О НЕКОТОРЫХ ПРЕДВАРИТЕЛЬНЫХ ПРЕОБРАЗОВАНИЯХ ОТКРЫТОГО ТЕКСТА ТИПА «ALL-OR-NOTHING» ДЛЯ УСИЛЕНИЯ СТОЙКОСТИ ШИФРА К МЕТОДУ ПОЛНОГО ОПРОБОВАНИЯ

Варфоломеев А.А.

кандидат физико-математических наук, доцент, Московский государственный технический университет имени Н.Э. Баумана,

г. Москва, Российская Федерация, a.varfolomeev@mail.ru

Аннотация. **В работе содержатся некоторые 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.**

Рекомендации, предлагаемые в работе, учитывают различные определения понятия «ключ», в том числе из известного российского словаря криптографических терминов.

Данные рекомендации существенно повышают сложность восстановления злоумышленником открытого текста указанным методом.

Ключевые слова: криптография, регулирование, AON преобразование, асимметрия, стандарты, ГОСТ 28147-89, ГОСТ Р 34.13 -2015.

I. Введение

В работе автора [11] приведен ряд рекомендаций по повышению стойкости шифра с малым размером ключа к методу полного опробования. Данная работы преследует ту же цель, но при других условиях.

Использование малого 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, …». Положение не распространяется на «симметричный криптографический алгоритм, использующий криптографический ключ длиной, не превышающей 56 бит», и получение лицензии на применение такого алгоритма не требуется. Он может быть применен не только «для обеспечения собственных нужд юридического лица или индивидуального предпринимателя».

При выработке рекомендаций исходили из следующих предположений:

1. Используется стандартный шифр, например, ГОСТ 28147-89 или ГОСТ Р 34.12-2015 в одном из режимов по ГОСТ Р 34.13 -2015, без внесения каких - либо изменений в их работу.

2. В качестве определения ключа используется определение из ряда международных стандартов. Например, согласно стандарту ИСО/МЭК 18033-1 и другим, «ключ(key) – изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование».

В данной трактовке понятия «ключ» не сказано, как определяется криптографическое преобразование: однозначно или нет. Именно возможность неоднозначного определения ключа, а определения в некотором количестве вариантов, использовалось в рекомендациях 1 и 2 из [11]. Именно вносилась асимметрия в объем работы законных пользователей при зашифровании открытого текста и расшифровании.

Но известный российский «Словарь криптографических терминов» [8] содержит другое определение:

«Ключ (криптосистемы) [key (ofacryptosystem)] — изменяемый элемент (параметр), каждому значению которого однозначно соответствует одно из отображений, реализуемых криптосистемой. Все возможные значения ключа составляют множество ключевое криптосистемы. Ключи могут быть составными, т. е. содержать несколько частей, обеспечивающих различные функции криптосистемы. Например, при реализации алгоритма шифрования электронной схемой в качестве ключей могут использоваться начальные состояния элементов памяти схемы, функциональные узлы и др.»

Как видно эта трактовка понятия «ключ» предполагает «однозначное» определение криптографического отображения (преобразования), реализуемого криптосистемой.Часть рекомендацийиз [11] (3 и 4)остаются в силе и при такой трактовке понятия «ключ».Но возникает вопрос о возможности использования асимметрии в процессах зашифрования и расшифрования, внося многозначность в предварительное преобразование открытого текста типа «All-Or-Nothing» [2-9]. Но для этого необходимо изменить определение этого преобразования, которое в классическом определении из работы [3] является взаимно однозначным..

При этом предполагается, что рекомендации не должны быть связаны с изменением применяемых алгоритмов шифрования, в том числе и стандартизированных.

II. Определение преобразования «All-OrNoting» и его изменение

Впервые определение преобразования AONT (All-Or-NothingTransform) появилось в работе Райвеста [3]. Далее в работах Бойко[5] и Стинсона [7] и в других работах были предложены различные реализации этого преобразования. AONT не является преобразованием шифрования. В качестве AONT рассматривались также известное преобразование OAEP (OptimalAsymmetricEncryptionPadding) [2] и другие. Но для наглядности рекомендаций рассмотрим первоначальное определение AONT.

