УДК 004.056.55

К. О. ЗАХАРОВА

ИССЛЕДОВАНИЕ ПАРАМЕТРОВ ШИФРОВАНИЯ АЛГОРИТМА С ПЕРЕМЕННОЙ ФРАГМЕНТАЦИЕЙ БЛОКА

Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева

В данной статье представлены рекомендации по подбору параметров алгоритма шифрования с переменной фрагментацией блока, разработанные на основе исследования полученных результатов работы алгоритма с различными параметрами шифрования (p и q). Исследование результатов работы алгоритма с переменной фрагментацией блока при выборе различных параметров проводится с использованием методик тестирования псевдослучайных последовательностей, включающих в себя статистические и графические тесты над шифрованными последовательностями с использованием различных параметров в бинарном представлении. Статистический тест выбран из подборки тестов Д. Кнут, а именно проверка корреляции. В качестве графического тестирования проводилось построение k-граммного распределения. На основе результатов исследования работы алгоритма с различными параметрами шифрования (p и q), сформулированы следующие рекомендации по подбору параметров: p и q – взаимно-простые числа, разбиение последовательности на p-подблоки больше, чем разбиение на q-подблоки (p > q).

Ключевые слова: *шифрование, алгоритм шифрования, тестирование псевдослучайных последовательностей, параметры шифрования, статические тесты, графические тесты.*

Введение

Как известно, в настоящее время активно развиваются методы криптоанализа и одновременно увеличивается быстродействие вычислительной техники. Это обуславливает необходимость дальнейшего совершенствования методов шифрования при передаче информации по открытым каналам [1].

Ранее был предложен алгоритм шифрования с динамическим изменением размеров криптографических примитивов в различных раундах [2], в работе [3] была представлена модернизация данного алгоритма, полное описание алгоритма содержится в работе [2], на рис. 1 представлена схема шифрования данным алгоритмом.

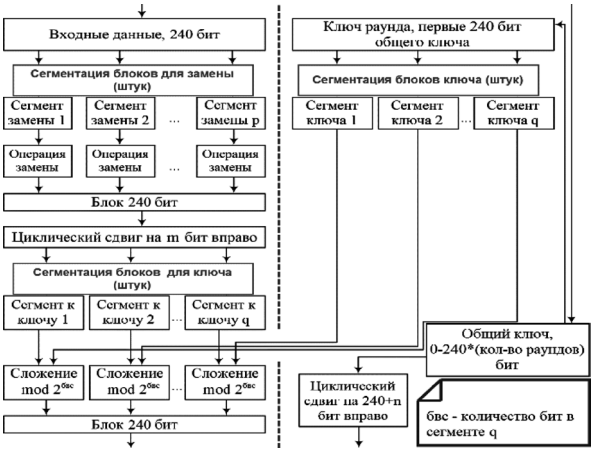

Рис. 1. Схема шифрования

Автор ставил задачу: сравнить результаты зашифрования по такому алгоритму с различными наборами значений параметров и выдать рекомендации для наиболее эффективного использования этого алгоритма.

Выбор наборов параметров для исследования алгоритма

Данный алгоритм исследуется впервые, поэтому рекомендации по подбору параметров шифрования отстутствуют. При исследовании параметров проводилось шифрование 3-х текстов, длина текста должна быть кратна 240 бит. Текст должен быть не слишком коротким и не слишком длинным, поэтому выбрана длина 240×19 = 4560 бит. Для шифрования использовались ключи длиной 240 бит разной степени стойкости. Стойкость ключа оценивалась по результатам проверки корреляции бит ключа

