ISSN 2223-2966
№7 2018
(июль)

НАУЧНО–ПРАКТИЧЕСКИЙ ЖУРНАЛ

СОВРЕМЕННАЯ НАУКА

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ

Серия

ЕСТЕСТВЕННЫЕ и ТЕХНИЧЕСКИЕ НАУКИ

www.nauteh-journal.ru

ООО "НАУЧНЫЕ ТЕХНОЛОГИИ"

ISSN 2223-2966

СОВРЕМЕННАЯ НАУКА:
АКТУАЛЬНЫЕ ПРОБЛЕМЫ
ТЕОРИИ И ПРАКТИКИ

ЕСТЕСТВЕННЫЕ И ТЕХНИЧЕСКИЕ НАУКИ

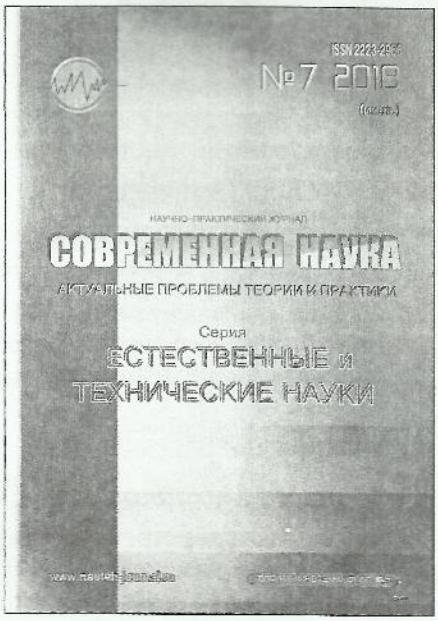
№ 7 2018 (ИЮЛЬ)

Научно-практический журнал

Scientific and practical journal

(ВАК - 05.11.00, 05.12.00, 05.13.00, 03.02.00, 14.01.00)

Учредитель журнала
Общество с ограниченной ответственностью
«НАУЧНЫЕ ТЕХНОЛОГИИ»



Журнал издается с 2011 года.

Подписной индекс издания
в каталоге агентства «Пресса России» — 80016

В течение года можно произвести подписку
на журнал непосредственно в редакции.

В НОМЕРЕ:

Издатель:
Общество с ограниченной ответственностью
«Научные технологии»

Адрес редакции и издателя:
109443, Москва, Волгоградский пр-т, 116-1-10
Тел/факс: 8(495) 755-1913

E-mail: redaktor@nauteh.ru
http: //www.nauteh-journal.ru
http: //www.vipstd.ru/nauteh

Журнал зарегистрирован Федеральной службой
по надзору в сфере массовых коммуникаций,
связи и охраны культурного наследия.

Свидетельство о регистрации
ПИ № ФС 77-44912 от 04.05.2011 г.

Журнал отпечатан в типографии
ООО «Типография АзаЛит» тел../факс: (495) 973-8296

Подписано в печать 20.07.2018 г. Формат 84x108 1/16
Печать цифровая Заказ № 0385 Тираж 2000 экз.

ISSN 2223-2966

Редакционный совет

СОДЕРЖАНИЕ CONTENTS

ОБЩАЯ БИОЛОГИЯ

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

РАДИОТЕХНИКА И СВЯЗЬ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

КЛИНИЧЕСКАЯ МЕДИЦИНА

ИНФОРМАЦИЯ

РАЗРАБОТКА, ТЕСТИРОВАНИЕ И ОЦЕНКА ШИФРАТОРА С ПЕРЕМЕННОЙ ФРАГМЕНТАЦИЕЙ БЛОКА ДЛЯ ПРОТОКОЛА БЕЗОПАСНОГО ОБМЕНА ИНФОРМАЦИЕЙ

Митращук Владимир Владимирович
Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева
rtimidalv@gmail.com

