УДК 002.6

О ВОЗМОЖНОСТЯХ ИСПОЛЬЗОВАНИЯ СТАНДАРТА AES В КОРПОРАТИВНЫХ СЕТЯХ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Вердиев С.Г., Нагиева А.Ф.
Азербайджанский технологический университет, Гянджа, Азербайджан
E-mail: info_tel@inbox.ru

Статья посвящена вопросам защиты информации в корпоративных сетях путем шифрования передаваемых данных. Для криптографического шифрования открытых текстов используется алгоритм Rijndael. Процесс шифрования состоит из последовательности итераций, $N^k/32$ осуществляемых над любой из промежуточных структур (блоков) State (состояние). Приведен пример шифрования открытого текста документа, используемого в почтовой связи, и соответствующая ему криптограмма, составленная с применением стандарта Advanced Encryption Standard (AES).

Ключевые слова: защита информации, корпоративные сети, криптография, шифрование данных, открытые тексты, алгоритм Rijndael, стандарт AES, итерационные превращения, процедуры Sub Byte, Shift Rows, Mix Columns и Add Round Key

В современном электронном мире, в условиях непрерывно растущих потоков передаваемых и обмениваемых данных текстов документов, речей и изображений, возникает проблема защиты информации. Готовое к передаче сообщение называется открытым, другими словами, незащищенным текстом. Развитие электронной техники делает их уязвимыми для злоумышленников, они легко могут быть перехвачены. Разработанные методы и средства шифрования данных в большинстве случаев предотвращают несанкционированный доступ к передаваемым данным путем шифрования, в результате чего открытые тексты преобразуется в шифрограмму, или скрытый текст.

В зашифрованном тексте применяются совокупность символов и сами условные знаки для придания недоступности открытому тексту. Известно, что для реализации процесса шифрования используется специальный алгоритм. Действия с подлежащей шифрованию информацией математически описываются в следующем виде:

$$C = E\,k_1(M);\;\; M' = D\,k_2(C),$$

где C (ciphertext) – криптограмма, или зашифрованный текст; M' (message) – открытый текст; E (encryption) – функция шифрования, криптографически преобразующая открытый текст [1]; k_1 – ключ шифрования, являющийся параметром функции E; M – содержание расшифрованного текста; D (decryption) – функция расшифровки, выполняющая преобразование шифрованного текста в открытый; k_2 – ключ, с помощью которого выполняется расшифровка текста.

Среди множества разработанных и используемых для шифрования данных симметричных и асимметричных алгоритмов нами был выбран AES (Advanced Encryption Standard), который как стандарт повсеместно был принят к применению взамен DES (Data Description Standard). Основу его составляет алгоритм Rijndael. При этом используется не сеть Feistel, используемая в DES, а многочлен поля

$$GF(2^8) - m(x) = x^8 + x^4 + x^3 + x + 1,$$

с применением корней которого строится алгоритм в виде расширения поля $GF(2)$.

Необходимо отметить, что биты данных нумеруются начиная с 0 от наименьшего до наибольшего значения. Основной задачей при этом является отображение кодов в виде полинома многочлена. Например, байт вида 10110101 представляется как многочлен вида

$$x^7 + x^5 + x^4 + x^2 + 1.$$

Данный многочлен $m(x)$ был выбран с целью обеспечения эффективности представления элементов поля [2].

В алгоритме Rijndael блок и ключ имеют переменную длину, и их длины, независимо друг от друга, могут быть выбраны равными 128, 192 или 256 битам. Процесс шифрования состоит из последовательности итераций, осуществляемых над любой из промежуточных структур (блоков), называемых State (состояние). Байты State и Key изображаются в виде матриц, число строк в которых равняется четырем, а столбцов $N^b/32$ и $N^k/32$. Здесь $N^b/32$ является длиной блока, а $N^k/32$ – ключа [3].

Входные и выходные значения алгоритма представляются в виде одномерного массива бай-

тов с определенной длиной. Сначала формируются столбцы, затем строки массивов State и Key и лишь затем массивы входа. Процесс шифрования состоит из процедур, исполняющих четыре различные превращения в виде следующих итераций.

1. Sub Byte – процедура подмены байтов.
2. Shift Rows – процедура сдвига строк.
3. Mix Columns – процедура смещения столбцов.
4. Add Round Key – процедура дополнения ключа.

Число итераций в зависимости от длины блока N^r и ключа N^b определяется по таблице 1 [4].

