УДК 681.324.067

ПРОСТОЙ СПОСОБ РАЗРАБОТКИ «ЛЕГКИХ» АЛГОРИТМОВ ШИФРОВАНИЯ

А.С. ПОЛЯКОВ

Объединенный институт проблем информатики Национальной Академии Наук Беларуси, Республика Беларусь

Поступила в редакцию 21 декабря 2016

Аннотация. Предложен подход к разработке «легких» алгоритмов шифрования, предусматривающий использование секретных алгоритмов шифрования и передаваемого сообщения в качестве ключа шифрования. Предлагается модель построения простых в реализации и быстродействующих алгоритмов.

Ключевые слова: сообщение, защита информации, ключ шифрования.

Abstract. An approach to the development of «lightweight» cipher algorithms is considered. The confidential cipher algorithms and message as the cipher key is proposed. The model for design of simple and high-speed encryption algorithms is suggested.

Keywords: message, data protection, cipher key.

Doklady BGUIR. 2017, Vol. 104, No. 2, pp. 11-16
The simple approach to the development of lightweight cipher algorithms
A.S. Poljakov

Введение

Последнее десятилетие характеризуется быстрым развитием «повсеместной» компьютеризации до уровня «всепроникающих» устройств во всех сферах применения информационых технологий, включая «Интернет-вещи» (Internet of Things), технологию радиочастотной идентификации (RFID-метки) и вычислительных сетей физических объектов, оснащенных встроенными технологиями для взаимодействия друг с другом и внешней средой («умный дом»).

Для обеспечения защиты информации в указанных выше сферах использования информационных технологий необходимы простые в реализации, быстродействующие алгоритмы шифрования. Исследования в этом направлении ведутся в области «легковесной криптографии» (LWC – lightweight cryptography), имеющей целью создание легких и быстрых алгоритмов шифрования. В 2007 году коллектив авторов [1] предложил «ultra-lightweight» алгоритм шифрования Present, представляя его как алгоритм, требующий небольших затрат на аппаратную реализацию и обеспечивающий высокую производительность. В 2009 году А. Пошманн [2] привел математическую аргументацию и обоснование необходимости развития направления «lightweight cryptography» (переведенное как "облегченная" или "легковесная" криптография).

Появилось много публикаций о разработке криптоалгоритмов, представляемых как «lightweight algorithms» [3–6], в том числе алгоритмы Present и Clefia международного стандарта ISO/IEC 29192-2:2012 [7]. Но характеристики этих алгоритмов оказались либо незначительно лучше (Present), либо хуже (Clefia) характеристик известных стандартных алгоритмов [8].

В связи с повсеместным развитием компьютеризации всех аспектов жизнедеятельности общества и внедрением компьютерных технологий в самые низкоуровневые сферы социальной жизни (ubiquitous computing – ubicomp), необходимы «легкие» алгоритмы шифрования, к которым относятся алгоритмы, разрабатываемые специально для устройств с ограниченными или крайне малыми ресурсами.

Общим свойством таких алгоритмов являются требования к площади кристалла, на котором алгоритм может быть реализован; вычислительной мощности процессора, на котором выполняются вычисления; к оперативной памяти устройства и т.п. Алгоритмы должны быть легкими с точки зрения реализации (программной или аппаратной) и высокопроизводительными для обеспечения обработки информации в реальном масштабе времени. Существенным является и тот факт, что во многих случаях не требуется защита информации на продолжительное время. В данной работе рассматривается именно такая трактовка понятия «легкие» алгоритмы шифрования.

Описание подхода

В указанных выше областях «повсеместной» компьютеризации возможность использования обновляемого секретного ключа затруднительна. Поэтому нужны алгоритмы, в которых ключ содержится в самом алгоритме. Отсюда следует, что алгоритмы шифрования должны быть секретными. Для разработки "легких" алгоритмов шифрования представляется целесообразным использовать подход, основанный на следующих принципах:

1) алгоритмы шифрования являются секретными;

2) отсутствуют передаваемые секретные ключи шифрования.

