УДК 681.3.06: 519.248.681

РЕЗУЛЬТАТЫ АНАЛИЗА АЛГОРИТМА ШИФРОВАНИЯ ADE

Р.В. ОЛЕЙНИКОВ, В.И. РУЖЕНЦЕВ, М.С. МИХАЙЛЕНКО, А.Б. НЕБЫВАЙЛОВ

Выполнен анализ конкурсной заявки алгоритма шифрования ADE, представленного на открытый конкурс криптографических алгоритмов в качестве кандидата на национальный стандарт шифрования Украины. Показано, что в спецификации шифра допущены ошибки, приводящие к невозможности расшифрования на некоторых ключах. Обнаружено существование достаточно большого количества слабых ключей ADE, использование которых приводит к значительному снижению криптографической стойкости шифра.

An analysis of the competition application of the ciphering algorithm ADE submitted to the public competition of cryptographic algorithms as a candidate to the national ciphering standard of Ukraine is carried out. It is shown that there are errors in the specification which result in the impossibility of decryption on some keys. The existence of a sufficiently large number of ADE weak keys is revealed, which leads to a considerable decrease of cryptographic cipher security.

ВВЕДЕНИЕ

В октябре 2006 года в Украине был начат национальный конкурс симметричных блочных алгоритмов шифрования [1]. На конкурс было подано 5 алгоритмов, представленных несколькими исследовательскими коллективами. Один из этих алгоритмов – ADE – является модифицированным вариантом широко распространенного стандарта шифрования AES/Rijndael [2]. Отличия ADE заключаются в широком применении ключезависимых операций, что улучшает статистические свойства шифра и его стойкость к известным методам криптоанализа. Тем не менее, использование таких операций потенциально грозит появлением значительного количества классов «слабых» ключей шифрования, при использовании которых криптографическая стойкость шифра значительно снижается.

1. ОПИСАНИЕ КОНКУРСНОЙ ЗАЯВКИ

В конкурсную заявку входит непосредственно спецификация алгоритма ADE, программная реализация, её исходные тексты и описание интерфейса, несколько вариантов тестовых и отладочных векторов. Кроме того, приводятся рекомендации по программной реализации шифра на различных платформах, результаты тестирования производительности, а также. Выполнено обоснование и проведен выборочный анализ свойств компонентов шифра, рассмотрены подходы к реализации различных криптоаналитических атак применительно к ADE, проведен статистический анализ выходной последовательности шифра (режим CBC) в соответствии с набором тестов NIST STS [3].

2. КРАТКОЕ ОПИСАНИЕ ШИФРА ADE

Как уже отмечалось выше, рассматриваемый алгоритм шифрования построен на основе AES и имеет SPN-структуру с чередованием блоков линейного и нелинейного преобразования.

В общем виде, шифр ADE можно представить в следующем виде:

$$ADE_{K_0} =$$

$$= \sigma_{K_{10}} \circ \pi_{K_{10}} \circ \gamma_{K_{10}} \circ \sigma_{K_9} \circ \prod_{i=0}^{8} \left(\theta_{K_i} \circ \pi_{K_i} \circ \gamma_{K_i} \circ \sigma_{K_i} \right),$$

где σ_{K_j} – *AddRoundKey(State, RoundKey)* – операция побитового сложения с раундовым ключом K_j по модулю 2; π_{K_j} – *ShiftRows(State, RoundKey)* – управляемый циклический сдвиг строк состояния шифра; γ_{K_j} – *ByteSub(State, RoundKey)* – нелинейное преобразование (подстановка), зависящая от раундового ключа; θ_{K_i} – *MixColumn(State, RoundKey)* – блок линейного преобразования, также управляемый раундовым ключом.

Основное отличие ADE от AES заключается в том, что все используемые преобразования при шифровании являются ключезависимыми.

3. АНАЛИЗ СПЕЦИФИКАЦИИ ШИФРА

Несмотря на достаточно хорошее описание, в спецификации присутствуют ошибки, потенциально приводящие к необратимости прямого преобразования (невозможности корректного расшифрования), в частности:

3.1. Корректное расшифрование в режиме простой замены невозможно при наличии раундовых ключей, содержащих байты со значением 0 или 1.