Таблица

	Гр. параметров 1	Гр. параметров 2	Гр. параметров 3	Гр. параметров 4
1-й раунд	($p = 4$, $q = 8$)	($p = 8$, $q = 4$)	($p = 4$, $q = 9$)	($p = 9$, $q = 4$)
2-й раунд	($p = 3$, $q = 12$)	($p = 25$, $q = 5$)	($p = 3$, $q = 8$)	($p = 8$, $q = 3$)
3-й раунд	($p = 2$, $q = 6$)	($p = 12$, $q = 3$)	($p = 5$, $q = 9$)	($p = 9$, $q = 5$)
4-й раунд	($p = 5$, $q = 10$)	($p = 6$, $q = 2$)	($p = 6$, $q = 11$)	($p = 11$, $q = 6$)
5-й раунд	($p = 6$, $q = 12$)	($p = 12$, $q = 6$)	($p = 7$, $q = 12$)	($p = 13$, $q = 7$)
6-й раунд	($p = 7$, $q = 14$)	($p = 14$, $q = 7$)	($p = 8$, $q = 13$)	($p = 15$, $q = 8$)
7-й раунд	($p = 8$, $q = 16$)	($p = 8$, $q = 16$)	($p = 2$, $q = 5$)	($p = 17$, $q = 8$)
8-й раунд	($p = 9$, $q = 18$)	($p = 18$, $q = 9$)	($p = 9$, $q = 17$)	($p = 19$, $q = 9$)

[4], всего было использовано 7 ключей. С целью выявления параметров, обеспечивающих наиболее стойкое зашифрование, использовались группы параметров, представленные в таблице. Исследовались шифрованные последовательности, полученные на каждом раунде зашифрования.

Замены в каждом раунде предлагается проводить по таблицам с нулевыми коэффициентами корреляции между каждым входным и каждым выходным битами. Выбор конкретной таблицы соответствующего размера в каждом раунде предпочтительно сделать секретным.

Все группы параметров можно классифицировать по таким характеристикам как:

– взаимно-простые p и q или кратные p и q;

– $p > q$ или $p < q$.

Исследование параметров алгоритма шифрования с переменной фрагментацией блока

Исследование параметров шифрования алгоритма с переменной фрагментацией блока проводилось на основании результатов графических и статистических тестов. Проводилось тестирование шифрованных последовательностей каждого текста, полученных в результате шифрования с использованием каждой группы параметров (табл. 1), каждого ключа.

Для анализа качества и изменения свойств шифруемой последовательности использовался показательный тест, а именно построили k-грамное распределение. Данный тест позволяет определять равномерность распределения символов в исследуемой последовательности на основе анализа частоты появления серий, состоящих из k бит. В исследовании было выбрано $k = 3$, определена равномерность распределения серии символов: $000, 001, 010, 100, 110, 011, 111$. Для последовательности, чьи свойства близки к свойствам случайной последовательности, разбросы между числом появлений серий каждого вида должны стремиться к нулю [5], в открытом тексте не наблюдается равномерного распределения серии символов. Для проведения данного тестирования было проведено пять раундов шифрования открытого текста каждой группой параметров шифрования и построены графики равномерного распределения, подробные результаты представлены в [4]. На рис. 2 представлен график распределения серий в шифрованной последовательности после 5 раундов шифрования, с использованием второй группы параметров.

Проведем сравнение графика распределения серий в шифрованной последовательности после 5-ти раундов шифрования с использованием второй группы параметров (рис. 2) с графиком распределения серий в шифрованной последовательности после 5-ти раундов шифрования с использованием четвертой группы параметров шифрования, представленным на рис. 3.

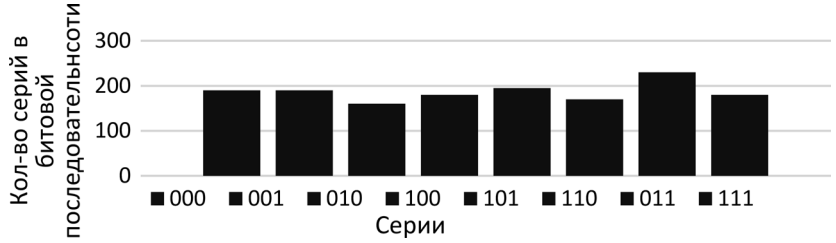

Рис. 2. Распределение серий в шифрованной последовательности второй группой параметров после 5-го раунда

