

О СТОЙКОСТИ ШИФРА RIJNDAEL С ТРИВИАЛЬНЫМ СПИСКОМ КЛЮЧЕЙ

Представлены новые универсальные методы анализа симметричных криптоалгоритмов — на основе рационального и 2-адического продолжения полиномов нормальной алгебраической формы. В основу методов положен поиск локальных максимумов целевой функции относительно архимедова или дискретного нормирования. Алгоритм содержит три этапа. На этапе предвычислений по результатам тестирования метода анализа на большой выборке ключей и открытых тестов составляется общая для шифра матрица условных вероятностей того, что бит ключа будет вскрыт как ноль, если в действительности он равен 0 или 1. На втором этапе для неизвестного ключа находятся вероятности вскрытия разрядов ключа нулем, и на основе сравнения с результатами предвычислений делается предположение об истинном значении разрядов ключа. На третьем этапе ключи опробуются, начиная с наиболее вероятных. Также можно использовать вариант метода, использующий вероятности вскрытия разрядов ключа единицей.

Анализ шифра RIJNDAEL с тривиальным списком ключей с числом раундов 1 и 2 показал, что сложность вскрытия разряда ключа падает по экспоненте от числа раундов. Экстраполяция этой зависимости на 10 раундов показывает, что сложность вскрытия трех битов ключа не превышает 2^{61} .

Данный метод криптоанализа является универсальным статистическим тестом, тесно связанным с природой исследуемого шифра.

A.G. Rostovtsev and N.Ju. Malyshev

Russia, St. Petersburg state polytechnic university

ON THE STRENGTH OF RIJNDAEL CIPHER WITH TRIVIAL KEY SCHEDULE

The approach to block cipher analysis is presented, based on embedding normal algebraic form into the set of rational or 2-adic numbers. Local maxima of goal function are searched with respect to Archimedean or discrete valuation for different initial approximations. The method includes three stages. In the first stage conditional probabilities matrices are computed for known keys. In the second stage the same probabilities are computed for the searched (true) key and compared with those from the first stage. In the third stage potential keys are tested, beginning from the most likely one.

Cryptanalysis of few-rounded RIJNDAEL with trivial key schedule shows that the complexity of key bit computation decreases exponentially of the number of rounds. Extrapolating this dependence to 10 rounds, it is reasonable to suggest that to compute three bits of the key about 2^{61} operations are needed.

The cryptanalysis method can be used as universal statistical test for any cipher, closely connected with the encryption method.

1. Методы анализа блочных шифров

Сложность криптоанализа блочного шифра на основе известных (выбранных) открытых текстов обусловлена тем, что трудно определить, насколько подобранный ключ близок к истинному. Небольшое изменение ключа или открытого текста вызывает значительное (в среднем 50%) изменение разрядов шифрограммы. Иначе говоря, трудно задать метрику, показывающую «расстояние» между подобранным и истинным ключом. Если метрика не определена, то все ключи являются равновероятными, а наилучший способ вскрытия ключа — перебор.

На сегодняшний день существует два способа задания такой метрики. Первый способ задает метрику, характерную для текстов и ключей «в среднем». При этом требуется большой объем открытых и соответствующих зашифрованных текстов, причем каждая

пара таких текстов при вскрытии ключа используется однократно или небольшое число раз. Примером является дифференциальный или линейный криптоанализ [1], [2].

Второй способ основан на вложении множества булевых функций в алгебраическую структуру над упорядоченным множеством. Это позволяет задать метрику, используя небольшое число открытых и зашифрованных текстов. Примером является метод Андельмана и Ридса [3], который основан на арифметическом продолжении множества булевых функций на множество вещественных чисел из диапазона от 0 до 1. Истинный ключ ищется как максимум целевой функции, определенной на множестве действительных чисел, с использованием техники дифференцирования.

Оценим количество открытых текстов необходимое для вычисления ключа. Для этого оценим число битов открытого текста, однозначно определяющих ключ, в предположении, что длина блока n равна длине ключа.