3.1.1 Небиективность преобразования ByteSub алгоритма ADE при нулевом значении байта раундового ключа.

Шифр ADE использует модифицированное (относительно AES) преобразование ByteSub (п.4.3.1 спецификации, формула (4.3)):

$$b = M \cdot (a \cdot \gamma)^{-1} + \beta,$$

где a – входной байт, γ – значение байта раундового ключа.

В описании шифра упоминается значение $\gamma = '01' = \{1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\}$, при котором преобразование ByteSub алгоритма ADE соответствует этому же блоку AES, другие значения γ не оговариваются.

Заметим, что при $\gamma = 0$ результат произведения $a \cdot \gamma$ всегда имеет нулевое значение, что определяет фиксированный (независимый от входа) выход преобразования ByteSub алгоритма ADE.

Соответственно, при $\gamma = 0$ преобразование ByteSub шифра ADE не является биективным, что

определяет небиективность всего шифрующего преобразования ADE при наличии хотя бы одного нулевого значения в байтах раундовых ключей.

В рассматриваемом случае, при наличии хотя бы одного нулевого байта в любом раундовом ключе алгоритма ADE корректное расшифрование (режим простой замены) маловероятно.

3.1.2 Небиективность преобразования Mix Column алгоритма ADE при наличии байтов раундового ключа со значением 0 или 1.

Алгоритм ADE использует модифицированное (относительно AES) преобразование MixColumn (п.4.3.3 спецификации):

$$\mathbf{M'} = \begin{pmatrix} s & s^2 & s^3 & \dots & s^{4i} \\ s^2 & s^4 & s^6 & \dots & s^{8i} \\ s^3 & s^6 & s^9 & \dots & s^{12i} \\ \dots & \dots & \dots & \dots & \dots \\ s^{4i} & s^{8i} & s^{12i} & \dots & s^{16i} \end{pmatrix}.$$

Исходя из раундового преобразования (п. 4.3 спецификации) и вызова функции MixColumn (State, RoundKey), подразумевается, что s – некоторый байт раундового ключа (метод выбора байта в спецификации не оговорен).

Соответственно, при $s = 0$ умножение любого входного вектора на матрицу $\mathbf{M'}$ в результате даст нулевой выходной вектор при любом входном значении.

При $s = 1$ умножение любого входного вектора на матрицу $\mathbf{M'}$ в каждом выходном байте будет давать одно и то же значение, равное сумме входных байтов.

В любом из этих случаев преобразование $\mathbf{M'}$ не имеет обратного, соответственно, цикловая функция небиективна.

Таким образом, выбор s из байтов раундового ключа со значением 0 или 1 приводит к невозможности корректного расшифрования (в режиме простой замены).

4. ОТЛИЧИЯ ПРОГРАММНОЙ РЕАЛИЗАЦИИ ОТ СПЕЦИФИКАЦИИ

Программная реализация, представленная в конкурсной заявке вместе со спецификацией шифра, не соответствует описанию шифра ADE.

В частности, обнаружены следующие расхождения:

– при генерации таблиц замены (ByteSub) нулевые значения подключей ($\gamma = 0$) заменяются единичными ($\gamma = 1$);

– при построении матрицы линейного преобразования M′ (MixColumn) нулевые и единичные значения подключей $\gamma = 0, \gamma = 1$ заменяются на $\gamma = 2$;

– реализация преобразования ShiftRows (п. 4.3.2 спецификации) определяет значения сдвигов $\{\lambda_j^u, \lambda_{j+1}^u\}$ из разных байтов, а не из одного, как задано в спецификации; сдвиг строки определяется не значением $\{\lambda_j^u, \lambda_{j+1}^u\}$, а результатом модульного сложения значения $\{\lambda_j^u, \lambda_{j+1}^u\}$ с соответствующим значением сдвига строки в алгоритме AES.