Таблица 1.Таблица определения числа итераций

Параметры	$N^b = 4(128b)$	$N^b = 6(192b)$	$N^b = 8(256b)$
$N^k = 4(128b)$	10	12	14
$N^k = 6(192b)$	12	12	14
$N^k = 8(256b)$	14	14	14

Процедура Sub Byte

В процедуре Sub Byte (Byte substitution – подмена байта) подмена байтов осуществляется с помощью таблицы подмены 1, называемой S-blok и S-box. Эта таблица применяется независимо друг от друга к каждому байту блока State, обеспечивая их нелинейное преобразование [5]:

$$b_{ij} = S(a_{ij});\ i, j = 1; 2; 8 \quad \text{(см. рис. 1).}$$

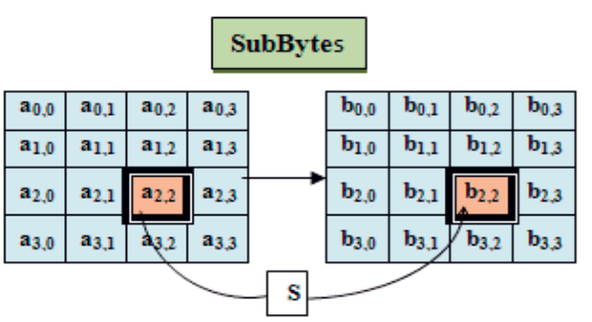


Рис. 1. Процедура Sub Byte

Процедура подмены объединяет в себе две операции. Для каждого байта в поле $GF(2^8)$ результат мультипликативного умножения заменяется своей обратной

$$b_i^{-1} = b_i \bmod m(x).$$

В это время байт 00 самопроизвольно превращается в зашифрованный текст. В нижеприведенной формуле для каждого байта в поле $GF(2)$ осуществляется преобразование affin:

$$b_i = b_i \otimes b_{(i+4)\bmod 8} \otimes b_{(i+5)\bmod 8} \otimes b_{(i+6)\bmod 8} \otimes b_{(i+7)\bmod 8} \otimes c_i,$$

где b_i – i-ый бит от b, а c_i есть i-ый бит, где $c = \{63\} = \{01100011\}$ при $i = \underline{1, 8}$.

Это преобразование можно записать с помощью матрицы как

$$\begin{Vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{Vmatrix} = \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{Vmatrix} * \begin{Vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{Vmatrix} + \begin{Vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{Vmatrix}$$

Рис. 2. Матрица преобразований

Процедура Shift Rows

При этом виде преобразования строки таблицы State по кругу сдвигаются влево на r_i байт: например, нулевая строка на $r = 1b$ и т.д. Таким образом, в сформированной после процедуры Shift Rows таблице выхода State столбцы объединяют в себе по одному байту от столбцов начальной (входной) таблицы State, как это показывает рис. 3.

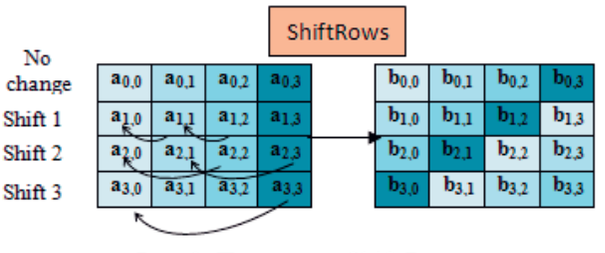


Рис. 3. Процедура Shift Rows

Зависимость значении величины r_i от значений N^b приведена ниже в таблице 2.

Таблица 2. Таблица значений величины r_i

N^b	r_1	r_2	r_3
4	1	2	3
6	1	2	3
8	1	3	4

Как видно из таблицы 2, значения сдвигов одинаковы для строк в 128 и 192 бит, а для строк в 256 бит различны [6].

Процедура Mix Columns

В этой процедуре с помощью линейного сдвига, являющегося обратным процедуре ShiftRow, производится смещение байтов столбцов таблицы State. Для обеспечения этого каждый столбец таблицы смешивается в отдельности (см. рис. 4).

Из столбцов формируется полином четвертой степени, который умножается на многочлен $c(x)=3x^3+x^2+x+2$, определяемый модулем x^4+1, в поле $\mathrm{GF}(2^8)$.

