УДК 004.056.55

Р.М. Михерский

ШИФР НА ОСНОВЕ СЛУЧАЙНЫХ ЧИСЕЛ С НЕРАВНОМЕРНЫМ РАСПРЕДЕЛЕНИЕМ

Предложен новый принцип построения криптографических систем с применением шифра на основе случайных чисел с неравномерным распределением. Показано, что данный метод шифрования обладает высокой степенью устойчивости к традиционным криптографическим атакам, таким как: перебор всех вариантов ключа, известный исходный текст и специально подобранные исходные тексты.

Введение

В настоящее время для криптографической защиты информации, в системах с секретным ключом, наиболее часто используются блочные шифры. Как правило, при создании современных блочных шифров их авторам приходится идти на компромисс между скоростью шифрования и устойчивостью к криптографическим атакам. На сегодняшний момент в среде разработчиков криптографических систем сложилось мнение, что нужно гарантировать безопасность системы на протяжении 50 лет с момента ее создания [1]. Тем не менее, практика показывает, что системы шифрования оказываются взломанными гораздо раньше, чем на это рассчитывают их создатели. Показателен пример шифра DES, который, принят в 1977 году в США как официальный стандарт шифрования [2], к концу 90-х годов 20 века уже безнадежно устарел и не мог противостоять криптографическим атакам [3]. По мнению ряда авторов, используемый в настоящее время, в США как официальный стандарт, шифр AES может быть уязвимым к атакам с использованием алгоритма XSL [4], к атакам с использованием информации о времени выполнения операций [5] и к атакам с применением дифференциального анализа ошибок [6]. Хотя подобные атаки на практике пока еще не реализованы, нет сновений утверждать, что они не будут реализованы в ближайшем будущем.

В данной работе предложен новый принцип построения криптографических систем, обладающих значительно большей устойчивостью к атакам, чем ныне существующие коммерчески используемые системы.

Алгоритм шифрования на основе случайных чисел с неравномерным распределением

Пусть абоненты А и В решили организовать секретную связь друг с другом. Для этого они выбирают в качестве ключа последовательность n случайных целых чисел $\{c_i\}$. Закон распределения этих чисел может быть равномерным, нормальным, либо любым другим. Значение чисел выбирается в интервале от 0 до 255.

Пусть абонент А решил переслать абоненту В секретное сообщение $\{a_i\}$ размера N. Числовые значения элементов сообщения лежат в интервале от 0 до 255.

Для этого он генерирует новую последовательность n случайных целых чисел $\{d_i\}$. Закон распределения этих чисел может быть нормальным, либо любым другим, кроме равномерного распределения. Значение чисел выбирается в интервале от 0 до 255.

Далее эта последовательность кодируется методом Хаффмана или другим алгоритмом кодирования с минимальной избыточностью. Получается новая последовательность $\{g_i\}$ размера n_1, причем

число элементов в новой последовательности меньше чем в предыдущей, т. е. $n_1 < n$. Затем к этой последовательности добавляется $n_1 - n$ элементов из шифруемого сообщения. В результате получается новая последовательность $\{f_i\}$ размера n (в реальной системе, вообще говоря, число добавляемых элементов шифруемой последовательности будет меньше, так как необходимо добавить элементы с информацией о том, где заканчивается последовательность $\{g_i\}$, и начинаются элементы шифруемого сообщения). Далее находится последовательность $\{b_i\}$ как сумма соответствующих элементов ключа $\{c_i\}$ и последовательности $\{f_i\}$ по модулю 256 т. е.:

$$b_i = f_i + c_i (\mathrm{mod} 256) \qquad (i=1,\ldots,n). \qquad (1)$$

Затем последовательность $\{b_i\}$ передается от абонента А к абоненту В по открытому каналу. Получив последовательность $\{b_i\}$, абонент В находит последовательность $\{f_i\}$ по формуле:

$$f_i = b_i - c_i (\mathrm{mod}\, 256) \qquad (i=1,...,n). \qquad (2)$$

Из этой последовательности выделяется $n_1 - n$ элементов шифруемого сообщения, а так же последовательность $\{g_i\}$, которая декодируется методом Хаффмана или другим соответствующим алгоритмом кодирования с минимальной избыточностью. В результате абоненту В становится известна последовательность $\{d_i\}$, а так же $n_1 - n$ элементов шифруемого сообщения.