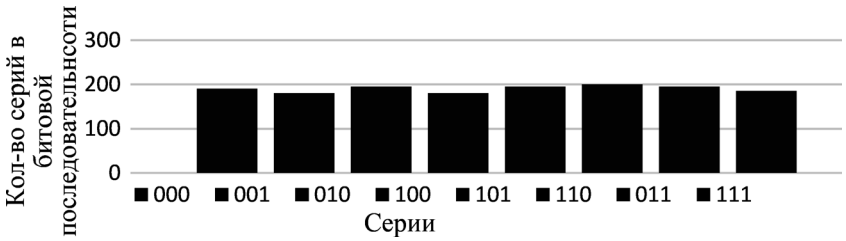

Рис. 3. Распределение серий в шифрованной последовательности четвертой группой параметров после 5-го раунда

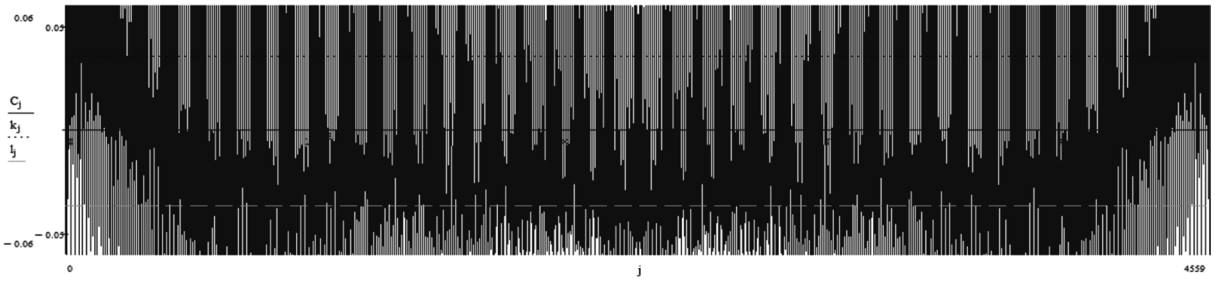

Рис. 4. График зависимости бит исходного текста

Проведя сравнительный анализ графиков, представленных на рис. 2 и рис. 3, можно сделать вывод, что свойства последовательности, полученной четвертой группой шифрования, близки к свойствам случайной последовательности, это означает что злоумышленнику будет затруднительно восстановить открытый текст из зашифрованной последовательности.

Для анализа качества шифрованных последовательностей был использован статистический тест из подборки Д. Кнута. Данный тест проверяет взаимонезависимость элементов последовательности.

Пусть $\varepsilon = \varepsilon_1\varepsilon_2\ldots\varepsilon_n$ – последовательность m-разрядных чисел длины n. Вычисляется статистика по формуле 1.

$$C_j = \Big(n(\varepsilon_0\varepsilon_j + \varepsilon_1\varepsilon_{(1+j)\bmod n} + \ldots + \varepsilon_{n-2}\varepsilon_{(n-2+j)\bmod n} + \varepsilon_{n-1}\varepsilon_{(n-1+j)\bmod n}) - (\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_{n-1})^2\Big) \Big/ \Big(n(\varepsilon_0^2 + \varepsilon_1^2 + \ldots + \varepsilon_{n-1}^2) - (\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_{n-1})^2\Big). \quad (1)$$

Для любого j значение C_j должно лежать в интервале

$$\left[\mu_n - 2{,}43\sigma_n;\ \mu_n + 2{,}43\sigma_n\right],$$

где $\sigma^2 = \dfrac{n^2}{(n-1)^2(n-2)}$ [5].

В данном исследовании используется анализ бинарных последовательностей длиной 4560 бит. Диапазон вычисляемых значений при тестировании принимает значения: [–0,036224; 0,035786]. Результат тестирования отображается в виде графика (рис. 4), на котором отображены границы вычисляемых значений тестирования. На графике границы диапазона выделены пунктиром, за пределы которого график не должен выходить, k_j – верхняя граница диапазона, l_j – нижняя граница диапазона. Выход графика за границы диапазона показывает, что прослеживается связь между битами последовательности, которая может позволить злоумышленнику вычислить открытый текст.

На рис. 4 представлен график результатов тестирования одного из исходных текстов.