Преобразование f, отображающее последовательность знаков (блоков) открытого текста m_1, …, m_s в последовательность знаков (блоков) псевдотекстаm`_1, …, m`_s`, называется AON преобразованием (AONT - All-Or-NothingTransform), если

- преобразование f обратимо;

- преобразование f и его обратное преобразование f^(-1) эффективно вычисляемы, то есть имеют полиномиальную сложность;

- вычислительно невозможно найти какие-нибудьзнаки (блоки) открытого текста, если не известны все знаки (блоки) псевдотекста.

В работе [3] предлагалось далее псевдотекст шифровать одним из режимов симметричного (блочного) шифрования. Также там отмечалось, что AONT должно быть псевдослучайным, чтобы атака с выбранным или известным открытым текстом не давала бы псевдотекст для его использования в методе опробования, вместо открытого текста.

В качестве примера описанного преобразования предлагалась следующая конструкция, которую мы рассмотрим в качестве примера. Для внесения случайности преобразования использовался случайный вектор K` (назывался ключом) достаточно большого размера, который вычислительно невозможно опробовать. Первые sзначений псевдотекста получались по правилу:

m`_i= m_iXORE1(K`,i) дляi=1,…,s. (2.1)

Здесь E1(K`,i) – преобразование E1зашифрования текста i на ключе K`.

Значение m`_(s+1) определяется по правилу

m`_(s+1) = K`XOR h_1 XOR h_2 … XOR h_s, (2.2)

гдеh_i = E2(K_0, m`_i XOR i) дляi= 1, …,s, (2.3)

а K_0 – известный всем двоичный вектор, играющий роль ключа в преобразовании E2зашифрования текста m_iXORi. Все числа здесь представляются двоичными векторами соответствующих размеров.Операция XOR – побитовое сложение двоичных векторов по модулю 2.

В оригинальной статье [3] рассматривается случай, когда E1 = E2 = E, хотя допускается различие этих преобразований.

Легко видеть, что описанное преобразование открытого текста соответствует всем требованиям определения AONT.

Использование известного старого российского стандарта шифрования ГОСТ 28147-89 в этой конструкции дает некоторые ограничения, в отличие от использования новых ГОСТ Р 34.12-2015 (блочные шифры) и ГОСТ Р 34.13-2015 (режимы блочных шифров). Например, размер векторов h_i, a, следовательно, и размер вектора K` ограничивался бы 64 битами при однократном применении базового блочного алгоритма, как величиной блоков открытого и шифрованного текстов в ГОСТ 28147-89. В отличие от этого в новых ГОСТах эта величина равна 128 битам (64 тоже допускается).

Размер вектора K` можно увеличить еще больше, если использовать в (2.3) вместо преобразования шифрования вычисление хеш-функции. В качестве хеш-функции можно выбрать российский стандарт ГОСТ Р 34.11-2012, размер хэш-кода в котором может быть равен 256 или 512 битам. Вычисление хеш-функции быстрее чем применение базового блочного шифра (см. п. 2.1.3 в ГОСТ Р 34.12-2015), что приводит к уменьшению времени работы как законных пользователей, так и злоумышленника. Это можно компенсировать многократным применением хеш-функции.

Предложимнекоторые варианты изменения всего процесса шифрования открытого текста. Эти варианты будут касаться только приведенного здесь AONTиз работы [3]. В случае применения упомянутых OAEPиз [2] или других предварительных преобразований открытого текста, вопрос должен рассматриваться отдельно.

Вариант 1. Выбирать при AONTв векторе K_0 часть координат случайно, при их опробовании законным пользователем при расшифровании.