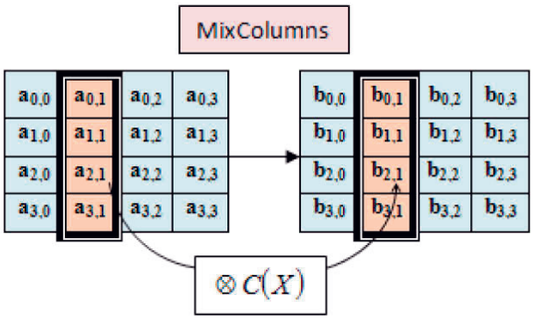


Рис. 4. Процедура Mix Columns

Эту процедуру можно изобразить в виде матрицы

$$\begin{Vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{Vmatrix} = \begin{Vmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 01 \end{Vmatrix} \cdot \begin{Vmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{Vmatrix}$$

Рис. 5. Матрица процедуры Mix Columns

Так как многочлены x^4+1 и $c(x)$ взаимно просты, это значит, что существует обратная операция умножения.

Процедура Add Round Key

В этой процедуре при каждой итерации блок State дополняется итерационным ключом (Round Key) – см. рис. 6.

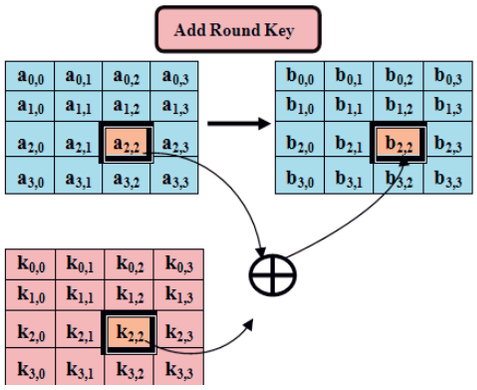


Рис. 6. Процедура Add Round Key

Ключ Round Key формируется с помощью процедуры Key Expansion, а длина его равняется длине блока State. Процедура Add Round Key суммирует побайтно каждый байт блока State с соответствующим байтом ключа по двум модулям [7].

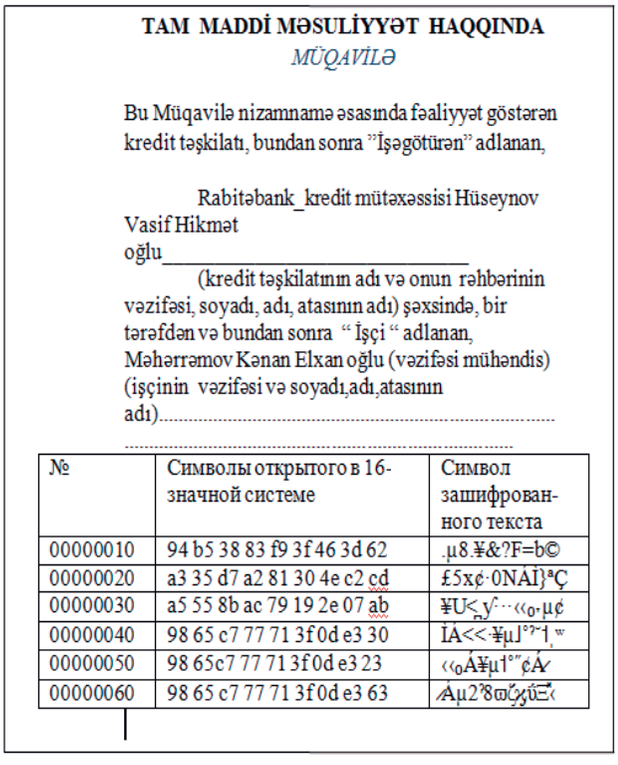
Процедура Key Expansion

Эта процедура состоит из двух подпроцедур. Первая подпроцедура используется для расширения ключа криптографического шифрования *k*. В целом, для алгоритма требуется расширенный ключ, состоящий из $N^b(N^r+1)$ слов (при длине слова 4 байта), из которых один начальный ключ, состоящий из N^b слов, для входа алгоритма и итерационные ключи для итераций [8].

Например, для блока с длиной 256 бит и 14 итераций длина расширенного ключа будет $128\cdot(14+1)=1920$ бит.

На вход процедуры Key Expansion задается первичный секретный шифровальный ключ *K* (Chipper Key), в результате чего получается линейный массив, состоящий из $N^b(N^r+1)$ слов. Этот массив представляется в виде $\{w_i\}i=0,N^b(N^r+1)$. Расширенный ключ формируется следующим образом [9]: его первые N^k слов сохраняют в себе шифровальный ключ (ChipperKey). Каждое его очередное слово w_i образуется путем сложения слов w_{i-1} (на одну позицию до w_i) и w_{i-N^k} (на N^k позиций до w_i) по двум модулям. Слова, находящиеся на делимой на величину N^k позиции, определяются следующим образом: сперва слово w_{i-1} сдвигается влево на $1b$ (один байт) и складывается с постоянной R_{coni}, принятой для этой итерации по двум модулям. Затем полученный результат складывается со словом w_{i-N^k} по двум модулям [10].

