УДК 004.045; 004.773

А.М. РОМАНЧЕНКО

МЕТОД ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КРИПТОАНАЛИЗА БЛОЧНОГО ШИФРА

Романченко А.М. **Метод оценивания результатов криптоанализа блочного шифра.**
Аннотация. Данная работа направлена на разработку метода численного оценивания криптостойкости блочного шифра к различным методам криптоанализа при заданных ограничениях. Его использование позволяет сравнивать криптостойкость разных шифров и быстро определять возможность их взлома на практике.
Ключевые слова: блочные шифры, криптоанализ, оценивание криптостойкости.

Romanchenko A.M. **The method of Evaluation of the Results of a Block Cipher Cryptanalysis.**
Abstract. This work aims to develop a method of numerical estimation of the reliability block cipher cryptanalysis to various methods under given constraints. Its use allows you to compare different cryptographic ciphers and quickly determine the possibility of breaking into practice.
Keywords: block ciphers, cryptanalysis, evaluation of cryptographic ciphers.

1. Введение. Криптографические алгоритмы являются неотъемлемой частью информационно-телекоммуникационных систем, в том числе и специального назначения. При этом анализ уязвимостей таких систем связанных с использованием криптографических алгоритмов - это важнейшая составляющая безопасности в информационной сфере. Любая уязвимость, связанная с криптографическими алгоритмами, может стать важным преимуществом для одной из сторон и потенциально способна привести к утечке информации ограниченного распространения.

Все уязвимости, связанные с использованием криптографических алгоритмов, можно разделить на несколько классов. Этими классами являются:

– уязвимости связанные с криптостойкостью используемых алгоритмов шифрования;

– уязвимости связанные с некорректным использованием(реализацией) алгоритмов;

– уязвимости криптографических сетевых протоколов.

Первые два класса уязвимостей реализуются на практике путем проведения криптоанализа используемых алгоритмов, а третий, кроме криптоанализа, включает в себя контроль среды передачи данных и оказание активных воздействий на информационную систему.

Одними из наиболее значимых являются уязвимости связанные с криптостойкостью блочных шифров. Исходными данными проведения криптоанализа блочного алгоритма шифрования является его спецификация. Зная алгоритм шифрования, данные для проверки

работоспособности модели можно сгенерировать самостоятельно. Результатом криптоанализа являются частные модели алгоритма шифрования (математические, вероятностные и т. п.), соответствующие конкретным методам и их параметры, на основе которых можно сделать вывод о реализуемости этого метода криптоанализа на практике. Наиболее существенными параметрами модели является объем и вид исходных данных, а также объем вычислительных ресурсов, требуемых для проведения криптоанализа. Практическую значимость произвольного метода криптоанализа с точки зрения объема исходных данных и объема вычислений можно оценить с помощью графика см. рисунок 1.

