УДК 004.056

A METHOD FOR FORMATION PARAMETERS OF CHAOS GENERATORS BASED ON HASH FUNCTIONS

Korchynskyi V.V., Kildishev V.I., K. Alfaion, Smazhenko K.O., Valyhurskyi Y.P., Polishchuk K.V.

O.S. Popov Odessa National Academy of Telecommunications,
1 Kuznechna St., Odesa, 65029, Ukraine.
vladkorchin@ukr.net

МЕТОД ФОРМУВАННЯ ПАРАМЕТРІВ ДЛЯ ГЕНЕРАТОРІВ ХАОСУ НА ОСНОВІ ХЕШ-ФУНКЦІЙ

Корчинський В. В., Кільдішев В.Й, Аль-Файюмі Халед, Смаженко К.О., Валігурський Ю.П., Поліщук К.В.

Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Кузнечна, 1.
vladkorchin@ukr.net

МЕТОД ФОРМИРОВАНИЯ ПАРАМЕТРОВ ДЛЯ ГЕНЕРАТОРОВ ХАОСА НА ОСНОВЕ ХЭШ-ФУНКЦИЙ

Корчинский В. В., Кильдишев В.Й., Аль-Файюми Халед, Смаженко К.А., Валигурский Ю.П., Полищук К.В.

Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная, 1.
vladkorchin@ukr.net

Abstract. Recently, more and more attention has been paid to the study issues of the properties phenomenon of dynamic chaos, which has penetrated practically all areas of scientific activity, including cryptography, radio-technical transmission systems, etc. Dynamic chaos opens new possibilities for the formation of random sequences that are used in cryptographic systems. Using such sequences, it is possible to solve problems of improving the cryptographic strength of streaming encryption systems. The reason for this is that the properties of dynamic chaos, which, as a rule, apply to gamma sequences: the motion of deterministic dynamic system under certain conditions has all the properties of the noise signal; the presence of nonlinearity and non-periodicity of the process. For the formation of gamma sequences, it is proposed to use software chaos generators, which, in contrast to linear congruent generators, have much a longer period. A characteristic feature of chaos generators is that minor changes in their initial parameters lead to the formation of new values of the oscillations. This allows the formation of various trajectories of the chaotic process, on the basis of which can create almost unlimited number combinations of gamma sequences of a given length. This article proposes a method of forming the initial parameters of program chaos generators based on conversion of the hash function of the password characters of the cryptographic system user.

Key words: generator, dynamic chaos, gamma sequence, hash function, cryptographic strength, encryption.

Анотація. Останнім часом все більше уваги приділяється питанням вивчення властивостей явища динамічного хаосу, яке проникло практично в усі галузі наукової діяльності, і, в тому числі, в криптографію, радіотехнічні системи передавання та інше. Динамічний хаос відкриває нові можливості з формування псевдовипадкових послідовностей, які використовуються в криптографічних системах. За допомогою таких послідовностей можна вирішувати завдання щодо поліпшення криптографічної

стійкості систем поточного шифрування. Основою для цього є властивості динамічного хаосу, які, як правило, ставляться до гам-послідовностей: рух детермінованої динамічної системи за певних умов має всі властивості шумового сигналу; наявність нелінійності і неперіодичності процесу. Для формування гам-послідовностей запропоновано використовувати програмні генератори хаосу, які на відміну від лінійно-конгруентних генераторів мають набагато більший період. Характерною особливістю генераторів хаосу є те, що незначні зміни їх початкових параметрів призводить до утворення нових значень коливання. Це дозволяє формувати різні траєкторії хаотичного процесу, на основі яких можна створювати практично необмежену кількість комбінацій гам-послідовностей заданої довжини. У статті запропонований метод формування початкових параметрів програмних генераторів хаосу на основі перетворення хеш-функції символів пароля користувача криптографічної системи.

Ключові слова: генератор, динамічний хаос, гама-послідовність, хеш-функція криптостійкість, шифрування.

Аннотация. В последнее время все больше внимания уделяется вопросам изучения свойств явления динамического хаоса, которое проникло практически во все области научной деятельности, и, в том числе, в криптографию, радиотехнические системы передачи и т.д. Динамический хаос открывает новые возможности по формированию псевдослучайных последовательностей, которые используются в криптографических системах. С помощью таких последовательностей можно решать задачи по улучшению криптографической стойкости систем поточного шифрования. Основанием для этого являются свойства динамического хаоса, которые, как правило, предъявляются к гаммам-последовательностям: движение детерминированной динамической системы при определенных условиях имеет все свойства шумового сигнала; наличие нелинейности и непериодичности процесса. Для формирования гамм-последовательностей предложено использовать программные генераторы хаоса, которые в отличие от линейно-конгруэнтных генераторов имеют гораздо больший период. Характерной особенностью генераторов хаоса является то, что незначительные изменения их начальных параметров приводит к образованию новых значений колебания. Это позволяет формировать различные траектории хаотического процесса, на основе которых можно создавать практически неограниченное количество комбинаций гамм-последовательностей заданной длины. В статье предложен метод формирования начальных параметров программных генераторов хаоса на основе преобразования хэш-функции символов пароля пользователя криптографической системы.

Ключевые слова: генератор, динамический хаос, гамма-последовательность, хэш-функция криптостойкость, шифрование.

