УДК 681.0.245

Л.К. Бабенко, Е.А. Ищукова

ПРИНЦИПИАЛЬНЫЕ ОСОБЕННОСТИ ПРОВЕДЕНИЯ ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА БЛОЧНЫХ ШИФРОВ*

Статья посвящена ключевым моментам проведения атаки на блочные алгоритмы шифрования с использованием метода дифференциального криптоанализа. Даны основные определения, широко используемые при описании рассматриваемого метода. Подробно рассмотрена возможность проведения атаки для шифра, усеченного для трех раундов.

Блочный шифр; секретный ключ; дифференциальный криптоанализ; дифференциал; входная разность; выходная разность.

L.K. Babenko, E.A. Ischukova

MAIN FEATURES OF DIFFERENTIAL CRYPTANALYSIS OF BLOCK CIPHERS

The article is devoted to key moments of carrying out of attack to block ciphers using the differential cryptanalysis. The basic definitions widely used at the description of the considered method are given. Possibility of carrying out of attack to 3-rounds cipher is in detail considered.

Block cipher; secret key; differential cryptanalysis; differential; input difference; output difference.

Теория информации в современном понимании получила начало своего развития с работы Огюста Кергоффса «Военная криптография», опубликованной в 1883 году. Позднее Клод Шеннон в своей работе «Теория связи в секретных системах» [1], опубликованной в 1949 году, сформулировал необходимые и достаточные условия недешифруемости системы шифрования. Долгое время криптография оставалась секретной наукой, в тайны которой был посвящен лишь узкий круг лиц. В первую очередь она была направлена на сохранение государственных секретов. Ситуация стала меняться во второй половине XX века с появлением персональных компьютеров. Когда практически каждый человек получил возможность оперировать электронной информацией, возникла естественная потребность защищать эту информацию от посторонних. Широкое распространение получило использование симметричной криптографии, а несколько позднее и асимметричной. В 1976 году в США был утвержден стандарт шифрования данных DES (Data Encryption Standard) [2], который применялся довольно длительное время (более 20 лет). При использовании криптоалгоритмов возникает необходимость проверки их стойкости к различным типам атак на шифрованные данные с целью получения ключа или исходного текста. Одним из блочных алгоритмов шифрования наиболее часто подвергавшимся различного рода атакам является DES. Именно для анализа этого алгоритма шифрования были разработаны такие мощные атаки как линей-

* Работа поддержана грантом РФФИ № 09-07-00245-а.

ный и дифференциальный криптоанализ, которые в дальнейшем стали применяться к целому классу блочных шифров.

Современные алгоритмы блочного шифрования разрабатываются таким образом, чтобы аналитик имел как можно меньше шансов отыскать секретный ключ, с помощью которого были зашифрованы данные, даже если ему известен сам алгоритм шифрования и есть в наличии несколько текстов и соответствующих им шифротекстов. Приступая к задаче анализа, первым делом аналитик определяет тот набор данных, который ему изначально известен для анализа. Так, если известен алгоритм шифрования и есть хотя бы одна пара открытый – шифрованный текст, то самым естественным способом анализа является последовательное опробование всех возможных вариантов ключа, которые могли быть использованы. Опробование производят до тех пор, пока зашифрование открытого текста на очередном ключе не приведет к получению имеющегося шифрованного сообщения. Такой способ анализа в разных источниках литературы имеет разные названия: «Метод полного перебора» [3], «Метод грубой силы» [4] или «Метод атаки в лоб» [2] или «Brut-force атака» [4]. У этого метода есть одно неоспоримое преимущество: рано или поздно искомый ключ будет найден и для этого будет необходим минимальный набор данных. Быстрота нахождения ключа будет зависеть от длины используемого секретного ключа и от вычислительной мощности, которая имеется в распоряжении аналитика. А также от удачи. Ведь может случиться так, что искомый ключ встретится одним из первых. В работе [3] достаточно подробно описано, как оценивать сложность подобного рода анализа.