Несоответствия в реализации частично устраняют неточности спецификации, но, соответственно, возникают вопросы к достоверности результатов статистического тестирования и обоснованности стойкости шифра к криптоаналитическим атакам.

5. КРИПТОАНАЛИЗ АЛГОРИТМА ШИФРОВАНИЯ ADE

Как уже было отмечено выше, спецификация и эталонная программная реализация имеют отличия. Алгоритм преобразования, определяемый в спецификации, на некоторых ключах шифрования не является симметричным блочным шифром, поскольку не имеет обратного преобразования. Более того, на таких ключах ухудшаются статистические свойства преобразования, и, соответственно, криптографическая стойкость.

Поскольку эти недостатки устранены в эталонной программной реализации, в дальнейшем будем ориентироваться на алгоритм шифрования, полностью соответствующий именно программной реализации.

Очевидно, что обилие ключезависимых операций значительно затрудняют проведение дифференциального [4] и линейного [5] криптоанализа, а также других атак на их основе, что справедливо отмечено и авторами шифра. В связи с этим целесообразно основное внимание уделить анализу свойств схемы разворачивания ключей и особенностям ключезависимых операций шифра ADE.

Схема разворачивания ключей ADE (в спецификации – «расширение ключа») практически полностью совпадает со схемой AES/Rijndael. Отличие составляет применение модифицированного S-блока (используется неприводимый полином, отличающийся от соответствующего полинома AES/Rijndael).

Соответственно, статистические свойства схем разворачивания подключей алгоритмов ADE и AES/Rijndael должны быть примерно одинаковыми. Для проверки этой гипотезы было выполнено статистическое тестирование выходных последовательностей схем разворачивания с использованием с набора тестов NIST STS. Размер блока и ключа шифров ADE и AES/Rijndael задавался равным 128 битам.

Генерация выборок осуществлялась следующим образом. Для случайного начального ключа K_0 формировались цикловые (раундовые) подключи $RK_0^0 - RK_0^{10}$ (отметим, что в соответствии со спецификацией, $RK_0^0 = K_0$). Следующий ключ шифрования принимался равным последнему сгенерированному подключу: $K_1 = RK_0^{10} = RK_1^0$, и так далее, в соответствии с соотношением $K_{i+1} = RK_i^{10} = RK_{i+1}^0, i = 0,1,...$ Выходная последовательность формировалась из сформированных подключей и имела следующий вид:

$$K_0 = RK_0^0, RK_0^1, \ldots, RK_0^{10} = K_1 = RK_1^0,$$

$$RK_1^1, \ldots, RK_1^{10} = K_2 = RK_2^0, \ldots, RK_i^{10} = K_{i+1} = RK_{i+1}^0, \ldots$$

Процесс генерации продолжался до формирования выборки соответствующего объема.

Полученные выборки тестировались пакетом NIST STS. Результаты тестирования для ADE и AES/Rijndael приведены соответственно на рис. 1 и рис. 2.

Как видно из приведенных рисунков, обе последовательности успешно прошли тестирование.

Соответственно, можно сделать предположение о равновероятности различных битовых комбинаций в каждом из подключей, в частности, значений $\{\lambda_0^u, \lambda_1^u\}$, управляющих байтовыми сдвигами на каждом цикле преобразования.

Равновероятность этих значений чрезвычайно важна для обеспечения перемешивания при зашифровании. В случае, если из-за значений ключевых битов сдвиги будут отсутствовать или сдвиг будет выполняться на одно и то же значение, активизация будет локализована в пределах одного 32-битового блока. Возможные отличия между активизацией байтов в AES и ADE, приводящие к ухудшению криптографических свойств, представлены на рис. 3.