Лемма 1. Для однозначного определения ключа в среднем необходимо $1.368 \cdot n$ битов открытых текстов, где n – длина ключа в битах.

Доказательство. Отображение множества открытых текстов в множество зашифрованных текстов можно задать таблично. Зашифруем фиксированный открытый текст на каждом из 2^n ключей. Если среди 2^n зашифрованных текстов шифртекст, соответствующий данному ключу, встречается однократно (или не встречается ни разу), то для определения ключа достаточно одного текста. Если данный шифртекст встречается дважды, то для определения ключа достаточно двух текстов и т. д.

Аппроксимируя случайное отображение пуассоновским процессом, получаем вероятность того, что данный открытый текст встретится в точности m раз: $\frac{1}{em!}$, где e — основание натурального логарифма. Математическое ожидание числа открытых текстов, необходимых для вскрытия ключа, равно

$$1 \cdot \frac{1}{e} + 1 \cdot \frac{1}{e} + 2 \cdot \frac{1}{e \cdot 2!} + 3 \cdot \frac{1}{e \cdot 3!} + \dots = 1 + \frac{1}{e} \approx 1,368. \quad \blacksquare$$

Очевидно, что второй способ задания метрики более привлекателен, так как дает возможность вычислить ключ по ничтожному количеству известных открытых текстов. Таким образом, в отличие от дифференциального и линейного методов анализа, использующих первый способ задания метрики, от методов анализа, применяющих второй способ, невозможно защититься периодической сменой ключа.

Вместе с тем, оригинальный метод Андельмана и Ридса неэффективен, так как продолженная целевая функция имеет множество локальных максимумов, а с увеличением числа раундов шифра сложность вычисления производной превышает сложность перебора ключей. В данной работе предлагается новый универсальный метод анализа симметричных шифров на основе рационального и 2-адического продолжения полиномов нормальной алгебраической формы.

2. Анализ шифра методами продолжения нормальной алгебраической формы

В основе метода лежит идея вычисления ключа с помощью нахождения максимума специальной целевой функции [4]. Данная функция принимает наибольшее значение только для истинного ключа. Кроме того, она позволяет упорядочить все ключи по степени близости к истинному ключу. Чем ближе тестируемый ключ к истинному ключу (по отношению к побитной метрике), тем больше соответствующее значение целевой функции. Таким образом, меняя по одному разряду подбираемого ключа и сравнивая значения целевой функции можно вычислить ключ.

2.1. Целевая функция

Пусть $\mathbf{x} = (x_1, \dots, x_N)$, $\mathbf{y} = (y_1, \dots, y_N)$ – известные блоки открытого и зашифрованного текста, а $\mathbf{k} = (k_1, \dots, k_n)$ – подбираемый ключ. Предположим, что пара \mathbf{x}, \mathbf{y} однозначно определяет ключ. Определим целевую функцию

$$H = \prod_{i=1}^N (f_i(\mathbf{x}, \mathbf{k}) \oplus y_i \oplus 1),$$

где $f_i(\mathbf{x}, \mathbf{k})$ – булева функция, представляющая алгоритм шифрования, и определяющая значение i -го бита шифрограммы, \oplus – операция сложения по модулю 2.

Лемма 2. Условие $H = 1$ выполняется тогда и только тогда, когда ключ k совпадает с истинным ключом. Для всех других значений ключа $H < 1$.

Доказательство. Вначале покажем, что если аргументы продолженного на $\mathbb{Q}[x_1, \dots, x_n]$ многочлена Жегалкина принимают значение из интервала $(0, 1)$, то и сам продолженный многочлен Жегалкина принимает значения из этого интервала. Действительно, абсолютная величина разности элементов из $(0, 1)$ неотрицательна и не превышает 1, т. е. лежит в $(0, 1)$. Произведение элементов из $(0, 1)$ лежит в $(0, 1)$. Это справедливо для любой записи продолженного многочлена (с раскрытием скобок или без раскрытия скобок).