Один из возможных вариантов такого подхода основан на применении идеи Г. Вернама и предложения К. Шеннона о возможности использования элементов передаваемого сообщения в качестве ключа шифрования. В 1926 г. Г. Вернам [9] предложил одноразовую систему шифрования, основанную на следующих принципах:

– длина ключа шифрования равна длине передаваемого сообщения;

– шифрование производится с помощью ключа, каждый элемент которого сформирован случайным образом («одноразовой ленты» – по определению Х. Файстеля [10]);

– ключ используется только один раз для передачи только одного сообщения.

Шеннон показал, что одноразовые системы обеспечивают совершенную секретность и являются абсолютно нераскрываемыми, поскольку их шифртекст не содержит достаточной информации для восстановления открытого текста. Недостатком такой системы является необходимость подготовки специальной случайной последовательности (ключа шифрования) и доставки этого ключа Адресату абсолютно защищенным способом.

Преимущества системы Вернама можно использовать, если в качестве ключа шифрования применять текст передаваемого сообщения. Такой вариант рассматривался К. Шенноном [11], который предложил специальное название для абсолютно защищенных шифров, в которых «само передаваемое сообщение используется в качестве ключа», назвав их шифрами «с автоключом». В таких шифрах шифрование начинается с помощью некоторого первичного ключа и продолжается с использованием элементов сообщения.

Недостаток этого способа в том, что текст сообщения на лингвистическом языке, используемый в качестве ключа шифрования, не в полной мере удовлетворяет требованиям случайной «одноразовой ленты» в связи с наличием известных статистических характеристик текста. В теории связи считается [11], что язык может рассматриваться как некоторый вероятностный процесс, который создает дискретную последовательность символов в соответствии с некоторой системой вероятностей, т.е. последовательность символов языка может рассматриваться как случайная последовательность, имеющая некоторые известные статистические характеристики. Но статистические характеристики сообщения можно изменить с помощью приема, применяемого в известных криптоалгоритмах, в которых для решения этой задачи выполняется многократное преобразование элементов сообщения с использованием секретного ключа и различных операций, основные из которых представлена в таблице.

Основные операции, используемые в известных криптоалгоритмах [12–15]

Алгоритм	Наименование операции				
	Сложение по mod 2	Сложение по mod 2^{32}	Умножение по mod 2^{32}	Подста-новка	Циклический сдвиг
AES (Rijndael)	+	–	–	+	+
MARS	+	+	+	+	+
RC6	+	+	+	–	+
Twofisch	+	–	–	+	+
Serpent	+	–	–	+	+
ГОСТ 28147-89	+	+	–	+	+
СТБ 34.101.31-2010	+	–	–	+	+

С учетом вышеизложенного алгоритм шифрования сообщения $S = \{s_1, s_2, \ldots, s_n\}$ можно представить следующим образом.

Создается множество первичных ключей шифрования $K = \{k_1, k_2, \ldots, k_m\}$, выбирается множество операций $O = \{o_1, o_2, \ldots, o_r\}$ и множество $\underline{O} = \{\underline{o}_1, \underline{o}_2, \ldots, \underline{o}_r\}$ инверсных к ним операций.

Задается множество $P = \{p_1, p_2, \ldots, p_t\}$ правил вычисления случайных величин по значениям первичного ключа и элементов передаваемого сообщения, которые используются в качестве входных данных для операций алгоритма. В качестве примера возможных правил можно представить такое: в заданном векторе (которым может быть первичный ключ шифрования или очередной элемент сообщения) выделяются несколько разрядов, арифметическое значение которых определяет величину другого вектора.

Зашифрование элемента s_1 производится с использованием выбранного из K первичного ключа и элемента s_1, по значениям которых с помощью правил из множества P вычисляются входные данные для выбранной из множества O последовательности операций. Результат выполнения описанных действий представляет собой зашифрованное значение $\underline{s}_1$ первого элемента сообщения S.