Теоретическая оценка вероятности появления такого события (байты каждой колонки сдвигаются на одно и то же значение) для всех 10 циклов шифрования (размер блока и ключа – 128 битов) при случайных, равновероятных и независимых раундовых ключах равна

$$P(K_S^0(\lambda_0^u, \lambda_1^u) = K_S^0(\lambda_2^u, \lambda_3^u) = K_S^0(\lambda_4^u, \lambda_5^u) =$$
$$= K_S^0(\lambda_6^u, \lambda_7^u) | \ldots | K_S^9(\lambda_0^u, \lambda_1^u) = \ldots,$$
$$= K_S^9(\lambda_6^u, \lambda_7^u)) = \left(2^{-6}\right)^{10} = 2^{-60},$$

где $K_S^j(\lambda_{2i-1}^u, \lambda_{2i}^u)$ – значение байтового сдвига i-й строки ($i = 1,2,3,4$) на j-м цикле шифрования алгоритма ADE.

Таким образом, при хорошей схеме разворачивания вероятность появления цепочки подключей, при которой алгоритм 128-битовый шифр распадается на 4 шифра с блоком в 32 бита составляет величину 2^{-60}, что чрезвычайно мало, и вычислительный поиск такого слабого ключа является практически нереализуемой задачей.

Эта гипотеза была проверена в ходе вычислительного эксперимента. С помощью аппаратного генератора случайных чисел («Гряда») формировались ключи шифрования (блок и ключ – размером 128 битов), выполнялась схема разворачивания, а в полученных подключах выполнялся поиск совпадения значений, при которых активизация не выходит за пределы одного 32-битового блока:

$$K_S^0(\lambda_0^u, \lambda_1^u) = K_S^0(\lambda_2^u, \lambda_3^u) = K_S^0(\lambda_4^u, \lambda_5^u) = K_S^0(\lambda_6^u, \lambda_7^u),$$

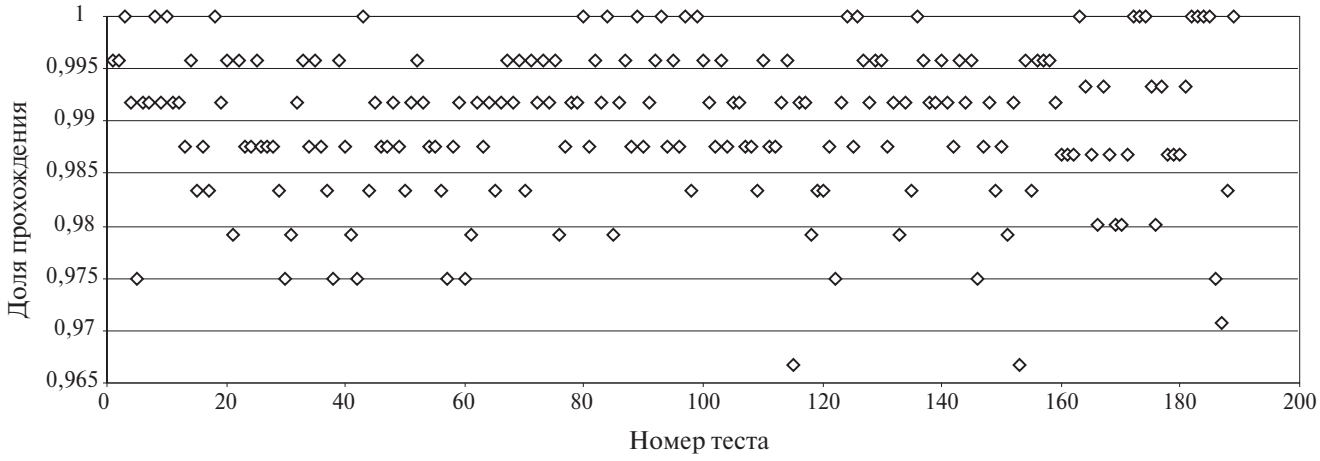

Рис. 1. Результаты статистического тестирования последовательности раундовых ключей ADE