Таким образом, значение 1 — максимально возможное для продолженной булевой функции. Для двоичных аргументов полукольцо продолженных многочленов Жегалкина превращается в кольцо, совпадающее с \mathbf{G}_n . Поэтому если $f \in \mathbf{G}_n = 1$, то продолженный многочлен f тоже принимает значение 1. Если $f \in \mathbf{G}_n = 0$, то продолженный многочлен f тоже принимает значение 0. Если целевая функция принимает значение 1, то продолженная целевая функция на этом же наборе аргументов принимает значение 1. ■

Если $k_i \in \{0, 1\}$, то для всех ключей, кроме истинного, получаем $H = 0$, то есть все ключи кроме истинного ключа равновероятны. Расширим множество значений k_i до какого-нибудь упорядоченного множества.

Каждая булева функция может быть единственным образом представлена полиномом из кольца полиномов Жегалкина \mathbf{G}_n :

$$\mathbf{G}_n \cong \mathbb{F}_2[k_1, \dots, k_n] / (k_1^2 \oplus k_1, \dots, k_n^2 \oplus k_n),$$

Определим продолжение кольца \mathbf{G}_n на множество \mathbb{Q} рациональных чисел с евклидовым нормированием и на множество \mathbb{Z}_2 целых 2-адических чисел с дискретным показательным нормированием.

Для вложения \mathbf{G}_n в соответствующую структуру над \mathbb{Q} используется продолжение:

$$a \oplus b \rightarrow |a - b|, ab \pmod{2} \rightarrow ab. \quad (1)$$

Отметим, что в случае такого продолжения теряется ассоциативность, но объемлющая структура имеет «характеристику» 2.

2-адическая норма val целого числа определяется следующим образом: $\text{val}(2^a b) = -a$, где b — нечетное число. Для вложения \mathbf{G}_n в соответствующую структуру над \mathbb{Z}_2 по аналогии с приближением вещественных чисел рациональными целое 2-адическое число будем приближенно представлять элементом кольца $\mathbb{Z}_2 / 2^m \mathbb{Z}_2 \cong \mathbb{Z} / 2^m \mathbb{Z}$. В этом случае минимальное значение нормирования равно $-m$ и продолжение имеет вид

$$a \oplus b \rightarrow a + b \pmod{2^m}, ab \pmod{2} \rightarrow ab \pmod{2^m}. \quad (2)$$

Операцию сложение можно также продолжать так:

$$a \oplus b \rightarrow |a - b| \pmod{2^m}. \quad (2a)$$

Продолжение (2) обеспечивает гомоморфное вложение кольца \mathbb{G}_n в кольцо $\mathbb{Z}/2^m\mathbb{Z}[k_1, \dots, k_n]/\mathfrak{A}_m$, где $\mathfrak{A}_m = (k_1^m(1 - k_1^{2^{m-2}}), \dots, k_n^m(1 - k_n^{2^{m-2}}))$. В случае продолжения (2a) объемлющая структура не является кольцом. Аргументы определяются над множеством $(0, 1)$. Продолжение (2) и (2a) приводит к тому, что нули исходной целевой функции в \mathbb{G}_n становятся целыми 2-адическими числами, для которых определено отношение порядка.

Представляя функции $f_i(\mathbf{x}, \mathbf{k})$ многочленом из \mathbb{G}_n , а затем, продолжая полученные многочлены до многочленов над \mathbb{Q} или \mathbb{Z}_2 получим более подходящую целевую функцию H .

Если тестируемый ключ совпадает с истинным ключом, то $H = 1$ (при рациональном продолжении) или $\text{val}_2(H) = 0$ (при 2-адическом продолжении). Если тестируемый ключ отличен от истинного, то $0 \leq H < 1$ или $-m \leq H < 0$. Это позволяет судить о том, насколько близок тестируемый ключ к истинному ключу.