TESTING AND ESTIMATION OF ENCRYPT QUALITY WITH ALTERNATING BLOCK FRAGMENTATION FOR THE PROTOCOL OF SECURE DATA EXCHANGE

V. Mitrashchuk

Summary. The increase in computing power and the ubiquitous proliferation of computers, the emergence of the Internet of things (IoT), distributed networks and other new technologies makes us think more and more about improving the means of protecting information. The present encrypt must provide the ability to configure not only a unique key, but also free parameters of the algorithm. Popular and common symmetric ciphers, at best, use table replacements of 4–8 bits for this. It is necessary to develop and research algorithms that perform substitution with alternating block fragmentation. This will help extend the variability of the substitution for irreducible polynomials by combining and rearranging sub-blocks of variable length. The paper shows an improved encryption algorithm with alternating block fragmentation of the secure communication protocol unit, which meets the criteria described above, for which testing and performance evaluation was performed to establish cipher characteristics. All the results were obtained with the help of the developed cross-platform encryption program for Linux, ARMhf and Windows using the encryption of files on the computer. The speed of the encryption is estimated by the encrypt program, starting and stopping the timer before and after the encryption function is executed. The quality of the ciphertext is determined by two powerful tests, one of them (graphic) was finalized for the purpose of interpretation by the program. The encrypt speed is determined to be 120 kilobytes/s. Recommendations on the encrypt program configuration and chaotization characteristics for various cipher elements are formulated. The encryption showed better results than other solutions [9], showing the results of randomizing the graphical test for 1 round instead of 3 rounds. The comparison was conducted with the results that the authors provided. The necessity of introducing the third criterion is substantiated. The proposed solution can be used to protect the telemetry of IoT devices, drones, smart home systems; protection of voice communications, messages, files. It can also be used for video transmission in the presence of multi-core processors

Keywords: information encryption, transmission protocol, secure data exchange, symmetrical key, alternating block fragmentation, testing and estimation.

Аннотация. Увеличение вычислительной мощности и повсеместное распространение компьютеров, появление Интернета вещей (IoT), распределенных сетей и других новых технологий заставляет все больше задумываться о совершенствовании средств защиты информации. Настоящий шифратор должен предоставлять возможность конфигурирования не только уникального ключа, но и свободных параметров алгоритма. Популярные и распространенные симметричные шифры, в лучшем случае, используют для этого таблицы замен из 4–8 бит. Необходимо вести разработку и исследование алгоритмов, которые осуществляют замену подблоками переменной длины, чтобы определить область их применения. Это поможет расширить вариативность замены по неприводимым многочленам при помощи комбинирования и перестановки подблоков переменной длины. В работе показан улучшенный алгоритм шифрования с переменной фрагментацией блока протокола безопасного обмена информацией, соответствующий критериям, описанным выше, для которого проведено тестирование и дана оценка качества работы с целью установления характеристик шифра. Все результаты были получены при помощи разработанной кроссплатформенной программы-шифратора для Linux, ARMhf и Windows при помощи шифрования файлов на компьютере. Оценку скорости выполнения шифрования производит программа-шифратор, запуская и останавливая таймер до и после выполнения функции шифрования. Качество шифртекста определяется по двум мощным тестам, один из них (графический) был доработан с целью возможности интерпретации программой. Определена скорость шифратор — 120 килобайт/с. Сформулированы рекомендации по конфигурации шифратора и характеристики хаотизации для различных элементов шифра. Шифратор показал результаты лучше, чем у других решений, продемонстрировав результаты хаотизации графического теста за 1 раунд вместо 3 раундов. Сравнение проводилось с результатами, которые предоставили авторы, подробнее изложено в основном тексте статьи. Обоснована необходимость внедрение третьего критерия. Предлагаемое решение может быть использовано для защиты телеметрии приборов IoT, беспилотников, систем умного дома; защиты голосовой связи, сообщений, файлов. Возможно использование и для передачи видео при наличии многоядерных процессоров.

Ключевые слова: шифрование информации, протокол передачи, безопасный обмен данными, симметричный ключ, переменная фрагментация блока, тестирование и оценка.

Введение

Необходимость в защите информации присутствует практически в любой сфере деятельности, разница обычно состоит лишь в количестве средств, которые субъект готов затратить на защиту своих данных. Стоимость не единственный аспект, с которым столкнется любой, кто желает обеспечить защиту информации. Вторая проблема — это надежность существующих решений, независимо от их цены.

С течением времени способы защиты информации совершенствовались и становились более технологичными, также, как и способы преодоления защиты [1–9]. Но желание достичь такой реализации системы безопасности, которая будет обеспечивать абсолютную безопасность, существовало всегда. Особенно это актуально для вопроса криптографической защиты информации. Шифрование данных сегодня — это выбор между ресурсоемкостью алгоритма и его надежностью. Все попытки приблизиться к абсолютно безопасному шифрованию данных и их передаче сводились к практически не реализуемым или бессмысленным вещам.

В случае симметричного шифрования, можно добиться такой надежности шифра, что, теоретически, при полном переборе всех возможных ключей будет получаться огромное множество логически связанных сообщений, определить какое из них истинное ни злоумышленник, ни компьютер не сможет. Даже сообщения, имеющие известный формат пакета протокола передачи данных, после перебора всего множества и фильтрации полученных данных по известной структуре, все равно, в поле данных будут оставлять достаточное множество вариаций, если у пакета небольшая длина (а большая длина для пакетов протокола обычно и не требуется).