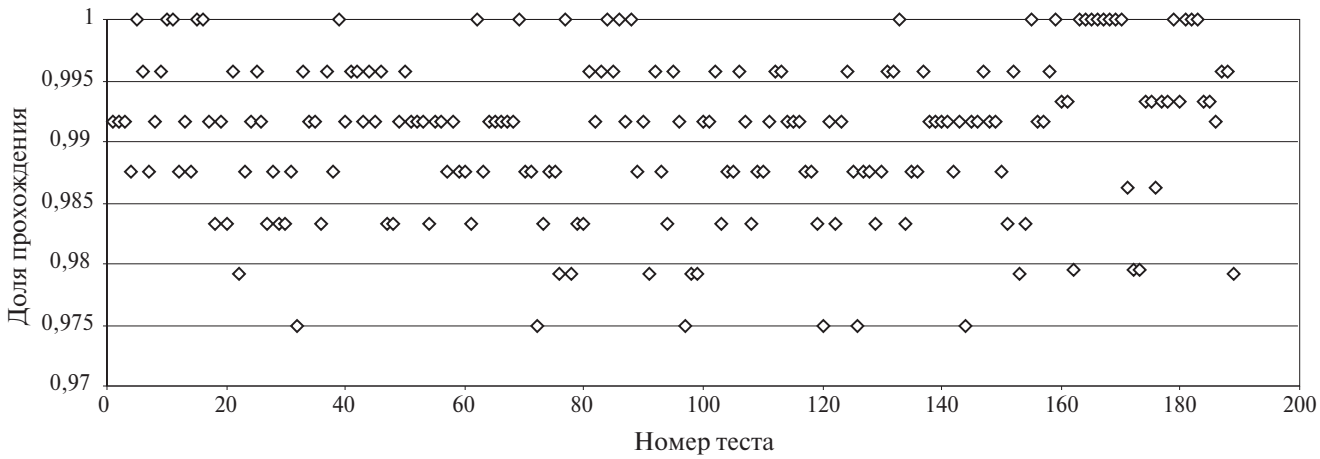

Рис. 2. Результаты статистического тестирования последовательности раундовых ключей AES/Rijndael

$$K_S^1(\lambda_0^u,\lambda_1^u) = K_S^1(\lambda_2^u,\lambda_3^u) = K_S^1(\lambda_4^u,\lambda_5^u) = K_S^1(\lambda_6^u,\lambda_7^u),$$

$$K_S^2(\lambda_0^u,\lambda_1^u) = K_S^2(\lambda_2^u,\lambda_3^u) = K_S^2(\lambda_4^u,\lambda_5^u) = K_S^2(\lambda_6^u,\lambda_7^u),$$

...

$$K_S^9(\lambda_0^u,\lambda_1^u) = K_S^9(\lambda_2^u,\lambda_3^u) = K_S^9(\lambda_4^u,\lambda_5^u) = K_S^9(\lambda_6^u,\lambda_7^u).$$

Вопреки теоретической оценке, результаты статистического эксперимента позволили обнаружить достаточно большое количество ключей шифрования (мастер-ключей), чьи развернутые подключи соответствуют такому требованию. После обработки примерно 8 млрд. (2^{33}) случайных значений, были отобраны следующие ключи, представленные в шестнадцатеричной нотации:

```
fd 58 e5 2c d8 83 d8 f7 e3 2a c0 69 1c 3c 1c 7f
15 72 1f e8 00 2e 00 b4 76 66 ec fb 38 20 38 bd
32 b5 e1 ed 88 e0 88 b8 86 3f 74 8f b0 cf b0 7f
64 7a e4 cb bc 60 bc d1 a1 00 a8 15 90 aa 90 bf
03 7b fe 1c 50 2f 50 48 2b 81 24 71 3c 4a 3c ba
c1 60 b8 dd 18 46 18 fb dd 1f e8 4a 24 02 24 57
```

На полученных ключах алгоритм шифрования ADE (128/128) распадается на 4 шифра с размером блока 32 бита, каждый из которых обрабатывается независимо от других.

Полученный результат свидетельствует о факте существования слабых ключей ADE, при которых структура открытого текста отображается в структуру шифртекста, что является серьёзной уязвимостью шифра.

Факт наличия уязвимости дополнительно подтверждается тем, что при зашифровании на слабом ключе входного сообщения с большой избыточностью криптограмма не проходит статистическое тестирование NIST STS (рис.4), хотя для других ключей тестирование проходит успешно.