2.2. Поиск локального максимума

Поиск локального максимума осуществляется методом наискорейшего спуска, реализованного следующим образом. Пусть H^* — значение целевой функции для начального приближения на данной итерации. Каждый неопределенный разряд ключа поочередно заменяется на 0 и на 1, при этом вычисляется целевая функция H_0 и H_1 соответственно, затем разряду ключа присваивается первоначальное значение и проверяется очередной разряд ключа. Среди разрядов ключа, для которых выполняется неравенство $H_0 < H^* < H_1$ или $H_1 < H^* < H_0$, выбирается разряд, дающий максимум целевой функции H_0 или H_1 . Затем начальное приближение ключа изменяется в соответствии с найденным значением разряда и выполняется следующая итерация. Итерации повторяются до тех пор, пока не будет найден локальный максимум. Ключ, придающий целевой функции максимальное значение, и есть истинный ключ.

К сожалению, при переходе от \mathbb{G}_n к \mathbb{Q} или \mathbb{Z}_2 теряются некоторые свойства исходного кольца многочленов, поэтому целевая функция H имеет локальные максимумы, не отвечающие задаче криптоанализа. По этой причине метод наискорейшего спуска не всегда точно определяет ключ. Таким образом, можно лишь с определенной вероятностью предсказать истинное значение разрядов ключа. Если данная вероятность для каких-нибудь разрядов ключа отличается от 50% по аналогии с линейным криптоанализом, на основе большого количества статистических данных можно предсказать истинное значение ключа с любой точностью.

2.3. Метод анализа

Метод анализа строится на предположении о том, что вероятности вскрытия разрядов ключа нулями в зависимости от истинного значения ключа (z_{00} при истинном значении 0 и z_{01} при истинном значении 1) в среднем одинаковы для всех ключей.

Таким образом, можно рассчитать эти вероятности для большой представительной выборки ключей. А затем при нахождении значений разрядов неизвестного ключа сравнивать рассчитанную вероятность вскрытия разрядов нулем v_0 : если $v_0 = z_{00}$, то истинное значение данного разряда равно 0, если $v_0 = z_{01}$, то истинное значение данного разряда равно 1.

Алгоритм 1. Вычисление ключа шифра с использованием продолжения многочленов Жегалкина.

Вход. Алгоритм шифрования, множество открытых текстов X_i , множество соответствующих шифрограмм Y_i .

Выход. Ключ шифрования.

Метод.

1. На первом этапе (производится однажды для каждого шифра) для разных известных ключей по известным открытым и зашифрованным текстам провести N циклов поиска максимума целевой функции (N определяется необходимой точностью расчета вероятностей) и построить для каждого бита аргумента матрицу (N_{ij}) , где N_{ij} - число вскрытия разряда ключа значением i , когда на самом деле разряд принимал значение j .
2. Для каждого разряда ключа вычислить z_{00} , z_{01} и Δz .
3. Для исследуемого ключа и различных открытых текстов и шифрограмм провести R (R определяется значением Δz) циклов алгоритма 1 и построить вектор R_0 вероятностей того, что разряд ключа вскрывается 0.
4. По R_0 для каждого разряда рассчитать v_0 .
5. Для каждого разряда сравнить рассчитанные вероятности. Если $v_0 = z_{00}$ — истинное значение разряда равно 0, если $v_0 = z_{01}$ — истинное значение разряда равно 1.
6. Опробовать ключи, начиная с наиболее вероятных, до выявления истинного значения. Результат: ключ, для которого результат шифрования данного открытого текста соответствует данной шифрограмме.