На следующем шаге абонентами А и В в качестве ключа $\{c_i\}$ выбирается последовательность $\{d_i\}$ и весь вышеприведенный алгоритм повторяется для оставшихся элементов последовательности $\{a_i\}$. Подобные циклы продолжаются до тех пор, пока не будут переданы все N элементов сообщения $\{a_i\}$. При этом, абоненты будут знать новый секретный ключ $\{c_i\}$ размера n, который можно будет использовать для передачи нового сообщения.

Недостатки метода шифрования на основе случайных чисел с неравномерным распределением

Следует отметить некоторые недостатки вышеизложенного метода шифрования.

Во-первых, объем зашифрованного сообщения всегда больше объема исходного. Данный недостаток может быть достаточно серьезным, если необходимо передавать большие объемы зашифрованной информации через низкоскоростной канал связи. Решить эту проблему можно предварительным архивированием исходного сообщения, что, в свою очередь, также повысит устойчивость к атакам зашифрованного сообщения.

Во-вторых, в данной системе шифрования невозможен произвольный доступ к блокам зашифрованных данных, так как для того, что бы расшифровать данные в каком-то из блоков, необходимо расшифровать все предыдущие блоки.

В-третьих, для эффективной работы вышеописанной системы шифрования, необходимо применять высокоскоростной генератор случайный чисел с распределением отличным от равномерного и обладающий достаточно высокой устойчивостью к криптографическим атакам. Реализация такого генератора является достаточно не тривиальной задачей. Рассмотрим данный вопрос подробней.

Генерация случайных чисел с неравномерным распределением

Для генерации случайных чисел, в настоящее время, используется два подхода. Первый из них связан с созданием и применением специальных устройств, использующих какие-либо физические ис-

точники шума. Естественно, что шум в них должен иметь доказуемо случайное поведение. На практике в качестве таких источников использовались: нулевые вакуумные колебания электромагнитного поля [7], нестабильность частоты свободно колеблющегося осциллятора [8], тепловой шум полупроводникового диода [9], показания счётчика Гейгера [10] и т. д.

Как правило, подобные генераторы позволяют получить случайные числа с распределением отличным от равномерного, что и нужно для работы вышеописанного алгоритма шифрования.

Однако часто стоит задача получения случайных величин на обычном персональном компьютере без применения дополнительного оборудования. Учитывая это, зачастую более актуальным является второй подход, связанный с использованием событий от стандартных устройств компьютера: нажатий пользователем кнопок на клавиатуре или «мыши»; движение пользователем мыши; время откликов принтеров, сканеров, жестких дисков [11]; взаимодействие между потоками; «шум» видеокарты, счетчик тактов процессора и пр. Однако каждый из этих способов генерации энтропии имеет свои недостатки. Так, например, нажатие пользователем кнопок на клавиатуре или мыши обеспечивает достаточно медленный поток энтропии, кроме этого требует в процессе работы криптографической системы участие пользователя, что не всегда возможно. К недостаткам самого распространенного способа генерации энтропии – использования счетчика тактов процессора, можно отнести чувствительность фазового шума генераторов частоты к внешним помехам, а значит, возможность влиять на генератор случайных чисел извне [12].

Отметим, что счетчики тактов процессора позволяют получать равномерно распределенные случайные числа. Для большинства современных систем шифрования это является преимуществом, так как именно с такими числами эти системы и работают. Однако, в данной работе в описываемой системе, используются неравномерно распределенные случайные числа, поэтому непосредственное применение генератора случайных чисел на основе счетчика тактов процессора представляется затруднительным.

В работе [13] предложен способ генерации случайных чисел с помощью оптического манипулятора «мышь». Было показано, что в определенных, специально созданных условиях, оптический манипулятор может стать эффективным источником энтропии в системах криптографической защиты информации.

Схема эксперимента показана на рис. 1.

Рис. 1. Схема эксперимента по генерации случайных чисел с помощью оптического манипулятора

Оптический манипулятор «мышь» помещается на поверхность со сложным рельефом. При этом плоскость нижней поверхности мыши ориентируется не строго параллельно рабочей поверхности как в стандартном режиме использования, а под углом в 2 градуса. Это достигается увеличением высоты ножек с одной стороны мыши на 3 мм.

При выполнении вышеприведенных условий, курсор оптического манипулятора выходит из стабильного положения и начинает случайным образом перемещаться по экрану монитора. Это связано с тем, что система обработки изображений манипулятора в данном случае не может правильно сфокусироваться на поверхности, и в системе возникает достаточно сильный

«шум». Координаты X и Y, перемещающегося курсора, определяются и записываются на жесткий диск с помощью специально разработанной компьютерной программы.