Зашифрование второго и последующих элементов сообщения производится аналогично, только в качестве первичного ключа используется значение предыдущего элемента сообщения S. При зашифровании элементов s_i , $2 \le i \le (n-1)$ последней является операция, использующая результат зашифрования элемента s_{i-1} (т.е. $\underline{s}_{i-1}$). В результате применения описанной процедуры ко всем элементам сообщения S вычисляется зашифрованное сообщение $\underline{S} = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_n\}$.

Алгоритм шифрования на основе предлагаемого подхода может быть представлен как функция от перечисленных выше параметров в виде: $\underline{S} = F(K, O, \underline{O}, P, S, \underline{S}')$, где $\underline{S}' = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_{n-1}\}$

Реализация этой функции определяет конкретный алгоритм шифрования с выбранными значениями:

1) первичного ключа шифрования из множества K;

2) набора операций из O и $\underline{O}$;

3) правил вычисления входных данных для операций, выбранных из множества P;

4) последовательности выполнения операций.

Конкретная реализация алгоритма зашифрования описывается уравнением

$$\underline{s}_i = F(s_{i-1}, o_1, \ldots, o_j, p_1, \ldots, p_j, s_i, \underline{s}_{i-1}).$$

Схема алгоритма зашифрования представлена на рис. 1 для случая, когда при шифровании используются четыре операции $o_1 \div o_4$.

При расшифровании сообщения имеются некоторые особенности:

а) операции выполняются в обратном порядке;

б) применяются операции, инверсные использованным при зашифровании, поэтому модель алгоритма расшифрования выглядит следующим образом: $S = \underline{F}(K, \underline{O}, P, \underline{S})$.

Расшифрование полученного сообщения $\underline{S}$ начинается с элемента $\underline{s}_1$, при этом используется первичный ключ, по значению которого вычисляются входные данные для операций алгоритма при расшифровании элемента $\underline{s}_1$. В результате выполнения алгоритма расшифрования вычисляется исходное значение элемента s_1. Для вычисления элемента s_2 в качестве первичного ключа используется вычисленное значение s_1. Аналогично производится расшифрование остальных элементов $\underline{S}$: $s_i = F(s_{i-1}, \underline{o}_1, \ldots, \underline{o}_j, p_1, \ldots, p_j, \underline{s}_{i-1}, \underline{s}_i)$.

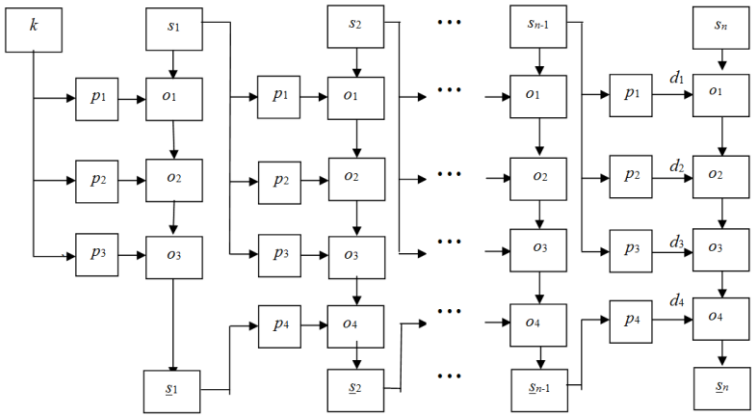

Рис. 1. Схема выполнения алгоритма зашифрования

Графическое представление алгоритма расшифрования приведено на рис. 2. Заметим, что значения входных данных для операций, выполняемых на последнем этапе зашифрования (т.е. d_1, d_2, d_3, d_4), можно использовать в качестве имитовставки для определения целостности сообщения. Совпадение этих значений с аналогичными значениями ($\underline{d}_1$, $\underline{d}_2$, $\underline{d}_3$, $\underline{d}_4$), вычисленными при расшифровании, свидетельствует об отсутствии искажений в сообщении, т.е. о его целостности.