Как видно по графику, представленному на рис. 4, наблюдается полная зависимость бит в открытой исходной последовательности – тест не пройден, злоумышленник легко может восстановить исходный текст из битовой последовательности.

В данной статье представлен результат проведения теста на взаимонезависимость бит шифрованной последовательности, полученной при шифровании сильным ключом K_2, это доказано проведением тестирования ключа [4]. На рис. 5 представлен график взаимонезависимости бит шифрованной последовательности после одного раунда шифрования с использованием четвертой группы параметров и ключа K_2, заметно что результат тестирования шифрованой последовательности сильным ключом уже после проведения одного раунда шифрования, с использованием рекомендуемых параметров, можно считать успешным и на данном

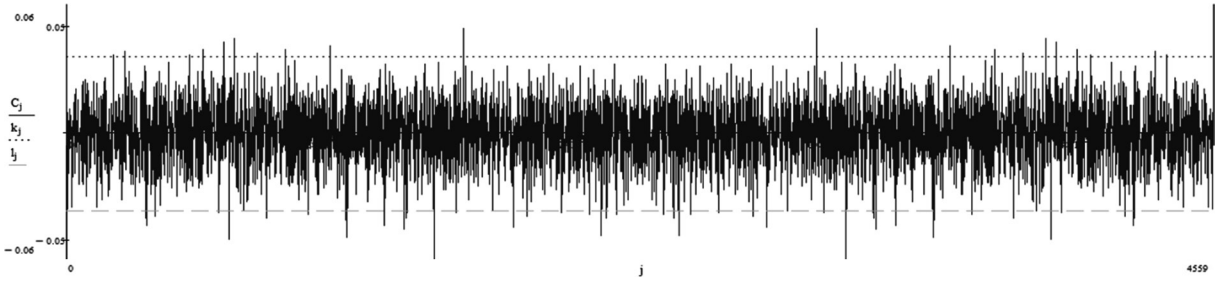

Рис. 5. Результат тестирования шифрованной последовательности ключом K_2

этапе можно предположить, что связи, просматриваемые на графике (рис. 5), аномальные. При проведении 8-ми раундов шифрования с использованием четвертой группы параметров, связей между битами в шифрованных последовательностях не прослеживается [4].

Сравнивая результаты тестирования всех шифрованных последовательностей на разных раундах [4] можно сделать вывод, что применение четвертой группы параметров для шифрования обеспечивает наиболее стойкий результат работы алгоритма. При использовании четвертой группы параметров шифрования равномерное распределения серий в шифрованной последовательности достигается за меньшее количество проведения раундов шифрования. В четвертой группе параметров выбраны такие p и q, что $p > q$ и они взаимно-простые.

Заключение

По результатам исследования параметров алгоритма симметричного шифрования с переменной фрагментацией блоков, можно сделать вывод, что данный алгоритм имеет более высокие результаты тестирования при выборе параметров таким образом, чтобы параметр разбиения блоков исходной битовой последовательности при шифровании на p-подблоки был больше параметра разбиения битовой последовательности на q-подблоки – ($p > q$), при этом параметры q и p взаимно-простые. Таким образом, можно сделать вывод, что при выборе параметров шифрования для алгоритма с переменной фрагментацией блока нужно учитывать, что увеличение количества разбиения блоков исходной битовой последовательности при шифровании на p-подблоков улучшает результат шифрования. Высокие показатели результатов тестирования алгоритма шифрования с переменной фрагментацией блоков указывают на то, что данный алгоритм может быть использован в различных областях, где требуется шифрование данных.

Литература

1. **Возможности** использования метода результативного искажения при создании сложных технических систем в высокотехнологичных отраслях промышленности/ С. Б. Коршиков, М. Н. Терентьев, М. Н. Мусолов // Электронный журнал «Труды МАИ». Выпуск № 47.

2. **Жданов О. Н., Соколов А. В.** Алгоритм шифрования с переменной фрагментаций блока. Проблемы и достижения в науке и технике / Сборник научных трудов по итогам международной научно-практической конференции. № 2. Инновационный центр развития образования и науки – Омск, 2015. – С. 153–159.

3. **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 – 2016 Pushpa Publishing House, Allahabad, India – Pages 573–589.