В качестве случайных чисел в таком генераторе использовались ненулевые значения цепных абсолютных приростов ΔX и ΔY координат X и Y.

Гистограммы частот этих величин показаны на рис. 2 и 3. Там же для сравнения приведены графики нормального распределения частот.

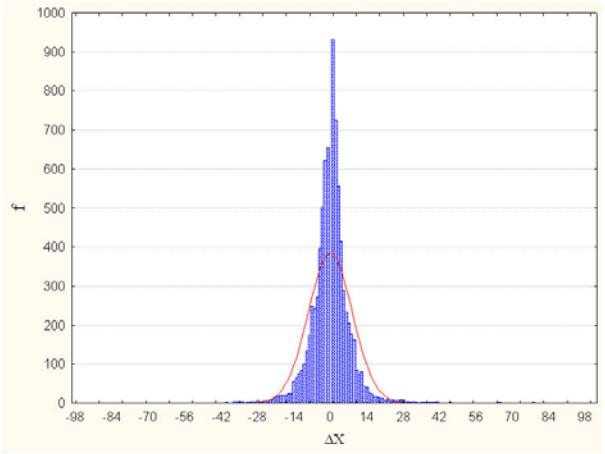

Рис. 2. Гистограмма частот f ненулевых цепных абсолютных приростов координат ΔX

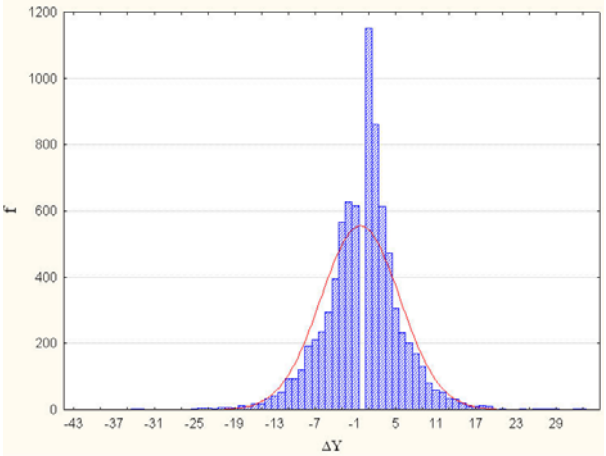

Рис. 3. Гистограмма частот f ненулевых цепных абсолютных приростов координат ΔY

Как видно из рис. 2 и 3 распределение случайных чисел, полученных с помощью оптического манипулятора, отлично от равномерного распределения. Это позволяет использовать полученные таким образом случайные числа в вышеприведенном алгоритме шифрования.

Следует обратить внимание на следующий недостаток. Скорость генерации энтропии в таком источнике составляет всего 971 бит/с. Поэтому использование подобного метода генерации случайных чисел не позволит создать высокоскоростную систему шифрования.

Более быстрым и эффективным методом генерации случайных чисел с неравномерным распределением может оказаться использование шума ПЗС-матрицы подключенной к компьютеру фото- и видео- техники. Однако, данный вопрос требует подробного дополнительного изучения.

Преимущества метода шифрования на основе случайных чисел с неравномерным распределением

Несмотря на вышеперечисленные недостатки и трудности, предложенный способ шифрования обладает достаточным набором преимуществ. Прежде всего, это высокий уровень криптографической стойкости, приближающийся к безусловной стойкости.

Пусть, например, в качестве ключа выбрана последовательность 10000 случайных чисел изменяющихся в пределах от 0 до 255 и имеющих нормальное распределение со среднеквадратическим отклонением $\sigma = 8$.

Тогда энтропия H_c, приходящаяся на один символ этой последовательности, определяется по формуле [14]:

$$H_c = \log_2 \sqrt{2e\pi\sigma^2} \qquad (3)$$

и равна $H_c = 5{,}047096$.

Соответственно энтропия H, приходящаяся на 10000 символов: $H = 50471$. Таким образом, для подбора ключа необходим перебор 2^{50471} вариантов, что при современном развитии вычислительной техники не представляется возможным. И маловероятно, что такой перебор удастся

осуществить при любом развитии вычислительной техники в обозримом будущем.

Следует отметить, что вышеописанный метод шифрования так же является устойчивым к традиционным криптографическим атакам на основе известного исходного текста и на основе специально подобранных исходных текстов. Действительно, знание злоумышленником текста, передаваемого в каком-то из блоков, равносильно знанию им части последовательности $\{a_i\}$. Но известные элементы последовательности $\{a_i\}$ никак не влияют на генерацию последовательности случайных чисел $\{d_i\}$ используемых для шифрования неизвестных элементов последовательности $\{a_i\}$.