Вместе с тем известно, что одним из важных свойств информации является ее своевременность. Поэтому применение метода полного перебора не всегда удовлетворяет практическим требованиям. Ведь даже сегодня провести полный перебор секретных ключей для алгоритма DES (необходимо сделать 2^{56} опробований) за один день весьма проблематично. В связи с тем, что вычислительная мощность с каждым днем неумолимо растет, стандарт DES был заменен на новый стандарт AES (Advanced Encryption Standard), где длина секретного ключа возросла до 128 бит. Так или иначе, в криптографии принято считать время анализа с помощью метода полного перебора эталонным. Это значит, что если аналитику удастся провести анализ алгоритма шифрования быстрее, чем это можно сделать с помощью полного перебора, то данный алгоритм шифрования будет считаться уязвимым и использовать его для шифрования данных нецелесообразно.

Предложенные в начале 90-х годов прошлого века два способа статистического анализа алгоритма шифрования DES позволили осуществлять атаку быстрее, чем это можно было бы сделать с помощью метода полного перебора. Метод линейного криптоанализа (linear cryptanalysis) был предложен японским ученым М. Матсуи [5] и позволял проводить анализ путем опробования 2^{47} пар текстов, зашифрованных на одном секретном ключе. Сразу следует отметить, что хоть степенной показатель в количестве опробований сократился со значения 56 до значения 47, здесь возникло условие, практически невыполнимое – наличие огромного объема информации, зашифрованной на одном и том же ключе. Метод дифференциального криптоанализа (differential cryptanalysis) был предложен Э.Бихамом и А.Шамиром [6, 7]. С помощью этого метода сложность анализа сократилась до 2^{37}. Однако опять же, для проведения анализа необходимо было иметь 2^{37} особым образом подобранных текстов, зашифрованных на одном и том же секретном ключе. Дальнейшее развитие этих методов показало возможность их применения к целому классу блочных шифров, позволило выявить слабые места других используемых алгоритмов шифрования. Сегодня оба эти метода, а также некоторые их усо-

вершенствования, например, линейно-дифференциальный метод, метод невозможных дифференциалов, широко используются для оценки стойкости вновь создаваемых шифров.

Название «дифференциальный криптоанализ» содержит английское слово difference - разность. Авторы этого метода предложили рассматривать не отдельные тексты, а пары текстов, имеющих различия в некоторых позициях. Для того чтобы определить это различие, достаточно пару текстов сложить между собой по модулю два. Результат даст на выходе значение 0 в тех позициях, в которых исходные тексты были равны между собой, и значение 1 в тех позициях, в которых исходные тексты отличались. Например, два 4-битовых сообщения X = 0011 и X' = 1010 в результате сложения дадут $\Delta X = 1001$. Значение ΔX принято называть дифференциалом или разностью. Полученная разность показывает, что во второй и третьей позициях исходные сообщения X и X' были равны, а в первой и четвертой отличались друг от друга. Заметим, что и для рассматриваемых нами алгоритмов шифрования, и для рассматриваемых сообщений нумерация позиций битов ведется слева направо от единицы, в отличие, например, от машинного представления двоичной информации, когда самый младший бит находится справа и отсчет ведется от нуля.

За счет каких механизмов становится возможным провести анализ, рассматривая не сами сообщения, а их различия? Рассмотрим процесс преобразования разностей при их прохождении через функцию F, например, некоторого Учебного алгоритма шифрования (см. рис. 1). Будем считать, что на вход рассматриваемой функции F поступает два независимых сообщения XR и XR' (R обозначает правую часть сообщения X, поступающего на вход раунда шифрования), разность которых равна ΔXR. Первое преобразование, которому будут подвергнуты сообщения XR и XR' – это перестановка с расширением (E-перестановка). Так как таблица, в соответствии с которой работает перестановка с расширением, известна, то легко можно определить значения E(XR) и E(XR'), которые появятся на выходе этой перестановки. Значит, можно определить, чему будет равно значение разности на выходе E-перестановки. Обозначим это значение разности как ΔA, тогда получим: $\Delta A = E(XR) \oplus E(XR')$.

