Программная реализация алгоритма шифрования на основе случайных чисел с неравномерным распределением

Р.М. Михерский[1], Д.М. Полянчук[1], М.В.Исаев[1]

[1]Крымский федеральный университет имени В.И. Вернадского, проспект академика Вернадского 4, Симферополь, Россия, 295007

Аннотация. Программно реализована криптографическая система защиты информации на основе случайных чисел с неравномерным распределением. Показано, что эта система обладает высокой устойчивостью к известным криптографическим атакам. Экспериментально определена скорость шифрования данных.

1. Введение

В современном мире ведущую роль играют электронные средства передачи, хранения, и обработки информации. При этом одной из главных проблем является защита передаваемых данных от несанкционированного доступа. В настоящее время для решения этой проблемы, как правило, используются криптографические методы защиты информации. Чаще всего с этой целью используются блочные шифры, например, такие как принятый в США в качестве стандарта шифрования данных шифр AES, или шифр ГОСТ 28147-89 - принятый в качестве стандарта в Российской Федерации. Хотя, на настоящий момент, не известно ни одной успешной атаки на эти шифры, существует достаточно веские основания предполагать, что такие атаки вполне возможны [1]. В связи с этим насущно стоит проблема разработки новых алгоритмов шифрования, обладающих более высокой степенью устойчивости к криптоанализу, чем существующие алгоритмы.

В работе [2] был предложен алгоритм шифрования на основе случайных чисел с неравномерным распределением. Этот алгоритм имеет ряд существенных преимуществ, главным из которых является высокая стойкость к криптографическим атакам. Однако до настоящего времени, этот алгоритм не был реализован на практике.

Целью данной работы явилась программная реализация метода шифрования на основе случайных чисел с неравномерным распределением, а так же анализ криптостойкости и скорости работы алгоритма.

2. Генерация случайных чисел с неравномерным распределением

Алгоритм шифрования на основе случайных чисел с неравномерным распределением достаточно подробно описан в работе [2]. Одной из главных задач при реализации этого алгоритма явилось создание высокоскоростного генератора случайных чисел с неравномерным распределением, имеющего высокую устойчивость к известным криптографическим атакам.

В настоящее время, при реализации подобных генераторов, в качестве источников энтропии используются: нулевые вакуумные колебания электромагнитного поля [3], нестабильность частоты свободно колеблющегося осциллятора [4], тепловой шум полупроводникового диода [5], показания счётчика Гейгера [6], события от стандартных устройств компьютера [7], счетчик тактов процессора [8], оптический манипулятор «мышь» [9].

В данной работе был реализован генератор случайных чисел, имеющий неравномерное распределение, использующий веб-камеру ноутбука.

Для генерации случайных чисел необходимо, чтобы веб-камера, подключенная к ноутбуку или компьютеру, находилась в темном помещении или была закрыта. Только в таких условиях матрица камеры будет выдавать шумы, которые являются полностью случайными и не зависят от внешних факторов. Пример шумов матрицы показан на рисунке 1.

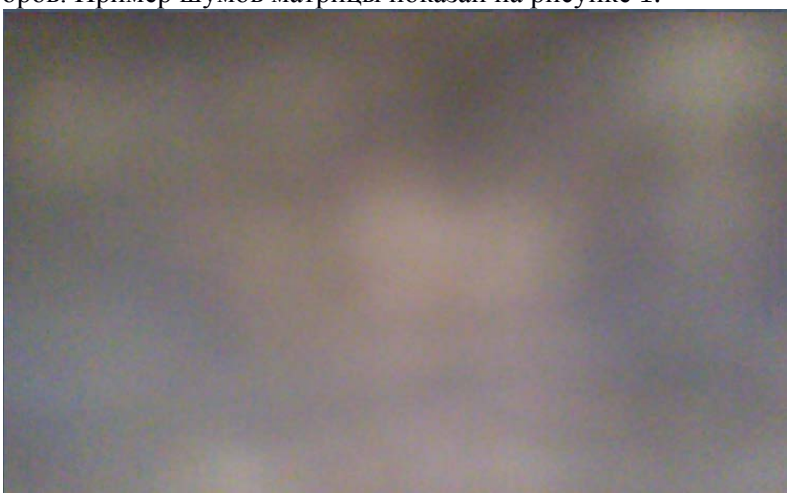

Рисунок 1. Шумы матрицы веб-камеры.

Когда камера находится в корректных условиях, делается два фотоснимка. Следует отметить, что между фотоснимками должен быть максимально меньший промежуток времени, что на практике даёт минимальные различия между фотографиями. После осуществления фотоснимков, из них необходимо получить так называемый bitmap – матрицу, в которой хранятся значения элементов изображения (пикселей). Для 24-х разрядного изображения каждый пиксель содержит в себе информацию о трех цветах (для цветовой модели RGB) – соответственно красном, зеленом и синем. На каждый цвет отводится 8 бит, то есть максимально возможное значение в десятичном представлении – 255, а минимальное 0. Значению 255 соответствует максимальная интенсивность цвета, а значению 0 – минимальная. На следующем шаге, в общем случае формируется двумерный массив (или bitmap), в который записываются соответствующие значения разностей компонент цвета для каждого из пикселей. Полученные разности могут изменяться от -255 до 255. Далее эти разности берутся по модулю 256 и записываются в последовательность $\{c_i\}$ целых чисел. Эта последовательность и используется в данном алгоритме в качестве ключа.