Вторая подпроцедура обеспечивает выбор итерационного ключа. Таким образом, для создания ключа итерации из расширенного массива ключей выбираются слова от $w\left|N^b i\right|$ до $w\left|N^b(i+1)\right|$. Описанная выше методика шифрования электронных данных была использована в корпоративной сети республиканского объединения «АзерПочт», в его Гянджинском филиале. Пример шифрования текста документа представлен на рис. 7. Так как алфавит и язык текста, а также его содержание не влияют на процедуры шифрования и не сказываются на эффективности криптографического алгоритма, то здесь представлен фрагмент текста на языке оригинала. Там же приводится и соответствующая ему криптограмма, составленная с использованием стандарта AES.



TAM MADDİ MƏSULİYYƏT HAQQINDA

MÜQAVİLƏ

Bu Müqavilə nizamnamə əsasında fəaliyyət göstərən kredit təşkilatı, bundan sonra "İşəgötürən" adlanan,

Rabitəbank_kredit mütəxəssisi Hüseynov Vasif Hikmət oğlu_____

(kredit təşkilatının adı və onun rəhbərinin vəzifəsi, soyadı, adı, atasının adı) şəxsində, bir tərəfdən və bundan sonra " İşçi " adlanan, Məhərrəmov Kənan Elxan oğlu (vəzifəsi mühəndis) (işçinin vəzifəsi və soyadı,adı,atasının adı).....

.....

№	Символы открытого в 16-значной системе	Символ зашифрованного текста
00000010	94 b5 38 83 f9 3f 46 3d 62	.µ8.¥&?F=b©
00000020	a3 35 d7 a2 81 30 4e c2 cd	£5x¢·0NÂÍ}ªÇ
00000030	a5 55 8b ac 79 19 2e 07 ab	¥U<¬y·‹‹₀.µ¢
00000040	98 65 c7 77 71 3f 0d e3 30	ÍA<<·¥µJ°?¯ì¸ʷ
00000050	98 65c7 77 71 3f0d e3 23	‹‹₀Á¥µ1°"¢Á
00000060	98 65 c7 77 71 3f 0d e3 63	Áµ2?8œÇ¿ûΞ‹

Рис. 7. Фрагмент и шифрограмма шифруемого текста

Как видно, здесь выполнено одно из основных требований к методам криптографического преобразования: длина зашифрованного текста не превышает длину исходного текста, например, длина исходного текста 160 байт, зашифрованного – 159 байт. Немаловажным преимуществом является и возможность ее реализации в системах, обладающих ограниченными вычислительными возможностями, каковыми являются почтовые сети, и не требует значительных дополнительных затрат на создание системы защиты.

Выводы

Апробация представленного метода защиты информации показала, что этот стандарт действительно является достаточно надежным инструментом шифрования электронных данных и может быть успешно использован в корпоративных сетях почтовых объединений для защиты информации.

Потенциально уязвимым моментом при использовании AES является вероятность доступа к шифровальным ключам. Для предупреждения этого нами разрабатывается методика передачи ключа открытым каналом по методу стеганографии, когда передаваемая ценная информация скрывается в другой, менее ценной.

Литература

1. Нагиева А. Ф. Корпоративные сети и проблемы безопасности // Молодой ученый (Казань). № 29 (133), 2016. – С. С. 34-36.
2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М.: ИД «Форум-Инфра-М», 2011. – С. 45-48.
3. Əliquliyev R.M. İmamverdiyev Y.M. Kriptoqrafiyanın əsasları // İnformasiya texnologiyaları (Bakı) // . 2006. – C. 688.
4. Əliquliyev R.M., İmamverdiyev Y.M. Kriptografiya tarixi // İnformasiya texbologiyaları (Bakı), 2006. – C. 190-192.
5. Cheswick W., Bellovin S., Addison W. Firewalls and Internet security // URL: http:// www. Anatoy.Su.Oz.au/danny/bookreview// firewals_ and_Internet Security. html (д.о. 15.12.2016).
6. Şeker Şadi Evren. AES (Advanced Encryption Standard) Kriptoloji. // http: //www.bilgisayar kavramlari. html (д.о. 20.12.2016).
7. Bender W., Gruhl D., Morimoto N., Lu A. Techniques for data hiding // IBM Systems Journal. Vol. 45, №3&4, 2006. – P. 336.
8. Bassard J. Modern Cryptology // Springer-Verlag, Berlin- Heidelberg. №23, 2008. – P. 103-106.
9. Cachin C. An Information-Theoretic Model for Cryptology // Lecture Notes in Computer Science. Springer, №10, 2008. – P. 23-26.
10. Nabiyev V.V. İç- içe bölütlenmiş gizli görüntü paylaşım şeması // 2014 İEEE 22nd Signal Processing and Communications Applications Conference, Trabzon, 2014. – P. 2074-2077.