В результате сложения данных, полученных на выходе перестановки с расширением с секретным раундовым подключом K_i первый выход (для исходного значения XR) станет равен $E(XR) \oplus K_i$, а второй выход (для исходного значения XR') станет равен $E(XR') \oplus K_i$. Разность текстов после операции сложения с подключом обозначим как ΔB.

$$\Delta B = E(XR) \oplus K_i \oplus E(XR') \oplus K_i = E(XR) \oplus E(XR') = \Delta A.$$

Из этого видно, что значение разности после операции сложения с секретным подключом остается таким же, каким оно было до этой операции. Это связано с тем, что оба сообщения XR и XR' зашифровываются на одном и том же секретном ключе, а это значит, что в одном и том же раунде значение секретного подключа K_i будет одинаковым как для сообщения XR, так и для сообщения XR'. Результат сложения двух одинаковых сообщений по модулю два равен нулю. Таким образом, получается, что операция сложения данных с секретным подключом **изменяет сами сообщения**, но при этом **не оказывает влияния на разность** этих сообщений.

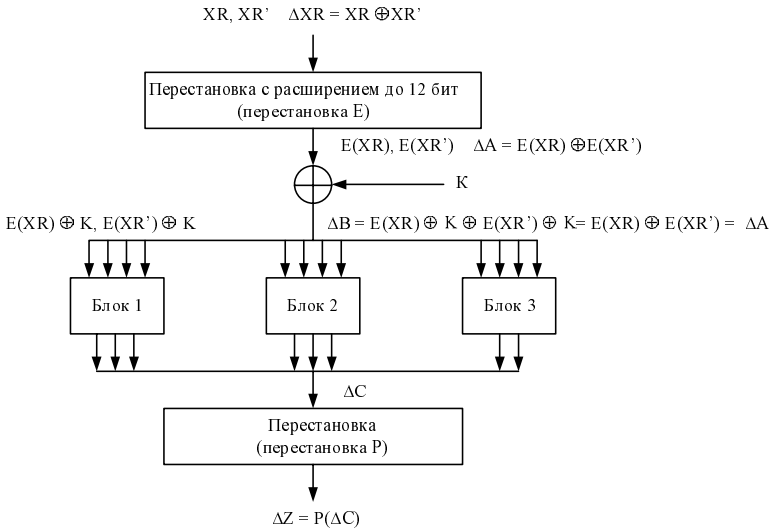

Рис. 1. Преобразование разности текстов при прохождении через функцию F учебного алгоритма шифрования

После сложения с секретным подключом данные поступают на вход трех блоков замены по четыре бита на каждый блок. Так как секретный ключ неизвестен, не возможно знать, какие именно значения поступают на вход блоков замены, однако их разность известна и равна ΔA. Блоки замены организованы таким образом, что, зная разность на входе в блок замены (входная разность), нельзя точно сказать, какая разность появится на выходе этого блока (выходная разность). Однако путем анализа блока замены, можно выявить, какая выходная разность будет наиболее вероятной.

Последним преобразованием является P-перестановка. Так как таблица, в соответствии с которой выполняется перестановка, известна, то легко можно преобразовать значение разности ΔC на входе P-перестановки к значению разности ΔZ на выходе этой перестановки, то есть на выходе преобразования функции F.

Таким образом, в результате рассмотрения прохождения разности двух текстов через преобразование функции F можно определить наиболее вероятную разность, которую мы ожидаем получить на выходе этого преобразования.

По условию проведения анализа, два сообщения, поступающие на вход некоторого преобразования (будь то отдельно взятый блок замены, или некоторая функция F, либо же алгоритм шифрования целиком) обрабатываются с помощью одних и тех же криптографических преобразований с участием одного и того же секретного ключа. Поэтому одно и то же входное сообщение X, при его зашифровании, всегда будет на выходе давать одно и то же значение Y. А это означает, что если входная разность двух сообщений в некотором криптографическом преобразовании равна нулю, то и выходная разность **всегда**, то есть с вероятностью p = 1, будет равна нулю (рис. 2). Это важное свойство широко используется при дифференциальном криптоанализе блочных шифров.

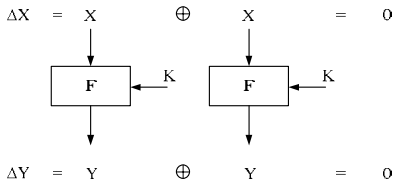

Рис. 2. Преобразование разности, равной нулю

Теперь рассмотрим целиком один раунд зашифрования. Для этого обратимся к рис. 3. На этом рисунке представлена общая схема прохождения разности пары текстов через один раунд шифрования.