4. **Захарова К. О.,** Методика тестирования алгоритма с переменной фрагментацией блока. [Электронный ресурс] GoogleDrive. URL: https://drive.google.com/open?id=1-RwL2aVF5MHknqnJjYdyAx9CG-MbXB4Q.

5. **Иванов, М. А.** Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

6. **Grosek O.,** Why use bijective S-boxes in GOST-algorithm. / O. Grosek, K. Nemoga, M. Zanechal // http://www.mat.savba.sk – Slovak Academy of Sciences, Bratislava, 1998, 13 c.

7. **Елемесов К. К., Утепова Э. О.** О перспективах и возможной области применения криптоалгоритма Жданова-Соколова. Информационные и телекоммуникационные технологии: образование, наука, практика / Сборник научных трудов по итогам II международной научно-практической конференции. Том II. – Казахстан: Алматы. КазНИТУ имени К. И. Сатпаева, 2015. – С. 110–112.

References

1. **Possibilities** of use of a method of productive distortion during creation of difficult technical systems in high-tech industries of the industry. S. B. Korshikov, M. N. Terentyev, M. N. Musolov. The Trudy MAI Online magazine. Release No. 47

2. **Zhdanov O. N., Sokolov A. V.** The encryption algorithm from a variable of fragmentations of the unit. Problems and achievements in science and the technique. Collection of scientific works following the results of the international scientific and practical conference. No. 2. Innovative center of development of education and science – Omsk, 2015. – With 153–159.

3. **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 – 2016 Pushpa Publishing House, Allahabad, India – Pages 573–589.

4. **Zaharova K. O.,** Methodology for testing the algorithm with variable block fragmentation. [Jelektronnyj resurs] GoogleDrive. URL: https://drive.google.com/open?id=1-RwL2aVF5MHknqnJjYdyAx9CG-MbXB4Q.

5. **Ivanov, M. A.** Theory, application and assessment of quality of generators of the pseudorandom sequences. M. A. Ivanov, I. V. Chugunkov. – M.: KUDITs-OBRAZ, 2003. – 240 pages.

6. **Grosek O.,** Why use bijective S-boxes in GOST-algorithm. / O. Grosek, K. Nemoga, M. Zanechal // http://www.mat.savba. sk – Slovak Academy of Sciences, Bratislava, 1998, 13 c.

7. **Elemesov K. K., Utepova E. O.** On the prospects and possible scope of the Zhdanov-Sokolov crypto algorithm. Information and telecommunication technologies: education, science, practice / Proceedings of the II International Scientific and Practical Conference. Volume II. – Kazakhstan, Almaty. KazNITIU named after K. I. Satpayev, 2015. – P. 110–112.

Поступила	*После доработки*	*Принята к печати*
21.08.2017	*22.12.2017*	*15.03.2018*

Zakharova K. O.

RESEARCH OF PARAMETERS OF ENCODING OF THE ALGORITHM WITH VARIABLE FRAGMENTATION OF THE UNIT

This article presents recommendations on the selection of parameters of the encryption algorithm with variable fragmentation of the block, developed on the basis of a study of the obtained results of the algorithm with different encryption parameters (p and q). The investigation of the algorithm's work with variable block fragmentation in the selection of various parameters is performed using pseudorandom sequence testing techniques, including statistical and graphical tests on encrypted sequences using various parameters in a binary representation. The statistical test is selected from a selection of D. Knuth tests, namely the correlation check. As a graphic test, we constructed a k-gram distribution. Based on the results of the study of the operation of the algorithm with various encryption parameters (p and q), the following recommendations for the selection of parameters are formulated: p and q are mutually prime numbers, the partition of the sequence into p-subblocks is greater than the partition into q-subblocks (p > q).

Keywords: *encryption, encryption algorithm, pseudo-random sequences testing, encryption parameters, static tests, graphic tests.*

Захарова Ксения Олеговна – магистрант, Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнева.

Zakharova Ksenia Olegovna – is the master, the Reshetnev Siberian State University of Science and Technology.

E-mail: Zakharovako@gmail.com.