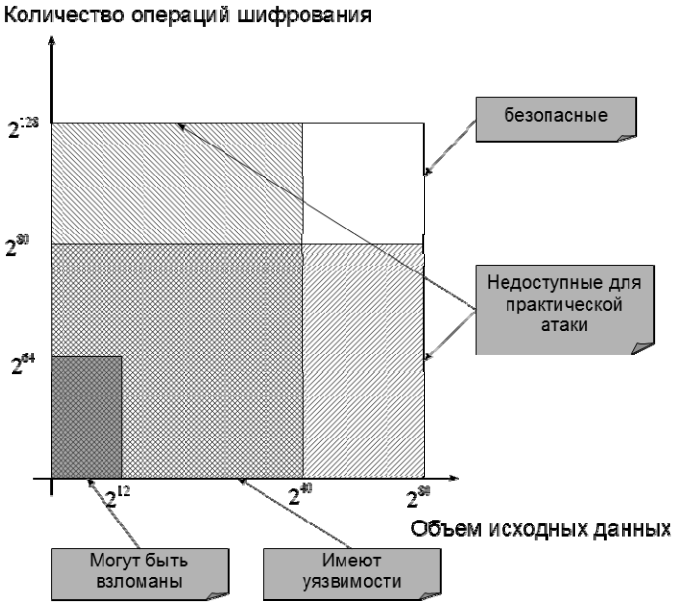

Рис. 1. Оценивание практической применимости различных методов криптоанализа

В данной работе предлагается комплексный подход к оцениванию криптостойкости блочных шифров с использованием обобщенного показателя криптостойкости. Преимуществом этого подхода является отражение криптостойкости алгоритма к нескольким методам криптоанализа с помощью одного числового показателя. Это дает возможность сравнительного анализа характеристик различных алгоритмов и быстрого оценивания их криптостойкости.

2. Оценивание результатов криптоанализа блочных шифров с использованием обобщенного показателя криптостойкости. Предлагается при оценивании криптостойкости произвольного блочного шифра использовать следующие методы криптоанализа:

– дифференциальный криптоанализ [4,7] и его разновидности если они дают результат лучше чем классический дифференциальный криптоанализ;

– линейный криптоанализ [5,6,7] и его разновидности если они дают результат лучше чем классический линейный криптоанализ;

– интегральный криптоанализ [8];

– алгебраический криптоанализ [9,10];

– метод полного перебора.

Предлагается в общем случае не использовать в составе обобщенного показателя криптостойкости результаты технических методов криптоанализа, так как в современных условиях эту атаку практически невозможно провести на практике – аппаратура шифрования, как правило, удалена от местонахождения криптоаналитика и какое-либо воздействие на нее не представляется возможным.

Результаты проведения криптоанализа блочных алгоритмов шифрования целесообразно представлять в форме обобщенного показателя криптостойкости. Обобщенный показатель стойкости формируется следующим образом:

$$F_{\Sigma} = \sum_{i=1}^{s} f_i(W, N, P_d)\,;\; F_{\Sigma} < F_d,$$

где f_i является функцией, характеризующей стойкость БШ к одному виду криптоанализа при заданных ограничениях количества исходных тестов W, количества вычислительных ресурсов N (выраженного в числе операций шифрования/расшифрования), и заданной вероятности вскрытия алгоритма шифрования при этих ограничениях. Количество методов криптоанализа, использованных в методике, обозначено как s. Функция f_i вычисляется как:

$$f_i(W, N, P_d) = \begin{cases} 0, \forall\, W, N\ P_{W,N} < P_d \\ 1, P_{W,N} \geq P_d \\ \dfrac{P_d}{\left(1 + \dfrac{\acute{W}}{W}\right)\left(1 + \dfrac{\acute{N}}{N}\right)}, P_{W,N} < P_d, \exists \acute{W}, \acute{N}\colon P_{\acute{W}\acute{N}} \geq P_d \end{cases},$$

т.е. она принимает значение 0 если при любых ограничениях вероятность успешной атаки меньше заданной вероятности P_d,

значение 1 если при заданных ограничениях вероятность успешной атаки больше или равна заданной вероятности. Если существуют такие условия, при которых вероятность успешной атаки больше или равна заданной вероятности, то значение функции вычисляется как отношение заданной вероятности к отношению количества требуемых исходных данных и имеющихся исходных данных, и отношению требуемых и имеющихся вычислительных ресурсов.

Для обобщенного показателя стойкости показателя была выбрана аддитивная форма, так как величина вклада отдельных составляющих, соответствующих определенному методу криптоанализа, не зависит от вкладов других методов. Превышение данным показателем порога $F_d = s * 10^{-6}$ будет означать, что исследуемый БШ является потенциально уязвимым по крайней мере для одной криптоаналитической атаки. Физический смысл данного показателя состоит в том, что он отражает существование хотя бы одного практического метода криптоанализа при значении показателя близком к 1, при значении показателя от 1 до N существует несколько практических методов криптоанализа, и при значении намного меньшем 1 он показывает, какое минимальное количество ресурсов (исходных данных или вычислительных мощностей) необходимо добавить к уже имеющимся для проведения хотя бы одной практической атаки.