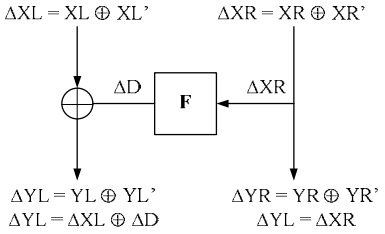

Рис. 3. Общая схема преобразования разности для одного раунда

Будем считать, что на вход алгоритма поступает некоторое значение X, которое разделяется на две равные части XL (левую часть) и XR (правую часть). Таким же образом выходное шифрованное значение Y образуется двумя составными частями YL (левой половиной) и YR (правой половиной) шифрованного сообщения. Кроме того, при изображении одного раунда шифрования будем опускать перестановку правой и левой части местами, так как она отсутствует в последнем раунде шифрования. Если рассматриваемый раунд не является последним, то прежде чем перейти к рассмотрению следующего раунда необходимо будет правую и левую часть сообщения поменять местами.

Из рис. 3 видно, что на вход раунда шифрования поступает некоторое сообщение X = (XL, XR) и сообщение X' = (XL', XR'). При этом левые половины сообщений образуют разность ΔXL, а правые половины – соответственно разность ΔXR. Значение разности ΔXR поступает на вход функции F. Ранее было показано, что путем анализа составляющих компонентов функции F можно предположить наиболее вероятное значение разности на выходе. На рис. 3 наиболее вероятное значение выходной разности обозначено как ΔD. Так как известно значение левой части входной разности ΔXL и известно наиболее вероятное значение разности на выходе из функции F – ΔD, то легко можно вычислить наиболее вероятное значение левой части выходной разности рассматриваемого раунда шифрования ΔYL: ΔYL = ΔXL ⊕ ΔD, а правая часть выходной разности рассматриваемого раунда шифрования ΔYR будет соответствовать правой части входной разности ΔXR, то есть: ΔYR = ΔXR.

Таким образом, можно проследить изменение разности пары текстов при рассмотрении отдельно взятого раунда шифрования. Рассмотрим еще один вариант для прохождения некоторого значения разности через один раунд шифрования. Для этого обратимся к рис. 4. Здесь, как и на рис. 3, на вход раунда шифрования

поступает пара текстов X и X', каждый из которых разделяется на две половины. Правая часть входных текстов образует разность ΔXR, которая поступает на вход F-функции шифрования. Путем анализа F-функции можно предположить наиболее вероятное значение разности на выходе этой функции. На рис. 4, как и на предыдущем рисунке, это значение также обозначено как ΔD. Можно подобрать входные сообщения X и X' таким образом, чтобы разность их левых частей, то есть входная разность ΔXL была равна значению ΔD: ΔXL = ΔD. Это можно сделать только в том случае, если рассматриваемый раунд шифрования является первым, когда существует возможность перебирать значения X и X'. В этом случае наиболее вероятным событием будет то, что в результате сложения левой части входной разности (ΔXL = ΔD) и наиболее вероятного выхода функции F (ΔD), левая часть выходной разности рассматриваемого раунда шифрования будет равна нулю: ΔYL = ΔXL ⊕ ΔD = 0.

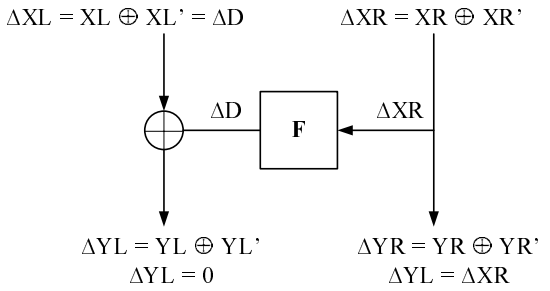

Рис. 4. Возможное преобразование разностей для одного раунда шифрования

Такой вариант прослеживания преобразования разности пары текстов может быть очень полезен при рассмотрении анализа алгоритма, состоящего из нескольких раундов шифрования.

Рассмотрим еще один вариант возможного прохождения пары разностей через один раунд шифрования. Для этого обратимся к рис. 5. Как видно из рисунка, на вход данного раунда шифрования поступает пара текстов, у которой правые части равны между собой, а значит, что их разность равна нулю (ΔXR = 0). Ранее, (рис. 2), было показано, что разность равная нулю при прохождении через любое криптографическое преобразование всегда на выходе дает значение разности, равное 0. Поэтому со 100 %-ной гарантией можно сказать, что на выходе функции F одного раунда шифрования, показанного на рис. 5, появится значение разности, равное нулю (ΔD = 0). Это позволяет сказать, что в данном случае раундовое преобразование не повлияет на изменение входной разности при ее прохождении через рассматриваемый раунд шифрования.