Угроза расшифровки может появится при накоплении большого количества пар открытого и зашифрованного текста, но получить такие пары злоумышленник сможет только на вычислительных машинах, которые будут производить шифрование, а этого можно избежать. Но и в таком случае возможно создать такой алгоритм симметричного шифрования, который после нескольких раундов будет давать непредсказуемые результаты, иначе говоря, закономерности будут практически отсутствовать, даже нейронная сеть не сможет их определить в достаточном качестве для восстановления исходной информации. Для защиты от подобной атаки в алгоритм можно добавить сцепку блоков, например, с вектором инициализации.

Симметричный алгоритм шифрования с переменной фрагментацией блока, который сможет выполнить требования, описанные выше, будет рассмотрен далее. Ключи такого алгоритма смогут иметь небольшую длину при сохранении требуемой надежности шифрования.

В работе [10] впервые в открытой печати представлен алгоритм шифрования с динамическим изменением размеров криптографических примитивов в различных раундах. Иными словами, предлагается проводить зашифрование текста, применяя замены по таблицам разных размеров в различных раундах.

В [10] проведены первые исследования, тестирование результатов зашифрования. В настоящей работе производится анализ модификации алгоритма [11]. Данная модификация адаптирована для использования в протоколе с целью создания наиболее безопасного канала обмена информацией, а именно: в алгоритме производится нормировка и сцепка блоков; используется раундовое преобразование над блоками размером 240 бит; длина общего ключа (ОК) алгоритма может быть от 0 до 240*(количество раундов) бит, другими словами, ОК может быть уникальным для каждого раунда; замена осуществляется по неприводимым многочленам [12, 13] в зависимости от длины подблока; динамическое изменение криптографических примитивов (подблоков) производится на блоки не одинаковой длины в пределах одного раунда, а произвольной, обеспечивая любые возможные комбинации; также предлагается производить линейный сдвиг после замены не на постоянную величину, а на случайную; аналогично предыдущему улучшению происходит сдвиг общего ключа случайно для каждого раунда. В итоге, получаются схемы на рис. 1.

Кроме того, была реализована кроссплатформенная программа-шифратор по схемам на рис. 1. Также, на ее основе будет реализован протокол безопасного обмена информацией [11].

Безопасный протокол обмена информацией позволяет установить зашифрованный канал связи с любой аппаратурой, тем самым, защитить конфиденциальность сведений и создать возможность недопущения выведения аппаратуры из строя и дезинформации в следствии навязывания ложных сообщений, благодаря методам имитозащиты, защиты от коллизий в служебных полях.

Первый критерий качества ОК и шифртекста. Посимвольная проверка

Авторы книги [14] предлагают оценочный метод посимвольной проверки, который считают самым сильным из всех рассмотренных в своей работе (подборка тестов Д. Кнута, система оценки статистических свойств «DIEHARD», CRYPT-S, руководство НИСТ и другие [15–18]).