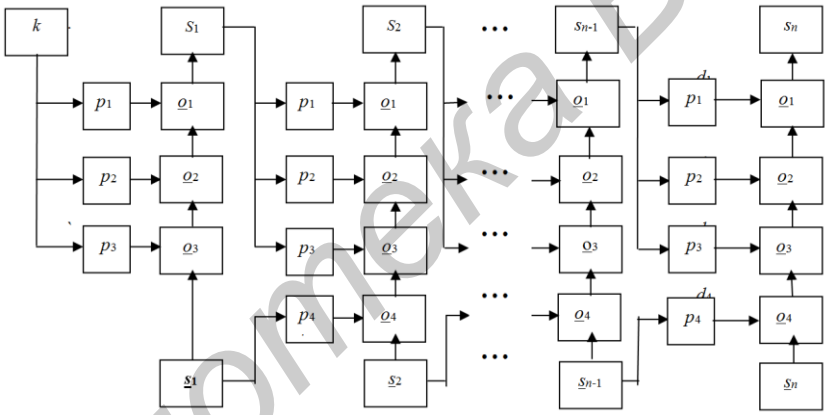

Рис. 2. Схема выполнения алгоритма расшифрования

Заключение

Алгоритмы на основе предложенного подхода очень простые и легко реализуемые как программно, так и аппаратно, что обеспечивает возможность пользователю разработать серию алгоритмов с различными множествами первичных ключей, операций, правил вычисления входных данных для операций и их последовательностью.

Поскольку при шифровании каждого нового сообщения выбирается новый начальный ключ, а в качестве секретного ключа используется новая последовательность символов (т.е. текст передаваемого сообщения), то это означает, что каждое сообщение зашифровывается с помощью нового алгоритма, отличающегося от всех предыдущих. Этот факт позволяет предполагать, что такие алгоритмы будут иметь значительную криптостойкость и смогут обеспечивать защиту информации в течение достаточно длительного промежутка времени.

В связи с простотой и небольшим количеством выполняемых операций, алгоритмы обладают высокой производительностью. Кроме того, они обеспечивают реализацию функции контроля целостности зашифрованной информации, предусматриваемой в стандартных криптоалгоритмах.

Список литературы

1. Present: An ultra-lightweight Block Cipher / A. Bogdanov et. al. // Proceedings of CHES/ 2007. № 4727. LNCS, Springer-Verlag. P. 450-466.
2. Poschmann A. Lightweight Cryptography – Cryptographic Engineering for a Pervasive World // Dissertation for the degree Doktor-Ingenieur Faculty of Electrical Engineering and Information Technology. Germany, Ruhr-University Bochum, 2009. 179 p.
3. Masanobu Katagi and Shibo Moriai. Lightweight Cryptography for the Internet of Things. [Electronic data]. – Access mode: www.iab.org/wp-content/IAB-uploads/2011/030 Kaftan.pdf. – Date of access: 20.09.2016.
4. Панасенко С., Смагин С. Облеченные алгоритмы шифрования // Мир ПК. 2011. № 7. С. 50–52.
5. Агафьин С.С. LW-криптография: шифры для RFID-систем. [Электронный ресурс]. – Режима доступа: http://bit.mephi.ru/wp-content/uploads/bit_1_2011_6.pdf. – Дата доступа: 30.10.2016.
6. Masanobu Katagi and Shiho Moriai. Lightweight Cryptography for the Internet of Things. [Electronic data]. – Access mode: www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf. – Date of access: 22.11.2016.
7. ISO/IEC 29192-2:2012. Information technology – Security techniques – Lightweight Cryptography – Part 2: Block ciphers.
8. Поляков А.С., Самсонов В.Е. Анализ возможных алгоритмов международного стандарта «Облегченная криптография» ISO / IEC 29192-2: 2012 // Информатика. 2014. № 3. С. 107–112.
9. Vernam G.S. Cipher printing telegraph systems for secret wire and radio telegraphic communication // J. Inst. Electric. Eng. 1926. Vol. 45. P. 109–115.
10. Feistel H. Cryptography and Computer Privacy // Scientific American. 1973. Vol. 228, № 5. P. 15–23.
11. Shannon C.E. Communication theory of secrecy systems // Bell System Techn. J. 1949. Vol. 28, № 4. P. 656–715.
12. Announcing the Advanced Encryption Standard (AES) / Federal Information Processing Standards Publication 197. – November, 26, 2001. [Electronic resource]. – Mode of access: http://csrc.nist.gov/archive/aes/index.html. – Date of access: 20.09.2016.
13. Gajand K., Chodowiec P. Hardware Performance of the AES Finalists – Survey and Analysis of Results // George Mason University, 2001. 54 p.
14. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
15. СТБ 34.101.31-2011. Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля злокачественности.

