и создаёт проблемы для нахождения правильного ключа. Тем не менее, результаты говорят об эффективности данной атаки по отношению к шифру RC5.

Таблица 4

Результаты реализации атаки

Раунд	Число ключей	Правильно
2	50	24
3	25	19
4	5	3

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Рябко Б.Я., Монарев В.А., Шокин Ю.И.* Новый тип атак на блоковые шифры // Проблемы передачи информации, 2005. - Т.41, № 4, -С.385-394.

2. *Schneier B. Applied Cryptography* // N.-Y., Wiley, 1996.

3. *B.Ya. Ryabko, V.A. Monarev*. Using information theory approach to randomness testing // Journal of Statistical Planning and Inference, 2005, -Vol. 133, № 1, -PP. 95-110.

4. *J. Massey, G. Khachatrian, M. Kuregi*an. Nomination of SAFER++ as Candidate Algorithm for the New European Schemes for Signatures, Integrity, and Encryption (NESSIE) Presented at the First Open NESSIE Workshop, November 2000.

Л.К. Бабенко, Е.А. Ищукова
Россия, г. Таганрог, ТРТУ

ОСОБЕННОСТИ ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА АЛГОРИТМА AES

В мае 2002 года в силу вступил новый стандарт блочного шифра США AES, в основе которого лежит алгоритм шифрования Rijndael. В связи со своей новизной алгоритм Rijndael является предметом многих обсуждений. Аналитики ищут его слабые места, однако их попытки пока не приносят особых успехов. Авторы статьи также стараются внести свой вклад в рассмотрение вопросов криптографической стойкости алгоритма. В стандарте AES алгоритм шифрования оперирует блоками, длина которых равна 128 битам. Как правило, исходный блок данных, промежуточные значения и зашифрованные данные на выходе алгоритма принято представлять в виде 16-байтового массива байтов, имеющего четыре строки и четыре столбца (каждая строка и каждый столбец в этом случае могут рассматриваться как 32-разрядные слова). Ключ шифрования также представляет собой такой же двумерный массива Каждый раунд шифрования состоит из четырех различных преобразований: замены байтов SubBytes(); сдвига строк ShiftRows(); перемешивания столбцов MixColumns и сложения с раундовым ключом AddRoundKey. Дифференциальный криптоанализ основан на прослеживании изменения схожести между двумя текстами, в процессе их последовательного прохождения через алгоритм шифрования. При этом, как правило, самое большое влияние на изменение схожести имеют те блоки алгоритма, в которых происходит нелинейное преобразование. Как правило, роль такого преобразования выполняют блоки замены, чаще всего обозначаемые как S-блоки. В алгоритме шифрования Rijndael подобного рода нелинейную замену данных выполняет преобразование **SubBytes**, обеспечивающее побайтную замену данных [1].

Нами было проанализировано преобразование **SubBytes** на предмет стойкости к дифференциальному криптоанализу и выявлено несколько особенностей, характерных для таблицы соответствия входных и выходных дифференциалов, показывающей с какой вероятностью на выходе блока появится та или иная разность ΔC, если на входе блока была разность ΔA. Знание этих особенностей может

существенно помочь при разработке алгоритма проведения дифференциального криптоанализа. Выявленные особенности следующие:

– максимальное значение в таблице равно 4, за исключением первой ячейки, соответствующей разностям $\Delta A = 0$ и $\Delta C = 0$, значение в которой равно 256;

– для каждой входной разности только одна выходная разность встречается с вероятностью $p = 4/256$, все остальные выходные разности имеют вероятность появления $p = 2/256$;

– нулевая разность на выходе может появиться только в том случае, если на входе тоже была нулевая разность, в отличие от алгоритма шифрования DES, где нулевая разность на выходе встречалась довольно часто при ненулевой входной разности;

– значение входной разности $\Delta A = 253$ остается неизменным на выходе с вероятностью $p = 4/256$, остальные входные разности либо не могут оставаться неизменными либо имеют вероятность в два раза меньшую.