Введем несколько определений, характерных для метода дифференциального криптоанализа, которыми мы будем оперировать в дальнейшем. Для наглядности используем рис. 6.

Характеристика – это пара дифференциалов, один из которых образован входными значениями некоторого преобразования, а второй – выходными значениями этого же преобразования. Дифференциал на входе преобразования также часто называют ***входной разностью***, а дифференциал на выходе преобразования – ***выходной разностью***.

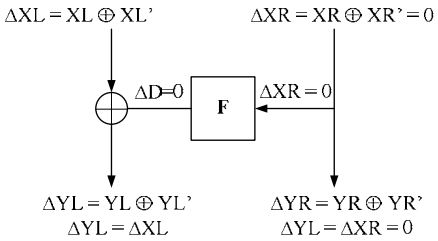

Рис. 5. Преобразование разности, равной нулю

Раундовая характеристика – это пара дифференциалов, один из которых образован входными значениями раунда шифрования, а второй – выходными значениями того же раунда.

Вероятность характеристики – это вероятность, с которой выходная разность характеристики будет получена для заданной входной разности характеристики.

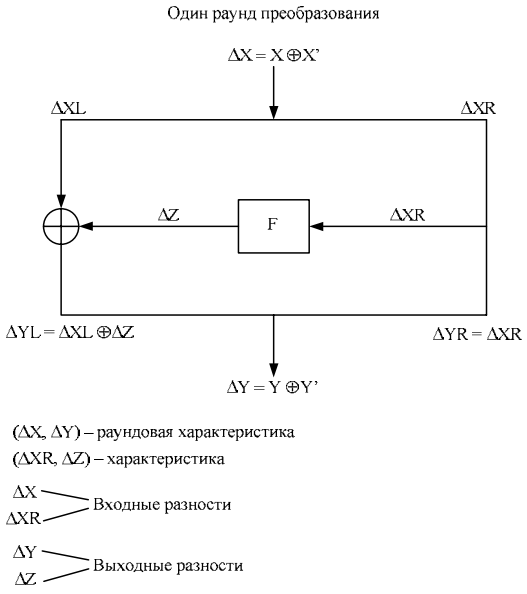

Рис. 6. Основные значения дифференциального криптоанализа

Теперь можно рассмотреть построение характеристики для алгоритма шифрования, состоящего из трех раундов. Проиллюстрируем рис. 7. Прохождение разностей через первый раунд шифрования организовано подобно тому, как это показано на рис. 4. На вход алгоритма шифрования подаётся пара текстов X и X', у которых правые части образуют разность ΔXR. При этом разность ΔXR должна быть подобрана так, чтобы вероятность характеристики (ΔXR, ΔD) была максимальной. Левые части сообщений X и X' при этом необходимо подобрать таким образом, чтобы они образовывали значение разности ΔD.

В таком случае можно ожидать, что на вход функции F второго раунда шифрования поступит значение разности, равное нулю. В таком случае на выходе функции F второго раунда появится значение разности, равное нулю. Выход функции F второго раунда сложится по модулю 2 со значением ΔXR (это хорошо видно на рис. 7), в результате чего на вход функции F третьего раунда шифрования поступит известное значение разности, равное ΔXR. На рис. 7 разность на выходе функции F третьего раунда обозначена как Δv, а не ΔD, как раньше. Это связано с определением значения вероятности характеристики. Пусть в первом раунде было определено, что значение разности ΔXR преобразуется к значению разности ΔD при прохождении через функцию шифрования F с некоторой вероятностью $\mathbf{p_1}$. Для второго раунда шифрования известно, что вероятность преобразования нулевой разности равна $\mathbf{p_2} = 1$. Для третьего раунда шифрования не важно, какая разность появится на выходе функции F. Это связано с тем, что левая часть входной разности третьего раунда шифрования равна нулю (ΔG = 0). Это значит, что левая часть разности на выходе алгоритма шифрования ΔYL будет равна разности, полученной на выходе функции F третьего раунда шифрования Δυ, так как: $\Delta YL = \Delta G \oplus \Delta\upsilon = 0 \oplus \Delta\upsilon = \Delta\upsilon$.