Например, если t координат вектора K_0 выбирать в AONTслучайно, а остальные координаты считать открытыми (известными для всех), то трудоемкость перебора законного пользователяпри расшифровании и злоумышленника при опробовании неизвестных случайных координат возрастет в 2^(t + s) раз. Для каждого варианта из опробуемых t бит ключа K_0 необходимо найти s векторов h_i = E2(K_0, m`_iXORi) для i= 1, …,s , чтобы восстановить K` = m`_(s+1) XORh_1 XORh_2 … XORh_s (естественно при каждом опробуемом варианте ключа шифрования по ГОСТ). Так как длина soткрытого текста должна быть достаточно большой, чтобы обеспечить преимущества применения AONT, то это может привести к неконтролируемому увеличению трудоемкости для законного пользователя, а не только для злоумышленника.

Вариант 2. Не шифровать и не передавать часть координат значения вектора m`_(s+1), при их опробовании законным пользователем при расшифровании.

В этом случае, например, если t координат вектора m`_(s+1) ( илиt бит соответствующего шифрованного текста) не известны ни законному пользователю ни злоумышленнику, то их придется им опробовать в 2^t вариантах, чтобы восстановить ключ K` из формул (2.3) и (2.2) и с его помощью найти весь открытый текст из соотношений

m_i = m`_iXORE1(K`,i) для i=1,…,s.

Числовые преимущества использования приведенных рекомендаций остались такими же, как и работе [11]. В рассмотренных в [11] примерах трудоемкость метода полного опробования ключей увеличивается с порядка 2^56 (при 56 битовом ключе шифрования) до порядка 2^97 операций.

III. Заключение

Вариант 1 ведет к частичному изменению определения AON преобразования, так как нахождение открытого текста по псевдотекстув этом варианте не является полиномиальным. Вариант 2 может быть использован с любым AON преобразованием.

Отказавшись от рекомендаций 1 и 2 из [11] в силу другого определения понятия ключа, достигли тех же целей усиления стойкости. Рекомендация 4 из [11] по выбору режима шифрования осталась той же, рекомендация 3 по AON преобразованию возможна в вариантах.

Численные значения увеличения стойкости шифрования при предложенных здесь рекомендациях остались теми же, что и в работе [11], но при этом используемое понятие «ключ» полностью соответствует определению из российского словаря криптографических терминов.

Список литературы

1. Mercle R. C., Secure Communications Over Insecure Channels, Comm. of the ACM, 1978, v.21, № 4, 294-299c.
2. Bellare M., Rogaway P. Optimal Asymmetric Encryption -- How to encrypt with RSA. - Eurocrypt '94, LNCS V. 950, Springer-Verlag, 1995.
3. Rivest R., All-Or-Nothing Encryption and the Package Transformation, 1997, Fast Software Encryption, LNCS № 1267: 210–218c.
5. Boyko V. On the Security Properties of OAEP as an All-or-nothing Transform. 1999, CRYPTO 99, LNCS № 1666, 503–518c.
6. Canetti R., Dodis Y., Halevi S., Kushilevitz E., Sahai A., Exposure-Resilient Functions and All-or-nothing Transforms, Eurocrypt`2000, 453-469c.
7. Stinson, D. R. Something About All or Nothing (Transforms). Designs, CodesandCryptography, 2001, 22 (2): 133–138.
8. Словарь криптографических терминов. / Под ред. Б. А. Погорелова и В. Н. Сачкова. - М.: МЦНМО, 2006. - 94 с.
9. Глухов М.М. О применениях квазигрупп в криптографии. Прикладная дискретная математика. № 2(2), 2008, 28-32.
10. Ключарев П. Г., Жуков Д. А. Введение в теорию алгоритмов: учеб. пособие. - М.: Изд-во МГТУ им. Н. Э. Баумана, 2012.
11. Варфоломеев А.А. Некоторые рекомендации по повышению стойкости шифра с малым размером ключа к методу полного опробования. – Вопросы кибербезопасности № 5(13) – 2015, 60-62.
12. D`Arco P., Esfahani N., Stinson D. All or Nothing at All. IACR ePrint Archive 2015/998, 23c.