Особенность применения данного метода состоит в том, что в ходе анализа мы имеем дело не со всей генеральной совокупностью возможных значений ключей, а лишь с некоторой выборкой, поэтому вероятности z_{00} , z_{01} и v_0 можно рассчитать лишь приблизительно, используя свойства биномиального и нормального распределений можно с вероятностью 99,7% [3] заключить, что:

$$z_{00} = [z_{00}^l, z_{00}^h] \approx \left[\frac{N_{00}}{N_{00} + N_{10}} - \frac{3}{2\sqrt{N_{00} + N_{10}}}, \frac{N_{00}}{N_{00} + N_{10}} + \frac{3}{2\sqrt{N_{00} + N_{10}}} \right] \quad (3)$$

$$z_{01} = [z_{01}^l, z_{01}^h] \approx \left[\frac{N_{01}}{N_{11} + N_{01}} - \frac{3}{2\sqrt{N_{11} + N_{01}}}, \frac{N_{01}}{N_{11} + N_{01}} + \frac{3}{2\sqrt{N_{11} + N_{01}}} \right] \quad (4)$$

$$v_0 = [v_0^l, v_0^h] \approx \left[\frac{R_0}{R} - \frac{3}{2\sqrt{R}}, \frac{R_0}{R} + \frac{3}{2\sqrt{R}} \right] \quad (5)$$

Таким образом, выражения (3) и (4) позволяют определить объем вычислений на первом этапе алгоритма:

$$(N_{00} + N_{10}) \geq \frac{9}{4(\Delta z_{00})^2}, \quad N \geq \frac{9}{2(\Delta z_{00})^2},$$

где

$$\Delta z_{00} = \Delta z_{01} = \frac{3}{2\sqrt{N_{00} + N_{10}}}.$$

Для точного определения значения разряда необходимо чтобы отрезок $[v_0^l, v_0^h]$ пересекал одновременно только один из отрезков $[z_{00}^l, z_{00}^h]$, $[z_{01}^l, z_{01}^h]$. А это возможно в том

случае, если Δz - расстояние между отрезками $[z_{00}^l, z_{00}^h]$ и $[z_{01}^l, z_{01}^h]$ будет больше отрезка $[v_0^l, v_0^h]$, т.е. $v_0^h - v_0^l < \Delta z$, или $R > \frac{9}{\Delta z^2}$. Таким образом, Δz определяет трудоемкость вскрытия соответствующего разряда ключа.

Кроме того, в ходе экспериментов выяснилось, что в процессе одного цикла нахождения локального максимума вскрываются не все разряды ключа. В среднем каждый разряд ключа вскрывается один раз за два цикла нахождения локального максимума. Таким образом, для набора необходимой статистики нужно, чтобы

$$N \geq \frac{9}{(\Delta z_{00})^2} \text{ и } R > \frac{18}{\Delta z^2}.$$

Также можно использовать вариант метода, основанный на вероятностях вскрытия разрядов ключа единицей.

3. Криптоанализ шифра RIJNDAEL с тривиальным списком ключей

Для тестирования разработанного метода был проведен анализ американского стандарта шифрования RIJNDAEL[5] с длиной ключа 128 бит (другое название этого шифра — AES). RIJNDAEL представляет собой блочный шифр с длиной блока 128 бит. На каждом из 10 раундов выполняются следующие операции: подстановка (замена) байтов по одному и тому же правилу, линейная операция перемешивания (умножение текста как вектора на матрицу), сложение текста с раундовым ключом по модулю 2, получаемым по фиксированному правилу из исходного ключа. Подстановка обладает наилучшими криптографическими качествами для противостояния линейному и дифференциальному методам криптоанализа. Операции сложения, подстановки и перемешивания описываются в терминах конечного поля из 256 элементов, что обуславливает перспективность методов криптоанализа, основанных на использовании алгебраических структур над этим полем.

На сегодняшний день RIJNDAEL является очень стойким шифром. Стойкость его по отношению к наиболее популярным дифференциальному и линейному методам превышает сложность перебора ключей. Только в 2002 г. появились предпосылки для некоторого снижения стойкости этого шифра. Куртуа и Пепржик показали, что вскрытие ключа сводится к решению системы из нескольких тысяч квадратных уравнений над конечным полем характеристики 2 от примерно такого же числа неизвестных (XSL-метод, см. работу [6], который не является универсальным). Стойкость RIJNDAEL по отношению к этому методу составляет примерно 2^{100} .