Другими словами, знание злоумышленником текста, передаваемого в каком-то из блоков, не поможет ему узнать сжатый ключ, находящийся в этом же блоке. Соответственно, он никак не сможет определить текст, зашифрованный в следующем блоке.

Для любого шифра, применяемого на практике, одной из самых важных характеристик является скорость шифрования данных. Оценим ее для вышеприведенного метода. Как видно из приведенного ранее алгоритма, наиболее ресурсоемкими являются операции связанные с кодированием и декодированием методом Хаффмана. Поэтому скорость шифрования данных, по порядку величины, будет близка к скорости кодирования ключевых последовательностей случайных чисел методом Хаффмана. Следует, отметить, что в реальных системах, скорость шифрования скорей всего будет ограничиваться скоростью работы генератора случайных чисел с неравномерным распределением.

Таким образом, можно сделать вывод, что вышеописанный метод шифрования может быть применен в криптографических системах с повышенными требованиями к безопасности, передаваемой информации.

1. *Фергюсон Н., Шнайдер Б.* Практическая криптография.: Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 424 с.
2. *ANSI X3.92*, “American National Standard for Data Encryption Algorithm (DEA),” American National Standards Institute, 1981.
3. *Авдошин С.М., Савельева А.А*. Криптографические методы защиты информационных систем // Известия АИН им. А.М. Прохорова. Бизнес-информатика. – 2006. – Т. 17. – С. 91–99.
4. *Courtois N., Pieprzyk J.* Cryptanalysis of Block Ciphers with Overdefined Systems of Equations // Advances in Cryptology – ASIACRYPT 2002 8th International Conference on the Theory Application of Cryptology and Information Security Queenstown, New Zealand, December 1–5, 2002 Proceedings. Lecture Notes in Computer Science (2501). – Springer, 2002. – P. 267–287.
5. *Osvik D. A., Shamir A. and Tromer E*. Cache Attacks and Countermeasures: the Case of AES // Topics in Cryptology - CT-RSA 2006, The Cryptographers’ Track at the RSA Conference. – Springer-Verlag, 2005. – P. 1–20.
6. *Saha D., Mukhopadhyay D., RoyChowdhury D.* A Diagonal Fault Attack on the Advanced Encryption Standar // Cryptology ePrint Archive. – 2009.
7. *Gabriel C., Wittmann C., Sych D. Dong R., Mauerer W., Andersen U. L., Marquard C. and Leuchs G.* A Generator for Unique Quantum Random Numbers Based on Vacuum States // Nature Photonics.– 2010. – № 4. – P. 711 – 715.
8. *Fairfield R.C., Mortenson R.L. and Koulthart K.B.* An LSI Random Number Generator, Advances in Cryptology: Proceedings of CRYPTO 84, Springer Verlag.– 1985. – P. 203 – 230.
9. *Richter M.* Fin Rauschgenerator zur Gewinnung won quasi-idealen Zufallszahlen fur die stochastische Simulation.: Ph.D. dissertation, Aechen University of Technology, 1992.
10. *Schneier B.* Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C. - John Wiley & Sons, Inc., 1996.
11. *Davis D., Ihaka R., Fenstermacher P.* Cryptographic Randomnes from Air Turbulence in Disk Drives. – In: Desmedit Y. G. (ed). Advances in Cryptology – CRYPTO 94. Lecture Notes in Computer Science. Springer-Verlag. – 1994. – Vol. 839. – P. 114–120.
12. *Ковалев А.В.* Реализация генераторов случайных чисел. – М.: Научная сессия МИФИ, 2007. – Том 12. – С. 176–177.

13. *Михерский Р.М., Попов О.И.* Генерация случайных чисел с помощью оптического манипулятора // Международный научно-технический журнал «Проблемы управления и информатики». – 2011. – № 4. – С. 152–155.
14. *Корн Г., Корн Т.* Справочник по математике (для научных работников и инженеров): Пер. с англ. – М.: Наука, 1973. – 832 с.

Получено 15.06.2011

Об авторе:

Михерский Ростислав Михайлович,
кандидат физико-математических наук,
заведующий кафедрой «Информатики и естественно-научных дисциплин».

Место работы автора:

Крымский филиал
Европейского университета,
г. Симферополь,
ул. Трубаченко/Поповкина 10/22.
Тел.: (0652) 49 9969.
mrm03@mail.ru