При таком подходе к вычислению стойкости БШ по значению этого обобщенного показателя сразу можно определить, является ли алгоритм шифрования устойчивым ко всем видам криптоаналитических атак или нет. Если значение показателя близко к 1, то целесообразно проведение одной из криптоаналитических атак, если значение показателя равно 0, то надежность алгоритма не позволяет его вскрыть даже теоретически, без существенных изменений в теории криптоанализа, и если значение показателя значительно меньше 1 то целесообразно проведение дальнейших исследований в направлении усовершенствования атаки или смягчения ограничений на применение атаки.

3. Пример реализации предложенного подхода к анализу криптостойкости блочного шифра. Рассмотрим пример анализа криптостойкости для двух практических блочных шифров — алгоритма шифрования DES и блочного шифра ГОСТ 28147-89.

Алгоритм DES в настоящее время используется ограниченно, так как он имеет недостаточную длину ключа, что позволяет вскрыть его методом полного перебора. Несмотря на то, что реализация криптоанализа методом полного перебора недоступна для одиночных

пользователей и небольших компаний из-за высокой стоимости вычислительных ресурсов, крупным компаниям и государственным службам такая реализация метода криптоанализа доступна.

Блочный шифр ГОСТ 28147-89, напротив, в настоящее время является государственным стандартом шифрования и повсеместно применяется для шифрования большого объема данных.

В качестве исходных данных предположим, что в наличии имеется $W = 2^{30}$ открытых текстов и соответствующих им шифртекстов, зашифрованных на одном ключе, что будет иметь место при шифровании и передаче стандартного фильма в одном сеансе связи. Объем вычислительных ресурсов имеющихся в наличии примем за 1024 стандартных машины класса Pentium 4 с частотой 3 ГГц, что соответствует потенциальным ресурсам небольшой организации или хакерской группы. При шифровании примерно со скоростью 150 Мбайт в секунду, которая близка к теоретическому пределу с учетом 4-х ядер и оптимизированной реализации, это составит порядка 2^{24} в секунду для одной машины и 2^{34} в секунду для 1024 машин. Время отводимое на расшифрование возьмем 8 суток, то есть $60 * 60 * 24 * 8 = 2^{20}$ за которое можно выполнить 2^{54} операций шифрования. Результаты отдельных видов криптоанализа выбранных алгоритмов по материалам открытых публикаций([1]-[5]) приведены в таблице 1.

Таблица 1. Результаты криптоанализа выбранных блочных шифров по материалам открытых публикаций

	DES	ГОСТ 28147-89
Линейный криптоанализ	$W = 2^{43}, N = 2^{43}$	-
Дифференциальный криптоанализ	$W = 2^{55}, N = 2^{55}$	-
Алгебраический криптоанализ	-	$W = 2^{64}, N = 2^{248}$
Интегральный криптоанализ	-	-
Полный перебор	$W = 1, N = 2^{56}$	$W = 1, N = 2^{256}$

$$F_{\Sigma}(DES) = \frac{1}{\left(1 + \frac{2^{43}}{2^{30}}\right) * 1} + \frac{1}{\left(1 + \frac{2^{55}}{2^{30}}\right) * \left(1 + \frac{2^{55}}{2^{54}}\right)} + \frac{1}{1 * \left(1 + \frac{2^{56}}{2^{54}}\right)}.$$

$$F_{\Sigma}(DES) \approx 1.2e - 4 + 9.9e - 9 + 0.2 \approx 0.200122.$$

Величина обобщенного показателя криптостойкости для алгоритма DES говорит о том, что при заданных условиях его вскрытие невозможно, но при некотором ослаблении ограничений его взлом является реальностью. То есть признаком потенциальной слабости является близость порядка этого показателя к 1. Он отражает

реальную возможность взлома данного алгоритма методом полного перебора, но с несколько большей вычислительной сложностью, чем выбрана нами в условиях задачи.