3. Анализ экспериментальных результатов

Шифр на основе случайных чисел с неравномерным распределением был программно реализован в среде программирования Visual Studio 2012 на языке C#. Длина ключевой последовательности n составила 10000 случайных целых чисел.

Исследование проводилось на ноутбуке Lenovo IdeaPad 310-15ISK со следующими параметрами: 2-х ядерный процессор IntelCore i3-6100U, частотой 2.3 ГГц, видеокарта NVIDIA GeForce 920MX 2 Гб, 4 ГБ ОЗУ, тип памяти DDR4, для генерации случайных чисел была использована встроенная веб-камера Lenovo EasyCamera с разрешением 1 Мп, операционная система Windows 10.

На рисунке 2 представлена гистограмма распределения разностей Δx компонент цвета используемых для генерации случайных чисел применяемых в ключевых последовательностях. Для сравнения сплошной линией представлен график нормального распределения.

Рисунок 2. Гистограмма распределения разностей Δx компонент цвета.

Как видно из этого рисунка, распределение полученных случайных чисел достаточно хорошо совпадает с нормальным распределением. Экспериментальное значение среднеквадратического отклонения составило $\sigma = 5{,}7665$.

Для тестирования работоспособности реализованной системы шифрования был выбран файл формата txt, размер которого составил 9,12 Мбит. В данном файле содержался роман Ф. М. Достоевского «Преступление и наказание». Эксперимент показал, что время шифрования этого файла составило 16,234 с. Соответственно, скорость шифрования - 562 кбит/с. Время дешифрования – 16,512 с, скорость дешифрования - 552 кбит/с. Таким образом, скорость шифрования практически совпадает со скоростью дешифрования.

Проведем оценку криптографической стойкости данной системы к атаке на основе перебора всех возможных ключей. Энтропия H_1, приходящаяся на одно число ключевой последовательности, определятся формулой [10]:

$$H_1 = \log_2 \sqrt{2e\pi\sigma^2} \quad (1)$$

Используя экспериментальное значение среднеквадратического отклонения σ, найдем, что энтропия $H_1 = 4{,}5749$. Тогда, энтропия H, приходящаяся на 10000 случайных целых чисел ключевой последовательности, равняется: $H = 45749$. Соответственно, для подбора ключа необходим перебор, по меньшей мере, 2^{45749} вариантов. Для подбора 256 битного ключа шифра AES необходим перебор всего 2^{256} вариантов.

Таким образом, представленная в данной работе система шифрования, имеет гораздо более высокую криптографическую стойкость, чем применяемые в настоящее время блочные шифры.

4. Литература

[1] Courtois, N. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations / N. Courtois, J. Pieprzyk // Advances in Cryptology. – Proceedings 8th International Conference on the Theory Application of Cryptology and Information Security Queenstown, New Zealand, December 1-5, 2002. Lecture Notes in Computer Science. – 2002. – Vol. 2501. – P. 267-287.

[2] Михерский, Р.М. Шифр на основе случайных чисел с неравномерным распределением / Р.М. Михерский // Проблемы программирования. – 2011. – Т.50, №. 7. – С. 90-91.

[3] Gabriel, C. A Generator for Unique Quantum Random Numbers Based on Vacuum States / C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquard, G. Leuchs // Nature Photonics. – 2010. – № 4. – P. 711-715.

[4] Fairfield, R.C. An LSI Random Number Generator, Advances in Cryptology / R.C. Fairfield, R.L. Mortenson, K.B. Koulthart // Proceedings of CRYPTO. – Springer Verlag, 1985. – P. 203-230.
[5] Richter, M. Fin Rauschgenerator zur Gewinnung won quasi-idealen Zufallszahlen fur die stochastische Simulation / M. Richter. – Ph.D. dissertation, Aechen University of Technology, 1992.
[6] Schneier, B. Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C/ B. Schneier. – John Wiley & Sons, Inc., 1996.
[7] Davis, D. Cryptographic Randomnes from Air Turbulence in Disk Drives / D. Davis, R. Ihaka, P. Fenstermacher // Advances in Cryptology. – Lecture Notes in Computer Science. – 1994. – Vol. 839. – P. 114-120.
[8] Ковалев, А.В. Реализация генераторов случайных чисел // А.В. Ковалев. – М.: Научная сессия МИФИ, 2007. – Т. 12. – С. 176-177.
[9] Mikhersky, R.M. Generation of Random Numbers by Means of Optical Manipulator / R.M. Mikhersky, O.I. Popov // Journal of Automation and Information Sciences. – 2011. – Vol. 43(8). – P. 76-80.
[10] Корн, Г. Справочник по математике (для научных работников и инженеров): пер. с англ. / Г. Корн, Т. Корн. – М.: Наука, 1973. – 832 с.

Software implementation of the encryption algorithm based on random numbers with non-uniform distribution

R.M. Mikherskii[1], D.M. Polyanchuk[1], M.V. Isaev[1]

[1]V.I. Vernadsky Crimean Federal University, Vernadskogo Prospekt 4, Simferopol, Russia, 295007

Abstract. A cryptographic system for protecting information based on random numbers with uneven distribution was implemented programmatically. It is shown that this system has a high resistance to known cryptographic attacks. The speed of data encryption is experimentally determined.

Keywords: cryptographic system of information protection, random numbers with non-uniform distribution, cryptography.