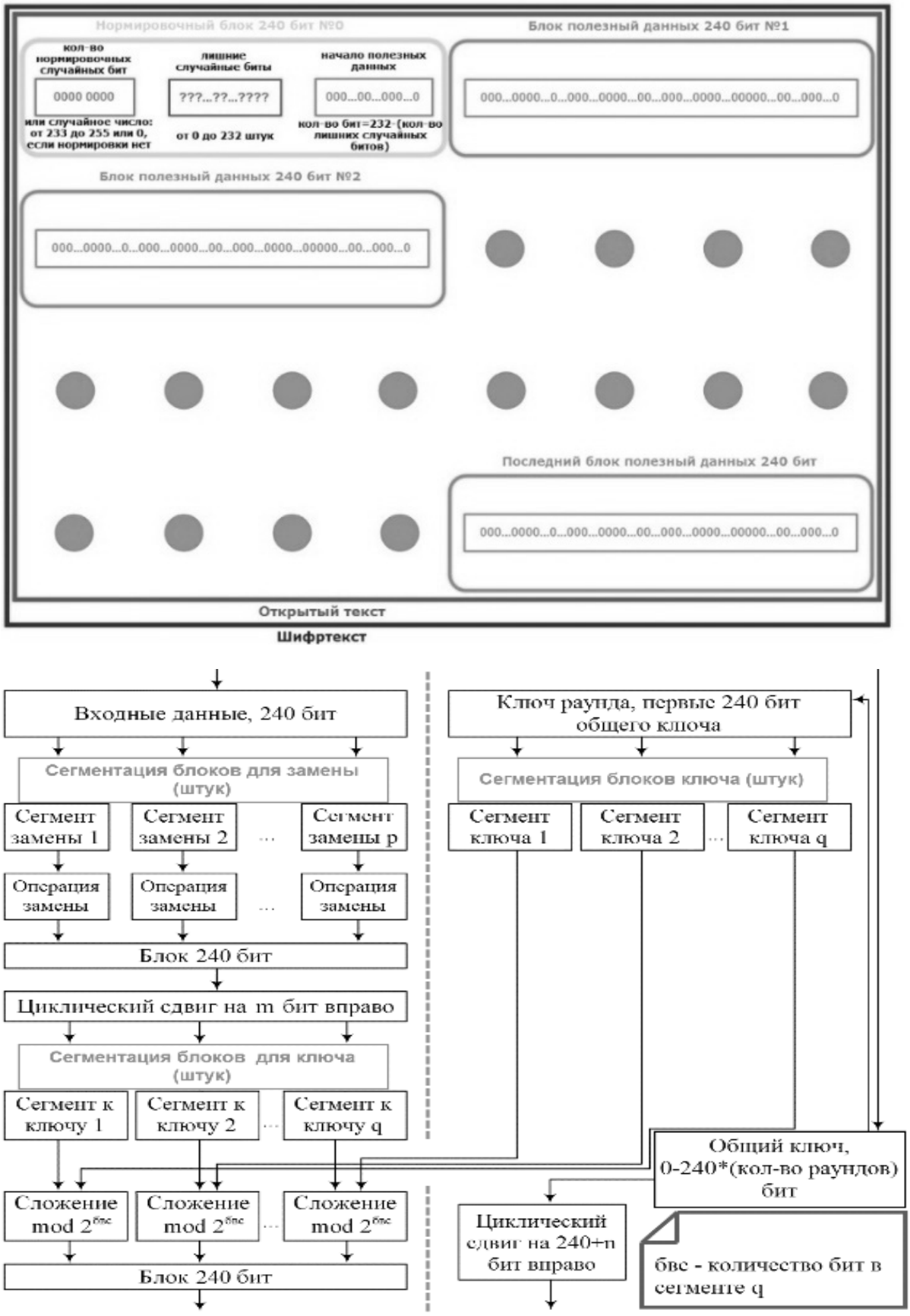


Рис. 1. Схемы нормировки и шифрования

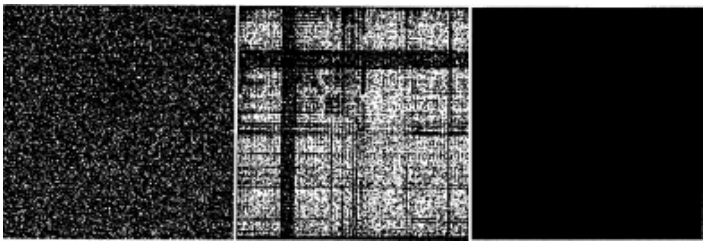


Рис. 2. Распределение координат из последовательности на плоскости

Данный метод заключается в проверке равномерности распределения символов в исследуемой последовательности на основе анализа частот появления каждого символа.

Пусть $\varepsilon = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ — последовательность блоков m-разрядных двоичных чисел длины n. Для выполнения критерия, все значения v_i (количество повторений) должны лежать в интервале по формуле (1).

$$\left[\frac{n-2.58\sqrt{n(2^m-1)}}{2^m}; \frac{n+2.58\sqrt{n(2^m-1)}}{2^m}\right] \quad (1)$$

Например, для последовательности $\varepsilon = 3\ 5\ 4\ 2\ 1\ 4\ 6\ 1$, $n = 8$, $m = 3$, все значения повторений $v_0 = 0$, $v_1 = 2$, $v_2 = 1$, $v_3 = 1$, $v_4 = 2$, $v_5 = 1$, $v_6 = 1$, $v_7 = 0$ принадлежат интервалу (2).

$$\left[\frac{8-2.58\sqrt{8(2^3-1)}}{2^3} = -1.41; \frac{8+2.58\sqrt{8(2^3-1)}}{2^3} = 3.41\right] \quad (2)$$

В первом критерии тест используется для анализа бинарных последовательностей по одному биту в отдельности, поэтому итоговая формула расчета диапазона значений примет более простой вид (3).

$$\left[\frac{n-2.58\sqrt{n}}{2}; \frac{n+2.58\sqrt{n}}{2}\right] \quad (3)$$

Тест только по каждому отдельному биту уязвим для комбинаций-чередований нулей и единиц. Например, 11110000, 10101010 и т.п. Поэтому в программе он используется одновременно с графическим способом распределения на плоскости, который адаптивно анализирует координаты с учетом их расположения относительно друг друга.

Второй критерий качества ОК и шифртекста. Распределение на плоскости

Авторы книги [14] предлагают графический метод распределения на плоскости. Данный тест осуществляется следующим образом. На поле размером $(2^R\text{-}1)(2^R\text{-}1)$, где R — разрядность чисел исследуемой последовательности, наносятся точки с координатами $(\varepsilon_i; \varepsilon_{i+1})$, ε_i — элементы исследуемой последовательности ε, i=1,…,(n-1). n — длина последовательности. Например, для последовательности ε=2 3 5 4 3 получим точки (2;3), (3;5), (5;4), (4;3).