$$F_{\Sigma}(GOST) = \frac{1}{\left(1+\frac{2^{64}}{2^{30}}\right) * \left(1+\frac{2^{248}}{2^{54}}\right)} + \frac{1}{1 * \left(1+\frac{2^{256}}{2^{54}}\right)}.$$

$$F_{\Sigma}(GOST) \approx 2.31e-69 + 1.5e-61 \approx 1.555e-61.$$

Для алгоритма ГОСТ очевидно, что порядок показателя криптостойкости очень далек далек от единицы, и это говорит о том, что даже с учетом существенных послаблений в ограничениях взлом этого алгоритма не представляется возможным, что и соответствует реальному положению дел - на сегодняшний день алгоритм ГОСТ 28147-89 не имеет значимых уязвимостей [2, 3].

4. Заключение. В данной работе предложен метод оценивания результатов криптоанализа блочных шифров. Он позволяет получить численную характеристику криптостойкости блочного шифра к нескольким методам криптоанализа. Метод основан на использовании обобщенного показателя криптостойкости который учитывает вычислительные ресурсы и объем исходных данных имеющиеся в распоряжении криптоаналитика. Данный метод может быть использован при определении практической возможности взлома различных блочных шифров и сравнения их между собой по этому показателю.

Литература

1. *Панасенко С.П.* Стандарт шифрования ГОСТ 28147-89. Обзор криптоаналитических исследований. URL: http://www.inssl.com/standart-of-cipher.html (дата обращения: 23.03.2015).
2. *Shorin V.V., Jelezniakov V.V., Gabidulin E.M.* Linear and Differential Cryptanalysis of Russian GOST // Electronic Notes in Discrete Mathematics. 2001. vol. 6. pp 538–547.
3. *Courtois N.* Security Evaluation of GOST 28147-89 In View Of International Standardisation // Cryptologia. 2012. vol. 36(1). pp. 2–13.
4. *Biham E., Shamir A.* Differential Cryptanalysis of the Data Encryption Standard // Springer-Verlag Computers. 1993. 188 p.
5. *Matsui M.* Linear cryptanalysis method for DES cipher // In Advances in Cryptology - EUROCRYPT'93. Springer-Verlag. 1993. LNCS 765. pp. 386–397.
6. *Biham E.* On Matsui Linear Cryptoanalysis // In Advances in Cryptology – EUROCRYPT '94. Springer-Verlag. 1995. LNCS 950. pp. 341–355.
7. *Keliher L.* Refined analysis of bounds related to linear and differential cryptanalysis for the AES // Fourth Conference on the Advanced Encryption Standard (AES4). Springer-Verlag. 2005. LNCS 3373. pp. 42–57.

8. *Knudsen L., Wagner D.* Integral cryptanalysis // Fast Software Encryption. Springer-Verlag. 2002. LNCS 2365. pp. 112–127.
9. *Courtois N.T., Pieprzyk J.* Cryptanalysis of Block Ciphers with Overdefined Systems of Equation //In Proceeding of Asiacrypt 2002. Springer-Verlag. 2002. LNCS 2501. pp. 378–385.
10. *Biryukov A., De Canniere C.* Block Ciphers and Systems of Quardatic Equations // In Fast Software Encryption. Springer-Verlag. 2003. LNCS 2887. pp. 274–289.