Поиск точной оценки количества таких слабых ключей не выполнялся, но факт обнаружения сразу нескольких значений для сравнительно небольшой выборки свидетельствует о существовании значительного количества слабых ключей шифрования алгоритма ADE.

Аналогичное тестирование было проведено для схемы разворачивания ключей AES/Rijndael, что подтвердило наличие этих свойств (неравно-

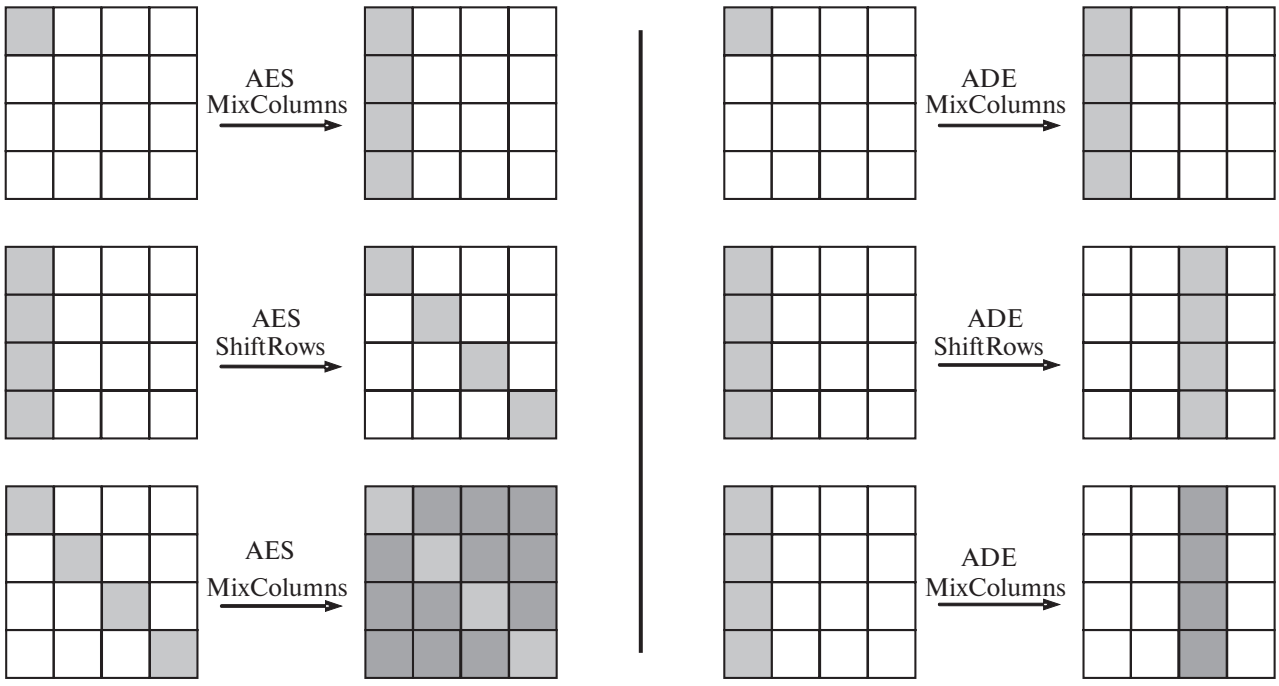

Рис. 3. Возможные отличия между активизацией байтов в AES и ADE

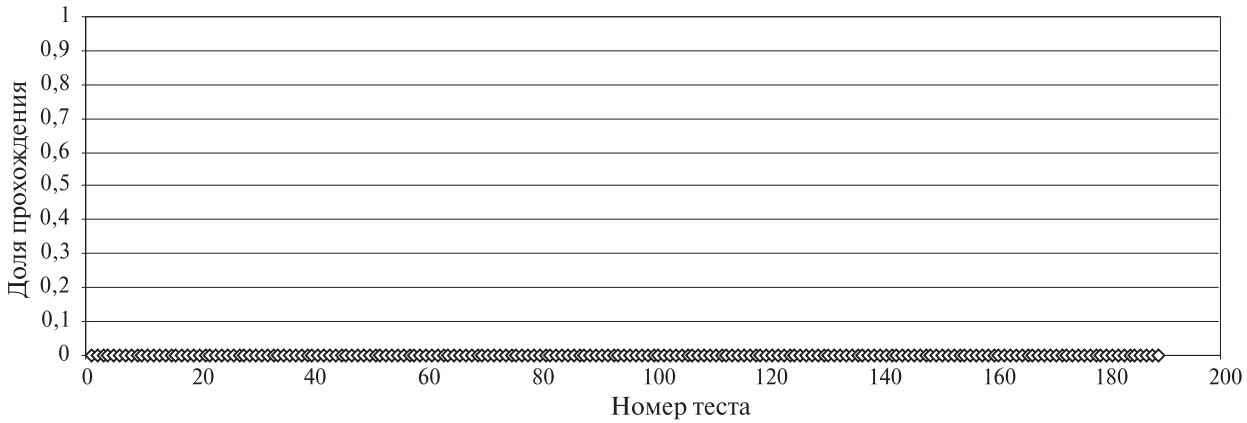

Рис. 4. Статистическое тестирование выходной последовательности ADE, полученной на слабом ключе

вероятность и зависимость битовых комбинаций) и в ключевой схеме AES/Rijndael.

Таким образом, использование схемы разворачивания ключей с недостаточно хорошими свойствами рассеивания вместе с введением большого количества ключезависимых операций привело к существованию значительного количества слабых ключей ADE, при которых алгоритм не соответствует требованиям к криптографическим свойствам и уровню стойкости современных блочных шифров.

ВЫВОДЫ

1. Спецификация алгоритма ADE, представленная в составе конкурсной документации, допускает существование ключей, при которых прямое преобразование не является обратимым (расшифрование невозможно), и, соответственно, сам алгоритм, определённый в спецификации, не является блочным шифром.

2. Программная реализация в составе конкурсной документации не соответствует спецификации. Обнаруженные несовпадения относятся к ключезависимым операциям, и приводят к корректировке небиективности шифрующего преобразования. Только алгоритм, чья программная реализация подана в составе конкурсной документации, можно отнести к блочным шифрам.