Далее, авторами книги [14] предлагается проводить визуальную оценку полученных результатов. Если между элементами последовательности отсутствуют зависимости, то точки на поле расположены хаотично (Рисунок 2, слева). Если на поле присутствуют зависимости — последовательность не является случайной (Рисунок 2, по центру). Для последовательностей большой длины хорошим результатом является черный квадрат (Рисунок 2, справа).

Предложенный графический метод был улучшен и преобразован в оценочный способ для выполнения оценки бинарной последовательности при помощи нормировки системы координат по длине тестируемого сообщения. В зависимости от длины сообщения, выбирается интервал изменения координат XY общий для координаты X и для координаты Y. Таким образом, чтобы множество координат (X, Y), которое задает бинарная последовательность слева-направо со сдвигом на 1 координату, вмещало все получаемые таким образом координаты не менее одного раза. Для этого XY подбирается таким образом, чтобы выполнялось условие (4).

$$(2^{XY-1})^2 < \frac{n}{XY} \leq (2^{XY})^2 \quad (4)$$

Где n — количество бит в сообщении. В идеале, должно выполняться равенство (5).

$$\frac{n}{XY} = (2^{XY})^2 \quad (5)$$

Оно говорит о том, что плоскость с интервалом изменения координат XY может вместить в себя каждую координату ровно один раз, другими словами, получится полностью черный квадрат или мера хаотичности будет равна 100%. Если же, выполняется условие (6), тогда лишние координаты (которые всегда будут свободны) определяются по формуле (7).

№	Кол-во бит в ОК или ШТ ($Q = 16$)			№	Максимальная практическая граница,		
-	960	5040	24480	9	63,90	62,70	62,92
Минимальная практическая граница, %				10	63,46	63,19	65,00
1	2,50	0,50	0,12	11	64,14	65,97	63,75
2	2,08	0,40	0,07	12	63,80	62,90	71,25
3	1,67	0,30	0,10	13	62,16	62,50	64,17
Средняя мин. практическая граница, %				14	63,72	63,00	64,58
-	2,08	0,40	0,10	15	63,68	62,90	67,50
Максимальная практическая граница, %				16	63,21	62,20	69,58
1	63,45	62,80	63,33	17	62,92	63,69	65,00
2	62,87	63,89	61,70	18	63,50	64,09	63,75
3	64,26	63,99	67,08	19	64,51	62,30	68,75
4	63,16	65,18	62,08	20	63,95	63,39	64,17
5	63,11	64,88	65,42	Мин. максимальная практическая граница,			
6	63,50	62,70	64,58	-	62,16	62,20	61,70
7	63,43	63,99	67,08	Средняя максимальная практическая			
8	63,43	63,49	65,00	-	63,54	63,49	65,33

Рис. 3. Расчет практических границ второго критерия

$$\frac{n}{XY} < (2^{XY})^2 \quad (6)$$

$$Q = (2^{XY})^2 - \frac{n}{XY} \quad (7)$$

Мера хаотичности будет равна значению (8), где b — количество черных (заполненных) пикселей, а p — количество всех пикселей изображения.

$$W = \frac{b}{p} \cdot 100 \quad (8)$$

Например, для последовательности ε=0 1 1 0 получим точки (0;1), (1;1), (1;0), (0;0), XY=1, Q=0, W=100% (полностью черный квадрат). В результате экспериментов определено, что для получения достоверных результатов длина последовательности должна быть не менее 100 бит, а лучше не менее 10000 бит.

Лишние координаты Q должны быть одинаковыми для разных тестов, чтобы их можно было сравнивать между собой и, лучше всего, минимальными, т.е. равными нулю. Вероятность попадания координат более длиной бинарной последовательности в уникальную позицию меньше, чем вероятность попадания координат меньшей по длине бинарной последовательности на графике той же размерности, поэтому после вычитания Q, во втором случае, значения получаются завышенными от расчетных. Во избежание этого нужно проводит эксперименты при одинаковых значениях Q, а лучше, при Q=0. Для программы шифрования, из-за нормировки, минимальное значение параметра Q равно 16. Достигается оно при длине сообщения: 960, 5040, 24480 и т.п.

Для того, чтобы уточнить теоретические границы на практике, были проведены дополнительные эксперименты, результаты которых можно увидеть на рис. 3.

По достижению максимальной практической границы в диапазоне от 62,15% и больше, можно утверждать, что бинарная последовательность успешно выполнила второй критерий, но чем больше данный показатель, тем меньше повторений координат на плоскости. Данные границы были получены при подаче на вход второму критерию последовательностей, о которых было заранее известно, что они являются псевдослучайными последовательностями.