References

1. Present: An ultra-lightweight Block Cipher / A. Bogdanov et. al. // Proceedings of CHES/ 2007. № 4727. LNCS, Springer-Verlag. P. 450-466.
2. Poschmann A. Lightweight Cryptography – Cryptographic Engineering for a Pervasive World // Dissertation for the degree Doktor-Ingenieur Faculty of Electrical Engineering and Information Technology. Germany, Ruhr-University Bochum, 2009. 179 p.
3. Masanobu Katagi and Shibo Moriai. Lightweight Cryptography for the Internet of Things. [Electronic data]. – Access mode: www.iab.org/wp-content/IAB-uploads/2011/030 Kaftan.pdf. – Date of access: 20.09.2016.
4. Panasenko S., Smagin S. Oblegchennye algoritmy shifrovaniya // Mir PK. 2011. № 7. S. 50–52. (in Russ.)
5. Agaf'in S.S. LW-kriptografiya: shifry dlya RFID-sistem / S.S. [EHlektronnyj resurs]. – Rezhim dostupa: http://bit.mephi.ru/wp-content/uploads/bit_1_2011_6.pdf. – Data dostupa: 30.10.2016. (in Russ.)
6. Masanobu Katagi and Shiho Moriai. Lightweight Cryptography for the Internet of Things. [Electronic data]. – Access mode: www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf. – Date of access: 22.11.2016.
7. ISO/IEC 29192-2:2012. Information technology – Security techniques – Lightweight Cryptography – Part 2: Block ciphers.
8. Polyakov A.S., Samsonov V.E. Analiz vozmozhnostej algoritmov mezhdunarodnogo standarta «Lightweight Cryptography» ISO/IEC 29192-2:2012 // Informatika. 2014. № 3. S. 107–112. (in Russ.)
9. Vernam G.S. Cipher printing telegraph systems for secret wire and radio telegraphic communication // J. Inst. Electric. Eng. 1926. Vol. 45. P. 109–115.
10. Feistel H. Cryptography and Computer Privacy // Scientific American. 1973. Vol. 228, № 5. P. 15–23.
11. Shannon C.E. Communication theory of secrecy systems // Bell System Techn. J. 1949. Vol. 28, № 4. P. 656–715.

12. Announcing the Advanced Encryption Standard (AES) / Federal Information Processing Standards Publication 197. – November, 26, 2001. [Electronic resource]. – Mode of access: http://csrc.nist.gov/archive/aes/index.html. – Date of access: 20.09.2016.
13. Gajand K., Chodowiec P. Hardware Performance of the AES Finalists – Survey and Analysis of Results // George Mason University, 2001. 54 p.
14. GOST 28147-89. Sistemy obrabotki informacii. Zashchita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya. (in Russ.)
15. STB 34.101.31-2011. Informacionnye tekhnologii. Zashchita informacii. Kriptograficheskie algoritmy shifrovaniya i kontrolya celostnosti. (in Russ.)

Сведения об авторе

Поляков А.С., к.т.н., доцент, ведущий научный сотрудник ОИПИ НАН Беларуси.

Information about the author

Poljakov A.S., Ph.D., associate professor, leading researcher of UIIP NAS Belarus.

Адрес для корреспонденции

220012, Республика Беларусь,
г. Минск, ул. Сурганова, д. 6,
ОИПИ НАН Беларуси
тел. +375-29-632-54-46;
e-mail: alexpolja@tut.by;
Поляков Александр Сергеевич

Address for correspondence

220012, Republic of Belarus,
Minsk, Surganova st., 6,
UIIP NAS Belarus
tel. +375-29-632-54-46;
e-mail: alexpolja@tut.by;
Poljakov Aleksandr Sergeevich