3. Поскольку из двух вариантов алгоритма ADE (определённого в спецификации и представленного в эталонной реализации) второй обладает большим уровнем стойкости, причём только он может быть назван блочным шифром, дальнейшие исследования проводились только для второго варианта.

4. В алгоритме шифрования ADE существует значительное количество слабых ключей, при использовании которых шифр обладает серьёзной уязвимостью (128-битовый шифр работает как 4 независимых 32-битовых шифра, и структура открытого текста полностью отображается в структуру шифртекста).

Литература

1. Положення про проведення відкритого конкурсу криптографічних алгоритмів. Інститут кібернетики імені В.М. Глушкова, ДСТСЗІ СБ України. http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=48383&cat_id=38710.
2. National Institute of Standards and Technology, FIPS-197: «Advanced Encryption Standard.» Nov. 2001. http://www.nist.gov/aes
3. NIST Special Publication 800-22A. Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf
4. E. Biham and A. Shamir. Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, New York, 1993.
5. M. Matsui. Linear Cryptanalysis Method for the DES Cipher. Lecture Notes in Computer Science, Advances in Cryptology, in proceedings of Eurocrypt '93, 1993.

Поступила в редколлегию 8.09.2008

Олейников Роман Васильевич, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.

Руженцев Виктор Игоревич, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ блочних симметричных шифров.

Михайленко Матвей Сергеевич, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: криптография та криптоанализ блочних симметричных шифров.

Небывайлов Алексей Борисович, аспирант кафедры БИТ ХНУРЭ, главный консультант управления спецтелекоммуникаций и технического обеспечения Государственного управления делами Президента Украины. Область научных интересов: блочные шифры, криптоанализ.