Целью проведенных исследований являлась оценка стойкости RIJNDAEL по отношению к методу криптоанализа на основе продолжения полиномов Жегалкина до полиномов над полем рациональных чисел. Для упрощения программы на каждом раунде использовался один и тот же ключ.¹ Эксперимент заключался в выполнении первого этапа анализа — получении для каждого бита ключа вероятностей z_{00} и z_{01} , вычислении Δz , и дальнейшем определении R - трудоемкости вскрытия соответствующих разрядов ключа.

Проводилось N циклов нахождения локального максимума целевой функции. На каждом цикле использовались новый ключ и новая пара открытый текст-шифrogramма. Ключ и открытый текст выбирались случайным образом из всего множества возможных вариантов. Число N оценивалось предварительно в процессе планирования эксперимента на основе предполагаемой необходимой точности расчета вероятностей z_{00} и z_{01} . В процессе работы строилась матрица (N_{ij}) . Затем рассчитывались вероятности z_{00} и z_{01} . По этим

¹ По-видимому, такое упрощение шифра не должно существенно сказаться на оценке его стойкости. В пользу этого предположения говорят эксперименты с другими «небольшими» шифрами, для которых матрицы преобладаний не зависят от того, является ли шифр степенным.

значениям вычислялось Δz и, наконец, для каждого разряда ключа определялась сложность его вычисления R .

Поскольку анализ 10-раундового шифра RIJNDAEL — сложная задача, требующая большого количества вычислительных ресурсов, исследовались варианты этого шифра с уменьшенным числом раундов. Использование тривиального списка ключей в этом случае оправдывается тем, что он не затемняет итоговую картину зависимости сложности от числа раундов.

3.1 Анализ RIJNDAEL (AddRoundKey)

В первом эксперименте проводился анализ простой модификации AES, состоящей только из 1 операции сложения открытого текста с ключом. Ожидалось, что в этом эксперименте все разряды ключа всегда будут вскрываться правильно, так как соответствующая целевая функция не имеет локальных максимумов, отличных от решения задачи анализа. Данное предположение подтвердилось экспериментально: метод анализа безошибочно определял значения всех разрядов ключа.

3.2 Анализ RIJNDAEL (1 раунд)

После добавления операций перестановки, смешения колонок, сдвига рядов и сложения с ключом количество локальных максимумов целевой функции, не отвечающих задаче анализа должно было увеличиться, а эффективность метода соответственно снизится, поэтому необходимо было с большей точностью рассчитать используемые вероятности. $\Delta z_{00} = \Delta z_{01} = 0.025$, поэтому $N \geq 14400$.

Было проведено 17617 циклов. В результате эксперимента выяснилось, что для 8 разрядов $\Delta z > 0$. Наиболее легкими для вскрытия являются 7, 6, 5 разряды ключа.

Таблица 3.2.1 Результаты эксперимента для шифра RIJNDAEL (1 раунд)

Номер бита	z_{00}^l	z_{00}^h	z_{01}^l	z_{01}^h	Δz	R
7	0,318561	0,359017	0,509175	0,552133	0,15016	800
6	0,341005	0,381687	0,480027	0,523302	0,09834	1862
5	0,354044	0,395715	0,472486	0,515426	0,07677	3055
4	0,387216	0,428351	0,467912	0,509831	0,03956	11502
3	0,404587	0,445257	0,456201	0,497459	0,01094	150397
0	0,405653	0,446091	0,451957	0,492457	0,00587	522392
1	0,396625	0,437011	0,439078	0,479663	0,00207	4200799
2	0,399058	0,439939	0,440706	0,481489	0,00077	30359252

3.3 Анализ RIJNDAEL (2 раунда)

Дальнейшее усложнение целевой функции снижает эффективность разработанного метода, поэтому необходимо вычислять искомые величины с большей точностью. $\Delta z_{00} = \Delta z_{01} = 0.015$, поэтому $N \geq 40000$.