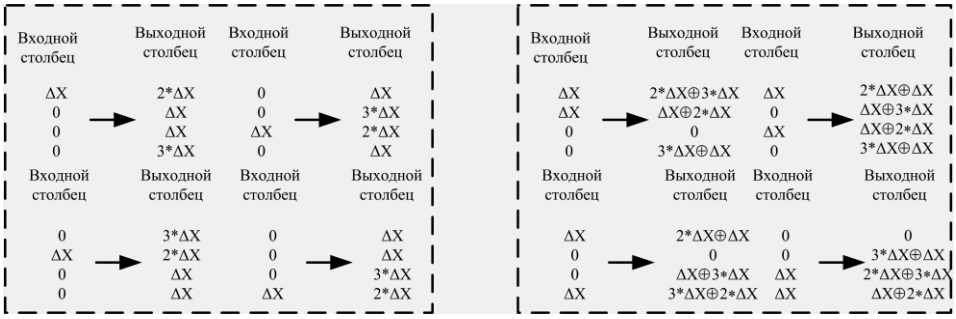

Рис. 1

Рис. 2

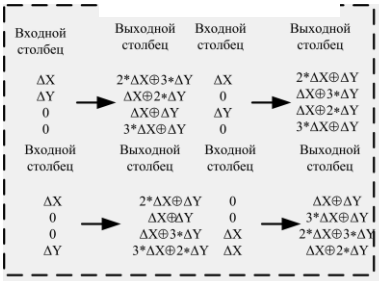

Рис. 3

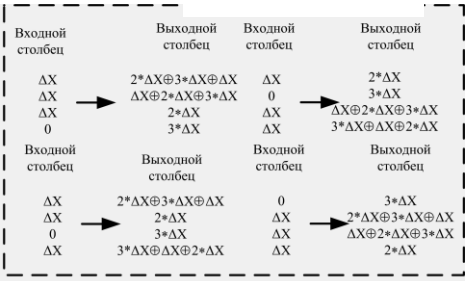

Рис. 4

Рис. 5.

Другим, оказывающим серьезное влияние на изменение дифференциалов в процессе прохождения данных через алгоритм шифрования, является преобразование перемешивания столбцов **(MixColumns)**, при котором столбцы состояния рассматриваются как многочлены над $GF(2^8)$ и умножаются по модулю x^4+1 на многочлен $g(x)$, имеющий вид $g(x)=\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$. В результате такого умножения байты столбца S_{0c}, S_{1c}, S_{2c}, S_{3c} заменяются соответственно на байты:

$S'_{0c} = (\{02\}*S_{0c}) \oplus (\{03\}*S_{1c}) \oplus S_{2c} \oplus S_{3c}$,
$S'_{1c} = S_{0c} \oplus (\{02\}*S_{1c}) \oplus (\{03\}*S_{2c}) \oplus S_{c3}$,
$S'_{2c} = S_{0c} \oplus S_{1c} \oplus (\{02\}*S_{2c}) \oplus (\{03\}*S_{3c})$,
$S'_{3c} = (\{03\}*S_{0c}) \oplus S_{1c} \oplus S_{2c} \oplus (\{02\}*S_{3c})$.

Рассматривая преобразование **MixColumns,** необходимо помнить, что разность рассматривается как сумма по модулю два между двумя состояниями текста, то есть $\Delta X = X \oplus X'$. В этом случае $2*\Delta X = 2*X \oplus 2*X'$ и $3*\Delta X = 3*X \oplus 3*X'$. Принимая это во внимание, нами были выявлены правила изменения разности столбцов в процессе прохождения данных через преобразование **MixColumns.** При этом рассматривались следующие варианты входных столбцов разностей:

– ненулевое значение имеет всего один байт (рис.1);

– ненулевое значение имеют два байта, и при этом ненулевые байты имеют одинаковое значение (рис. 2);

– ненулевое значение имеют два байта, и при этом ненулевые байты имеют разные значение (рис. 3);

– три ненулевых байта, имеющих одинаковое значение (рис. 4);

– все байты равны между собой и отличны от нуля (рис. 5).

Знание вышеприведенных свойств позволяет легко строить цепочки для прослеживания изменения состояний данных в процессе их прохождения через алгоритм шифрования. Дальнейший анализ будет заключаться в построении наиболее вероятной пары входная – выходная разность, нахождении соответствующих пар открытый – шифрованный текст и на их основе частичное или полное определение ключа.

Работа поддержана грантом РФФИ № 06-07-89010

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Л.К.Бабенко, Е.А.Ищукова.* Современные алгоритмы блочного шифрования и методы их анализа. – М: Гелиос АРВ, 2006. – 376 с.

А.Т. Алиев, А.В. Аграновский
Россия, г. Ростов-на-Дону, ФГНУ НИИ "Спецвузавтоматика"

ВОПРОСЫ ПОСТРОЕНИЯ КРИПТОСТЕГАНОГРАФИЧЕСКИХ СИСТЕМ. МОДЕЛЬ СТЕГАНОГРАФИЧЕСКОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ

Стеганографические методы защиты информации приобретают все большую популярность среди рядовых пользователей, вместе с тем использование этих средств сейчас весьма ограничено, что связано с нерешенностью ряда вопросов, основным из которых является вопрос оценки стойкости стегосистем к различным атакам. Еще совсем недавно никаких решений по теоретической и практической оценке стойкости стеганографических систем к атакам со стороны пассивного и активного противников просто не существовало. Более того, часть разработчиков стеганографических средств при проектировании последних даже не рассматривала возможные методы их стегоанализа. Отсутствие на настоящий момент средств сертификации и методов проверки надежности стеганографических систем приводит к тому, что использование последних без использования с ними в комплексе иных средств защиты информации не может гарантировать целостность и конфиденциальность защищаемой информации. Как следствие, стеганографии сейчас уделяется лишь роль некоторого дополнительного средства защиты, к которому не предъявляется никаких требований надежности и стойкости, и которое может использоваться исключительно на свой страх и риск обычными пользователями или коммерческими организациями. Данная работа посвящена вопросам