Может показаться, что после использования второго теста, в первом нет необходимости, но это не так. Учитывая, что чаще всего только 65% от последовательности занимает уникальную координату, то не все множество координат представлено в ней. Иначе говоря, при показаниях второго теста ниже 100%, всегда будет происходит случайное смещение количество нулей и единиц бинарной последовательности влево или вправо от равного их значения и, чем дальше от 100%, тем данные флуктуации будут сильнее. Поэтому, необходимо компенсировать этот недостаток первым критерием.

Обоснование необходимости внедрение третьего критерия

Благодаря первым двум тестам можно утверждать, что около 65% бинарной последовательности занимает уникальную координату на плоскости. Но что можно сказать об оставшихся 35%? Это множество координат,

которые повторяются и значительно уменьшить этот процент практически невозможно.

Как быть в такой ситуации? Необходимо принять факт наличия повторений координат. В принципе, это не является критичным, но только, если эти повторения распределены по всему множеству координат случайным образом.

Например, проведем мысленный эксперимент, если сгенерировать последовательность, которая успешно выполнит первые два критерия и покажет результат в 65% хаотичности, то, заменив все повторяющие координаты на значение, допустим, 00001111 для восьмибитных координат, то результаты теста не изменятся, а закономерность последовательности недопустимо увеличится.

Это произойдет, потому что, оба теста не определяют каким образом происходит повторение оставшихся 35% координат: они расположены закономерно относительно друг друга или равномерно распределены по всему множеству?

Возможно ли решить данную проблему? Да, но для этого необходимо вернуться к общей формуле первого критерия частотного анализа (1). Теперь ее не нужно упрощать, вместо этого, прировнять интервал изменения координаты XY из второго теста к значению разрядности числа частотного анализа m по формуле (1). Тогда получим формулу (9).

$$\left[\frac{k-2.58\sqrt{k(2^{XY}-1)}}{2^{XY}};\frac{k+2.58\sqrt{k(2^{XY}-1)}}{2^{XY}}\right] \quad (9)$$

Где размер текста тоже необходимо изменить, уменьшив его, в соответствии с разрядностью координаты, по формуле (10).

$$k=\frac{n}{XY} \quad (10)$$

Благодаря этому тесту можно убедиться в том, что 35% повторенных координат распределились по множеству случайно, а не закономерно. Также, в отличии от первого критерия, необходимо обеспечить возможность более точной интерпретации результатов третьего критерия с целью определения степени наличия закономерностей.

Достаточно будет использовать два оценочных показателя для третьего критерия: количество координат, по которым зафиксирован выхода за пределы допустимого интервала и максимальное значение выхода за допустимый интервал.

Программная реализация алгоритма шифрования

На основе вышеописанного алгоритма разработана программа-шифратор. Конфигурационный ключ (КК) программы состоит из ОК и конфигурационных настроек шифратора. Программа на данный момент позволяет шифровать текстовые сообщения и любые файлы со средней скоростью 120 килобайт/с (рис. 4). В будущем, необходимо произвести улучшение программы для увеличения показателя скорости преобразования при помощи распараллеливания шифрования блоков и многоядерных процессоров.

Одной из главных функций программы является генератор КК. Он позволяет случайным образом для каждого раунда генерировать ОК, сдвиг блока и ключа, задавать все параметры двух последовательных фрагментаций блока для замены подблоков и сложения с ключом раунда (КР). После каждой генерации КК производятся тесты на качество шифрования по заданным критериям оценки, в результате которых программа может принимать решение о повторной генерации ключа или о добавлении, уменьшении количества раундов.

Сохраненный КК можно использовать в программе или для подачи на вход библиотеке шифрования данного шифратора, программе-терминалу в случае автоматизации процесса шифрования, например, для связи с удаленной автоматической системой по беспроводному каналу или для шифрования в алгоритме протокола [11].

По результатам оценки качества шифртекста в различных ситуациях (рис. 5), можно сделать следующие выводы:

- если произвести замену хотя бы одним блоком замены по неприводимому многочлену от 120 бит и более, то это приведет к увеличению меры хаотичности и случайности шифртекста с наименьшим количеством раундов. Например, можно использовать подобные блоки замен в первых раундах. Чем больше степень неприводимого многочлена для замены, тем лучше (максимально — 240 бит);
- ключ вносит около 10% хаотичности, малые блоки 20%, средние 40%, а крупные 60%;
- случайная конфигурация очень часто приводит к необходимому результату при любом количестве раундов. Большое количество раундов может быть использовано для увеличения вариативности КК (при использования временных ключей вместо ОК) и хаотизации последовательностей со значительными закономерностями, а меньшее для повышения скорости.