Было проведено 45400 циклов. В результате эксперимента выяснилось, что для 4 разрядов $\Delta z > 0$. Наиболее легкими для вскрытия являются 7, 6, 5 разряды ключа.

Таблица 3.3.1 Результаты первого этапа эксперимента для шифра RIJNDAEL (2 раунда)

Номер бита	z_{00}^l	z_{00}^h	z_{01}^l	z_{01}^h	Δz	R
7	0,42035	0,44417	0,47407	0,49807	0,02990	20135

6	0,42857	0,45269	0,46928	0,49353	0,01659	65401
5	0,43110	0,45534	0,46692	0,49142	0,01158	134232
1	0,44695	0,47090	0,47253	0,49668	0,00163	6778813

3.4 Прогноз результатов анализа RIJNDAEL с полным числом раундов

Как видно из результатов экспериментов, разработанный метод эффективен для одно-раундового и двухраундового RIJNDAEL. Заметим, что с прибавлением каждого нового раунда Δz уменьшалась примерно в одинаковое число раз. Если предположить, что такая же зависимость будет наблюдаться и для большего числа раундов, то можно спрогнозировать значения Δz и R для RIJNDAEL с полным числом раундов (10 раундов).

Таблица 3.4.1 Прогнозируемые значения Δz и R для RIJNDAEL с полным числом раундов

Номер бита	Δz	R
7	2^{-24}	2^{53}
6	2^{-25}	2^{55}
5	2^{-28}	2^{61}

4. Заключение

Таким образом, можно предположить, что значения как минимум 3 из 128 разрядов ключа RIJNDAEL с полным числом раундов вероятно можно вычислить не более чем за 2^{61} итераций с помощью нового метода анализа. При этом для вскрытия ключа достаточно небольшого числа открытых и соответствующих зашифрованных текстов. Для уточнения стойкости RIJNDAEL необходимо провести исследования для большего числа раундов, хотя бы для 3, 4, 5.

Для оценки того, насколько случайным является отображение, индуцированное шифром или хэш-функцией, используются статистические тесты. Традиционно используются автокорреляционный и спектральный тесты, строгий лавинный критерий и др. Однако эти тесты никак не связаны с природой исследуемого отображения, поэтому их использование трудно объяснить иначе как данью традициям. Предлагаемый метод криптоанализа можно интерпретировать как универсальный статистический тест, тесно связанный с природой исследуемого отображения, индуцированного шифром.

Многочисленные эксперименты показывают, что этот тест позволяет выявлять закономерности, присущие шифру, лучше, чем большинство других статистических тестов. Несимметричное распределение (N_{ij}) позволяет модифицировать метод криптоанализа и использовать другие варианты атак для вскрытия ключа после получения матриц (N_{ij}) . Поэтому первый и второй этапы данного метода можно рекомендовать в качестве статистического теста для блочных шифров и хэш-функций.

ЛИТЕРАТУРА

1. **Biham E., Shamir A.** Differential cryptanalysis of DES-like cryptosystems // Advances in Cryptology — CRYPTO '90. LNCS. Springer-Verlag. 1991. V. 537. P. 2–21.
2. **Matsui M.** Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT '93. 1994. LNCS. Springer-Verlag. V. 765. P. 386–397.
3. **Andelman D., Reeds J.** On the cryptanalysis of rotor machines and substitution-permutation networks // IEEE transactions on information theory. 1982. V. IT-28. P. 578–584.

4. **Ростовцев А. Г., Маховенко Е. Б.** Введение в теорию итерированных шифров. — СПб.: Мир и Семья, Интерлайн, 2003.
5. National Institute of Standards and Technology (NIST). FIPS Publication 197: Advanced Encryption Standard (AES). Nov. 2001.
6. **Courtois N, Pieprzyk J.** Cryptanalysis of Block Ciphers with Overdefined Systems of Equations; in Asiacrypt 2002, LNCS 2501, pp. 267-287, Springer.