В связи с этим любое возможное значение разности на выходе F-функции третьего раунда шифрования обозначается как Δv, и считается, что для третьего раунда вероятность преобразования разности равна $\mathbf{p_3} = 1$, так возможно получение любого из возможных значений разности на выходе функции F третьего раунда шифрования.

Итак, внимательно рассмотрев рис.7, можно сказать, что для приведенных трех раундов шифрования характеристика будет иметь следующий вид: входная разность, образованная парой (ΔXL=ΔD, ΔXR); выходная разность, образованная парой (Δv, ΔXR). Известно три вероятности преобразования разностей для каждого из рассмотренных раундов шифрования, поэтому для того, чтобы определить вероятность рассмотренной 3-раундовой характеристики, необходимо эти вероятности перемножить между собой. В этом случае мы получим:

$$p = p_1 * p_2 * p_3 = p_1.$$

Для того чтобы оценить сложность предстоящего анализа, необходимо знать вероятность характеристики, которая определяет необходимое количество пар текстов, подлежащих перебору для нахождения пары открытый – закрытый текст, которая будет удовлетворять заданной характеристике.

Так как анализ выполняется с некоторой вероятностью, то это значит, что далеко не все пары текстов, которые можно рассмотреть, будут преобразовываться в соответствии с тем, как это показано на рис. 7. Из всего многообразия возможных пар текстов необходимо отобрать только такие, которые будут удовлетворять заданной характеристике. Пусть на вход рассматриваемого трехраундового алгоритма шифрования поступают два сообщения X и X', каждое из которых разделяется на две половины: X = (XL, XR) и X’ = (XL’, XR’). Эти два сообщения дают в результате сложения по модулю два значения разности ΔX = (ΔXL, ΔXR). Первым делом необходимо подобрать входную пару текстов таким образом, чтобы ΔXR при прохождении через функцию F давало наиболее вероятное (по сравнению со всеми остальными возможными значениями входной разности) значение разности на выходе F-функции. Кроме того, левые части текстов X и X' должны образовывать разность, равную значению ΔD. После того, как подбор входных текстов завершен, необходимо получить соответствующие им шифротексты, также состоя-

щие из двух частей: Y = (YL, YR) и Y' = (YL', YR'). При проведении анализа считается, что аналитик имеет возможность получать зашифрованные на некотором секретном ключе сообщения с помощью исследуемого алгоритма шифрования. При этом ключ шифрования аналитику неизвестен, он должен быть найден в результате анализа. После того как шифротексты будут получены, необходимо рассмотреть, чему равна разность их правых половин ΔYR. В соответствии с рассмотренной характеристикой разность ΔYR должна совпадать со значением правой части входной разности ΔXR, то есть должно выполняться условие:ΔYR = ΔXL.

Если это условие выполняется, то можно считать, что рассмотренные открытые тексты X и X', и соответствующие шифротексты Y и Y' удовлетворяют условиям заданной характеристики и пригодны для дальнейшего анализа. Такие тексты в рамках дифференциального криптоанализа принято называть ***правильной парой текстов***. Найденные правильные пары текстов предназначены для дальнейшего анализа с целью нахождения секретного ключа шифрования. Следует отметить, что в рассматриваемой схеме преобразования разностей можно провести анализ только первого и последнего раундов шифрования, а значит найти секретные подключи первого и третьего раундов: соответственно K_1 и K_3. Второй раунд шифрования исключается из анализа, так как на вход F-функции этого раунда поступает значение разности, равное нулю, что не позволяет исключать неправильные значения секретного подключа.

