., Ataki na VPN, Komp'yuterPress. 2002. No 3, pp.56-59.
9. Chmora A.L. Sovremennaya prikladnaya kriptografiya. M.: Gelios ARV, 2002. 256 p.
10. Resch J., Plank J. AONT-RS: Blending Security and Performance in Dispersed Storage Systems. Usenix FAST'11. URL: https://www.usenix.org/legacy/event/fast11/tech/full_papers/Resch.pdf.
11. Klyucharev P. G., Zhukov D. A. Vvedenie v teoriyu algoritmov: ucheb. posobie. M.: Izd-vo MGTU im. N. E. Baumana, 2012. 37 p.

2 Aleksandr Varfolomeev, Ph.D. (in Math.), Associate Professor, BMSTU, Moscow, a.varfolomeev@mail.ru