References

1. Panasenko S.P. GOST 28147-89 encryption standard. [Overview of cryptanalytic research]. Available at http://www.inssl.com/standart-of-cipher.html. (accessed: 23.03.2015). (In Russ.)
2. Shorin V.V. Jelezniakov V.V., Gabidulin E.M. Linear and Differential Cryptanalysis of Russian GOST. *Electronic Notes in Discrete Mathematics*. 2001. vol. 6. pp 538–547.
3. Courtois N. Security Evaluation of GOST 28147-89 In View Of International Standardisation. *Cryptologia*. 2012. vol. 36(1). pp. 2–13.
4. Biham E., Shamir A. Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag Computers. 1993. 188 p.
5. Matsui M. Linear cryptanalysis method for DES cipher. In Advances in Cryptology - EUROCRYPT'93. Springer-Verlag. 1993. LNCS 765. pp. 386–397.
6. Biham E. On Matsui Linear Cryptoanalysis. In Advances in Cryptology – EUROCRYPT '94. Springer-Verlag. 1995. LNCS 950. pp. 341–355.
7. Keliher L. Refined analysis of bounds related to linear and differential cryptanalysis for the AES. Fourth Conference on the Advanced Encryption Standard (AES4). Springer-Verlag. 2005. LNCS 3373. pp. 42–57.
8. Knudsen L., Wagner D. Integral cryptanalysis. Fast Software Encryption. Springer-Verlag. 2002. LNCS 2365. pp. 112–127.
9. Courtois N.T., Pieprzyk J. Cryptanalysis of Block Ciphers with Overdefined Systems of Equation. In Proceeding of Asiacrypt 2002. Springer-Verlag. 2002. LNCS 2501. pp. 378–385.
10. Biryukov A., De Canniere C. Block Ciphers and Systems of Quardatic Equations. In Fast Software Encryption 2003. Springer-Verlag. 2003. LNCS 2887. pp. 274–289.

Романченко Александр Михайлович — к-т техн. наук, старший преподаватель кафедры систем сбора и обработки информации Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: криптография, информационная безопасность, сетевые технологии. Число научных публикаций — 15. rcrst@newmail.ru; ул. Ждановская, д.13, Санкт-Петербург, 197198, РФ; р.т.: +7(812)237-19-60.

Romanchenko Alexander Mikhailovitch — Ph.D., senior lecturer of the information acquisition and data processing department, Mozhaisky Military Aerospace Academy. Research interests: cryptography, information security, network technology. The number of publications — 15. rcrst@newmail.ru; Zdanovskaya str.13, Saint-Petersburg, Russia, 197198; office phone: +7(812)237-19-60.

РЕФЕРАТ

Романченко А.М. **Метод оценивания результатов криптоанализа блочного шифра.**

Данная работа посвящена разработке обобщенного показателя криптостойкости который характеризует устойчивость блочного шифра к различным методам криптоанализа. Этот показатель формируется с учетом реальных возможностей криптоаналитика и учитывает количество исходных данных и вычислительных ресурсов используемых для анализа. Метод оценивания результатов криптоанализа основанный на использовании данного показателя позволит проводить сравнительный анализ криптостойкости разных шифров. Это показатель может быть использован, в том числе и для неизвестных сегодня методов, которые возможно будут открыты в будущем. При установке граничных значений предложенного показателя он может быть использован для формирования требований к криптостойкости алгоритмов для использования в аппаратуре или информационной системе. В работе приведены два примера использования метода для широко известных блочных алгоритмов шифрования – DES и ГОСТ 28147-89. Результаты применения метода совпадают с традиционными результатами оценивания криптостойкости этих алгоритмов шифрования.

SUMMARY

Romanchenko A.M. **The Method of Evaluation of the Results of a Block Cipher Cryptanalysis.**

This work is devoted to the development of a generalized indicator that characterizes the resistance of cryptographic block cipher to various methods of cryptanalysis. It is derived taking into account the real possibilities cryptanalyst and monitors the amount of input data and computing resources used for the analysis. The method of evaluation of the results of cryptanalysis based on the use of this indicator will allow for a comparative analysis of different cryptographic ciphers. This indicator may be used including methods for unknown today which might be visible in the future. When setting boundary values proposed indicator, it may be used for establishing the requirements for cryptographic algorithms for use in the apparatus or system information. The paper presents two examples of using the method for well-known block encryption algorithms - DES and GOST 28147-89. The results of applying the method coincide with the traditional evaluation of the reliability of the results of encryption algorithms.