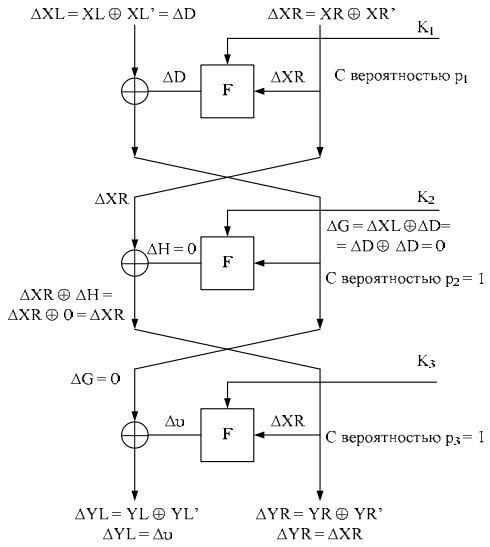

Рис. 7. Анализ трех раундов шифрования

Анализ первого и третьего раундов будет выполняться по одной и той же схеме. В первую очередь необходимо определить значения, которые поступают на вход функции F и появляются на выходе этой функции. Рассмотрим первый раунд шифрования. Известно, что на вход функции F поступает два сообщения: соответственно XR и XR', имеющие разность ΔXR. Какие сообщения появляются на выходе функции F, мы не знаем, но мы предполагаем, что их разность равна значению ΔD, так как рассматриваемые нами пары текстов являются правильными. Теперь соотнесем данные, которые нам известны с тем, как эти данные будут преоб-

разовываться при прохождении через F-функцию. Для этого несколько преобразуем рис. 1 так, как это показано на рис. 8.

Из рис. 8 видно, что, проходя через криптографические преобразования функции F сверху вниз, мы можем определить значение $\Delta B = \Delta A$ на входе S-блоков замены, а также непосредственно значения E(XR) и E(XR'). Неизвестным только остается значение ключа K_1. Проходя через криптографические преобразования функции F в обратном порядке, мы можем получить значение разности ΔC на выходе S-блоков замены. Для этого к известному нам значению разности ΔD необходимо применить преобразование, обратное перестановке P. На рис. 8 такое преобразование обозначено как P^{-1}. Важно отметить, что в данном случае не известно, какими именно значениями была образована разность ΔC, так как не известны сами значения выходов функции F.

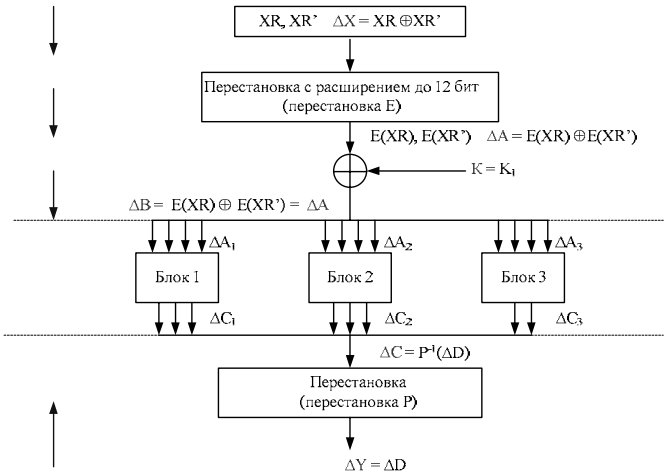

Рис. 8. Анализ первого раунда шифрования

Известно, что некоторое значение ΔA может быть образовано 2^n способами, где n – число бит, составляющих значение ΔA. Будем считать, что разность, как и сами тексты, можно разделить на составные части, соответствующие каждому из блоков замены. Так как в рассматриваемом примере задействовано три S-блока замены, то, соответственно, необходимо рассмотреть три входные разности ΔA_1, ΔA_2 и ΔA_3 и соответствующие им три выходные разности ΔC_1, ΔC_2 и ΔC_3. В ходе анализа необходимо перебрать все возможные варианты возможного образования разности ΔA_j, где j – номер рассматриваемого S-блока замены, и отобрать только те из них, которые при прохождении через блок замены будут давать на выходе известное значение разности ΔC. На рис. 9 показано соответствие текстов для искомых значений ΔA и ΔC.

Для каждой такой пары текстов необходимо определить возможное значение секретного ключа. Это легко сделать, так как известно, что на вход блоков замены поступает два возможных значения: $E(XR) \oplus K_1$ и $E(XR') \oplus K_1$. Поэтому для определения возможного значения подключа необходимо решить уравнения:

$$E(XR) \oplus K_1 = X\_Text1; \qquad E(XR') \oplus K_1 = X\_Text2.$$

Или, если записать иначе, получим:

$$K_1 = E(XR) \oplus X\_Text1; \qquad K_1 = E(XR') \oplus X\_Text2.$$

Анализ одной правильной пары текстов позволит получить несколько возможных значений для секретного подключа первого раунда K_1. Анализ следующей правильной пары текстов позволит также определить несколько возможных значений для секретного подключа первого раунда K_1. Анализ необходимо проводить до тех пор, пока один из подключей не начнет встречаться чаще остальных – это и будет искомый подключ.