Получено 03.07.2017

Вердиев Сакит Гамбай оглу, д.т.н., профессор Кафедры информатики и телекоммуникации (ИТК) Азербайджанского технологического университета (АТУ), Азербайджан, г. Гянджа. Тел. +99-450-378-73-37. E-mail: info_tel@inbox.ru.

Нагиева Абабил Фахраддин гызы, старший преподаватель Кафедры ИТК АТУ. Тел. +99-422-257-51-45. E-mail: nagiyevaababil@gmail.com.

ON AES STANDARD IMPLEMENTATION FOR CORPORATE NETWORKS

Verdiyev S.G., Nagiyeva A.F.
Azerbaijan Technological University, Ganja, Azerbaijan
E-mail: info_tel@inbox.ru

In this article corporate information protection by data encryption is considered. For plaintext encryption the usage of Rijndael algorithm is proposed. The algorithm operates on sequences of blocks called "states". Encryption involves four transformation stages named as follows: SubByte, ShiftRows, Mix-Columns and AddRoundKey. In the article an example of AES encryption of a typical plaintext representing a corporate mail is shown. It is confirmed that ciphertext length (160 bytes) is almost the same as plaintext length (159 bytes), which corresponds to the requirements. Field test results show the advantages of the proposed encryption method for telecommunication systems with limited computational capabilities.

Keywords: information protection, corporate networks, cryptography, data encryption, plaintext, Rijndael algorithm, Advanced Encryption Standard, AES, iterative transformations, SubByte, ShiftRows, MixColumns, AddRoundKey, corporate mail

DOI: 10.18469/ikt.2017.15.4.08

Verdiyev Sakit Gambay oglu, Azerbaijan Technological University, AZ2011, Azerbaijan, Ganja, Khatai st.103; Professor of the Department of Informatics and Telecommunications; Doctor of Technical Science. Tel.: +994503787337. E-mail: info_tel@inbox.ru.

Nagiyeva Ababil Faxraddin qızı, Azerbaijan Technological University, AZ2011, Azerbaijan, Ganja, Khatai st.103.; Senior Lecturer of the Department of Informatics and Telecommunications. Tel.: +994222575145. E-mail: nagiyevaababil@gmail.com.

References

1. Nagiyeva A.F. Korporativnie seti i problemi bezopasnosti [Corporative sets and problems of securi-ty]. *Molodoi ucheniy*, 2016, vol. 29, no. 133, pp. 34-36.
2. Shangin V.F. Informacionnaya bezopasnost kompyuternikh system i setey [Information security of computer systems and sets]. Moscow, Forum-Infra-M Publ., 2011. 45 p.
3. Aliguliyev R.M., Imamverdiyev Y.M. *Kriptoqrafiyanin asaslari* [Basis of cryptography]. Baku, Informasiya texnologiyaları, 2006. 688 p. (In Turkish).
4. Aliguliyev R.M., Imamverdiyev Y.M. *Kriptografiya tarixi* [The history of cryptography]. Baku, Informasiya texnologiyaları, 2006. 192 p. (In Turkish).
5. Cheswick W., Bellovin S., Addison W. *Firewalls and Internet security.* Available at: http:// www.anatoy.su.oz.au/danny/book-review/h/firewals_and_InternetSecurity.html (accessed 15.12.2016).
6. Sheker Shadi Evren. *AES (Advanced Encryption Standard) Kriptoloji* [AES (Advanced Encryption Standard) Cryptology]. Available at: https:// www.bilgisayar kavramlari.html. (accessed 20.12.2016)
7. Bender W., Gruhl D., Morimoto N., Lu A. Techniques for data hiding. *IBM Systems Journal*, 2006, vol. 45, no. 3&4, pp. 313-336.
8. Brassard J. *Modern Cryptology*. Springer-Verlag, Berlin-Heidelberg, 2008. pp.103-106 .
9. Cachin C. *An Information-Theoretic Model for Cryptology. Lecture Notes in Computer Science*. Springer, 2008, no. 10, pp. 23-36.
10. Nabiyev V.V., Ich iche bolutlenmish gizli goruntu paylashım sheması [Nested Compartment Secret Image Sharing Scheme]. *2014 IEEE 22 nd Signal Processing and Communications Applications Conference. Trabzon*, 2014, pp. 2074- 2077.

Received 03.07.2017