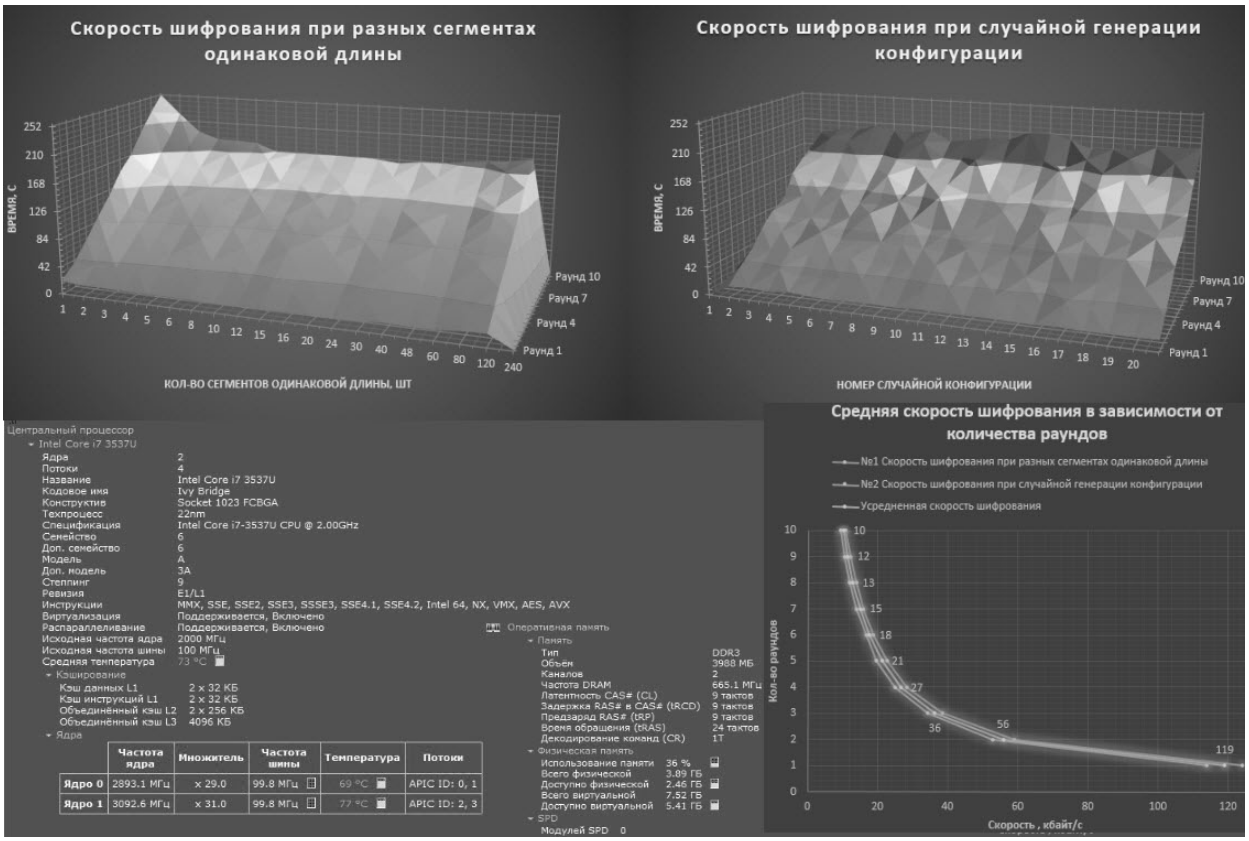


Рис. 4. Графические результаты анализа скорости и условия эксперимента

Настройки шифра	Критерий 1	Критерий 2	Настройки шифра	Критерий 1	Критерий 2
Исходный текст	✗	4.93%	- с ключом; - без замены; - 1 раунд.	✗	18.80%
- без ключа; - малые блоки; - 1 раунд.	✗	27.11%	- без ключа; - средние блоки; - 1 раунд.	✗	42.62%
- без ключа; - большие блоки; - 1 раунд.	✓	63.11%	- с ключом; - случайная конфигурация; - 1 раунд.	✓	63.68%
- с ключом; - случайная конфигурация; - 3 раунда.	✓	63.33%	- с ключом; - случайная конфигурация; - 5 раундов.	✓	63.75%

Рис. 5. Оценка качества шифртекста при разных конфигурациях

Заключение

Таким образом, удалось определить скорость шифрования алгоритма, основанного на принципе переменной фрагментации подблоков для осуществления замены. Она составляет 120 килобайт/с. Данный алгоритм был модифицирован и протестирован при помощи неприводимых многочленом размером до 240 бит. Данный алгоритм в ходе тестирования показал результаты шифртекста соответствующего результатам псевдослучайной последовательности всего за один раунд, вместо трех раундов, как это было представлено в первых исследованиях [9].