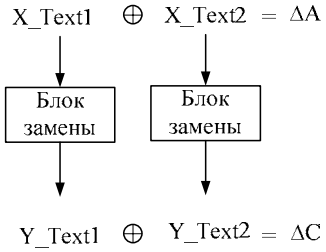

Рис. 9. Соответствие текстов для искомых значений ΔA и ΔC

Анализ третьего раунда шифрования будет сходен с анализом первого за тем исключением, что необходимо будет рассматривать другие данные. Так, на вход функции F третьего раунда шифрования будут поступать два сообщения, соответствующие правым частям известного шифротекста: YR и YR'. А на выходе функции F будет ожидаться разность, соответствующая значению разности ΔYR. Необходимо помнить, что нельзя сказать, какие именно сообщения появятся на выходе функции F третьего раунда шифрования, можно лишь предположить значение разности на выходе этой функции. Это связано с тем, что выход функции F третьего раунда шифрования складывается по модулю два с данными, которые поступали на вход функции F второго раунда шифрования. Согласно рассмотренной схеме, приведенной на рис. 7, на вход функции F поступают тексты, разность которых равна нулю, но при этом сами тексты, которые образуют эту разность, совсем не обязательно будут равны нулю. Именно поэтому они оказывают влияние на выходные значения третьего раунда шифрования, оставляя при этом неизменным значение разности ΔYL.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Шеннон К.* Теория связи в секретных системах [Электронный ресурс] / Режим доступа: http://www.enlight.ru/crypto/articles/shannon/shann__i.htm – свободный. – 11.09.2009.

2. *Шнайер Б.* Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.:ТРИУМФ. – 2002. – С. 648.

3. *Грушо А.А., Применко Э.А., Тимонина Е.Е.* Анализ и синтез криптоалгоритмов: курс лекций. – Йошкар-Ола, 2000. – 78 с.

4. *Панасенко С.* Алгоритмы шифрования. Специальный справочник. – СПб.:БХВ-Петербург, 2009. – 576 с.

5. *Matsui M.*, Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology – EUROCRYPT'93, Springer-Verlag, 1998. –386 p.

6. *Biham E., Shamir A.*, Differential Cryptanalysis of the Full 16-round DES, Crypto'92, Springer-Velgar, 1998. – P. 487

7. Biham E., Shamir A., Differential Cryptanalysis of DES-like Cryptosystems, Extended Abstract, Crypto'90, Springer-Velgar, 1998. – P. 2.

Бабенко Людмила Климентьевна
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: blk@fib.tsure.ru.
347928, г. Таганрог, ул. Чехова, 2, корпус "И".
Тел.: 8 (8634) 312-018.
Кафедра безопасности информационных технологий; профессор.

Babenko Lyudmila Klimentevna
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: blk@fib.tsure.ru.
Block “I”, 2, Chehov str., Taganrog, 347928, Russia.
Phone: 8 (8634) 312-018.
The Department of Security of Information Technologies; professor.

Ищукова Евгения Александровна
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: jekky82@mail.ru.
347928, г. Таганрог, ул. Чехова, 2, корпус "И".
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; доцент.

Ischukova Evgeniya Aleksandrovna
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: jekky82@mail.ru.
Block “I”, 2, Chehov str., Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
The Department of Security of Information Technologies; associate professor.

УДК 681.03.245

Л.К. Бабенко, Е.А. Ищукова

ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ ПОТОЧНЫХ ШИФРОВ*

Рассмотрены основные моменты анализа поточных алгоритмов шифрования с использованием метода дифференциального криптоанализа на примере алгоритма A5/1. Предложена методика проведения дифференциального анализа шифра A5/1, а также других шифров, имеющих сходное строение.

Поточные шифры; дифференциальный криптоанализ; регистр сдвига с обратной линейной связью.

* Работа поддержана грантом РФФИ № 09-07-00245-а.