Удалось расширить количество свободных параметров алгоритма шифрования, что увеличило вариативность КК и количество возможных способов осуществления замены по неприводимым многочленам при помощи комбинирования и перестановки подблоков переменной длины. Стойкость шифра можно всегда дополнительно повысить использованием имитовставки, основанной на временных ключах в протоколе безопасного обмена данными [11].

В будущем, показатели алгоритма могут быть улучшены при помощи многоядерный процессоров, увеличения производительности вычислительных устройств, качества сред передачи данных, увеличения блока с исходными данными, а также, при помощи использования устройств большей вычислительной размерности (например, троичные компьютеры) [19].

Необходимо внедрить третий критерий для более достоверных результатов определения случайность бинарных последовательностей ключей и шифртекста. Также реализовать возможность получения неприводимых многочленов не из заранее известных таблиц, а случайным образом, осуществляя поиск неприводимого многочлена отталкиваясь от случайной бинарной последовательности, тестируя ее алгоритмом Берлекемпа и в случае неудачи, инкрементируя значение случайной последовательности, продолжать поиск до достижения успеха. Генерацию ключа необходимо проводить один раз, до начала использования алгоритма.

ЛИТЕРАТУРА

1. Голубчиков Д.М., Румянцев К. Е. Квантовая криптография: принципы, протоколы, системы. Таганрог: Таганрогский технологический институт Южного федерального университета. 37 с.
2. Пригожин И., Садовничий В. А. Квантовые компьютеры и квантовые вычисления. Москва: Международный научный журнал, № 1, 2000. 116 с.
3. Китаев А., Шень А. Классические и квантовые вычисления. 193 с.
4. Белокуров В.В., Тимофеевская О. Д. Квантовая телепортация — обыкновенное чудо. Ижевск: РХД, 2000. 256 с.
5. Манин Ю. И. Вычислимое и невычислимое. М.: Сов. Радио, 1980. 128 с.
6. Нейман И. Математические основы квантовой механики. Москва: Издательство «Наука», 1964. 366 с.
7. Садовничий В. А. Квантовые вычисления: за и против. Ижевск: Издательский дом «Удмуртский университет», 1999. 212 с.
8. Садовничий В. А. Квантовый компьютер и квантовые вычисления. Ижевск: Ижевская республиканская типография, 1999. 288 с.
9. Menezes A., van Oorshot P., Vanstone S. Handbook of Applied Cryptography // CRC Press, 1997.
10. Жданов О.Н., Соколов А. В. Алгоритм шифрования с переменной фрагментацией блока // Проблемы и достижения в науке и технике, выпуск 2. Сборник научных трудов по итогам международной научно-практической конференции, № 2; Инновационный Центр Развития Образования и Науки, г. Омск, 2015. С. 153–159.
11. Митращук В.В., Протокол безопасного обмена данными на основе алгоритма шифрования с переменной фрагментацией блока // Молодежь. Общество. Современная наука, техника и инновации [Электронный ресурс]: материалы XVI Междунар. науч. конф. бакалавров, магистрантов, аспирантов и молодых ученых (17 мая 2017, г. Красноярск): электрон. сб. / под общ. ред. И. В. Ковалёва, М. В. Савельевой, Н. А. Шумаковой; Сиб. гос. аэрокосмич. ун-т.— Красноярск, 2017. С. 299–301.
12. Лидл Р., Ниддеррайтер Г. Конечные поля: В 2-х т. Т. 1. Пер. с англ. // Мир, г. Москва, 1988, С. 430.
13. Gadiel Seroussi Table of Low-Weight Binary Irreducible Polynomials // Computer Systems Laboratory HPL-98–135, HEWLETT PACKARD, 1998, P. 16.
14. Иванов М.А., Чугунков И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. Москва: КУДИЦ-ОБРАЗ, 240 с.
15. Кнут Д. Искусство программирования для ЭВМ: В 3 т. 3-е изд. Т. 2. Пер. с англ. Москва: Мир, 1998.
16. Marsaglia G. DIEHARD Statistical Tests.
17. Gustafson H. et. al. A computer package for measuring strength of encryption a algorithms // Journal of Computers and Security. Vol. 13. No. 8, 1994, P. 687–697.
18. A Statistical Test Suite for the Validation of Random and Pseudorandom Number Generators. NIST Special Publication 800–22 [Электронный ресурс]. URL: http://csrc.nist.gov (дата обращения: 15.11.2015).
19. Zhdanov O.N., Sokolov A. V. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic // Far East Journal of Electronics and Communications Volume 16 № 3, Pushpa Publishing House, India, 2016, P. 573–589.

Журнал «Современная наука: актуальные проблемы теории и практики»