The phenomenon of dynamic chaos [1–3] opens new opportunities for the formation of random sequences (RS) for their application in cryptographic systems [4–6]. Prerequisites for this are the following characteristics of dynamic chaos, which, as a rule are presented to the RS: the motion of deterministic dynamic system under certain conditions has all the properties of the noise signal; as well as the presence of nonlinearity and non-periodicity of the process.

In the articles [1–3] the characteristic feature of chaos generators showed that the minor changes in the initial parameters of the process lead to a significant change in the values of generating oscillations. This makes it possible to form different trajectories of the chaotic process, on the basis of which virtually unlimited number of combinations RS of given length can be created. However, the real implementation of dynamic chaos for encryption systems requires the search of methods by which the initial parameters of the generator based on the entered password can be formed. Unfortunately, in known research [1–3] this issue is given insufficient attention. The perspective of research in this direction, which is associated with the development of new cryptographic systems based on dynamic chaos, determines the actuality of the work.

The aim of this article is to develop methods of forming the initial parameters of software chaos generators based on the entered password and transformations of hash functions.

It is known [6–10] that in the construction of cryptographic random number generators it is advisable to use a hash function. Consider the task of initializing an initial vector based on a hash function for one or more chaos generators, with which gamma sequence is formed. Clearly, the initial state of the generators should be kept secret. The hash function used must satisfy the

properties which determine its cryptographic strength [8–10]: resistance to preimage restoration; as well as resistance to collisions of the first and second genius.

Suppose that for cryptographic system of streaming encryption [4] one or more software generators of chaos of logistic mapping [3] are used, by means of which it is necessary to form several gamma sequences:

$$x_{i+1} = ax_i(1-x_i), \quad (1)$$

where a = 3,9 – control parameter; $x_i =]0...1[$ – the initial value of the chaotic sequence. Other chaos generators [1–3] can be used. For forming the initial parameters (keys) of the chaos generators it is proposed to apply the transformation of password characters using hash function. This allows to hash an array symbols of arbitrary length into bit lines of specified length (hash code).

As an example, consider password consisting of the following symbols: ^B69PvH*F7UcHv$3. The results of hashing the symbols of this password using various hash functions are given in Table 1.

By example functions SHA-512 the method of forming the initial parameters for the five sequences chaos generator (1) are considered. It should be noted that the value of the parameter a influences on the quality of the generated sequence, so the scope of its change is limited. To simplify this task, it is assumed that the value of the control parameter is constant, i.e. a = 3,9.

Table 2 presents the results of the transformation obtained hash code a66d3ea958ba943895 in the initial parameters of the chaos generator (1), whose algorithm is as follows:

1) the hash code sequence is divided into segments of numbers certain length, for example, three (line № 1, Table 2);

2) in line № 2 – the results of transformation hash code segments to decimal numbers;

3) in line № 3 – decimal numbers are transformed to real numbers y_i;

4) in line № 4 is used the transformation operation according to the following algorithm

$$x_1 = y_1;\ x_2 = 1-y_2;\ x_3 = y_3;\ x_4 = 1-y_4;\ x_5 = 1-y_5;\ x_6 = 1-y_6. \quad (2)$$

Table 1 – The results of hashing symbols password ^B69PvH*F7UcHv$3

CRC32	45b8fa89
Haval	3347217c69a19aee3468e10da3a9d585
SHA-1	8fe552437292690894e8f2a23a705413c3e72f24
SHA-256	d8b4966f7267943e74c1a4e1697af81460f8a80448b29785b5cf9c12287c3bde
SHA-384	6a28c21ba8eafe3532c950ff9f3e6894aaef016824991537f883794d80cc1342d63666bcffaa935cc38414203488bd8e
SHA-512	a66d3ea958ba9438956dae1bc6bfe74e624edb0c2034980694575e412f3ab1a4d981027e8ae79eb55f65ffff39bd3e29b5469c73bded51833abd274848b916e3

This operation is necessary to improve the statistical properties of the formed sample. As a result of the transformation the following initial parameters of the chaos generator will be obtained: $x_1 = 0,2662_1$; $x_2 = 0,661$; $x_3 = 2709$; $x_4 = 0,7766$; $x_5 = 0,2371$; $x_6 = 0,7803$.

Table 2 – Transformation of the hash code into the initial parameters of the chaos generator.

№ actions	1	2	3	4	5	…	43	M_x
1	a66	d3e	a95	8ba	943	…	e3	
2	2662	3390	2709	2234	2371	…	227	
3	0,2662	0,339	0,2709	0,2234	0,2371	…	0,023	0,237
4	0,2662	0,661	0,2709	0,7766	0,2371	…	0,023	0,481

As can be seen in line № 3 of Table 2, the obtained values of the numerical sequence in the interval from 0 to 1 with the number of members $N = 43$ have an average value S_x = 0,237. This is a significant deviation from the theoretical significance of the mathematical expectation of uniform law M_x = 0,5. For this reason, the transformation operation (2) was proposed. The results presented in line № 4 of Table 2 showed the improvement of the statistical properties of the sequence, i.e., the value S_x = 0,481.

The proposed method of forming the initial parameters (keys) of the chaos generator based on the user password symbols allows to use a different set of hash functions. The received hash code as a result of hashing can be used for transformation into the needed range numbers of the initial parameters of the used chaos generator.

REFERENCES:

1. Shahtarin B.I. Generatory haoticheskih kolebanij. M.: Gelios ARV, 2007. 248 s.

2. Kuznecov S.P. Dinamicheskij haos. M.: Fizmatlit, 2006, 356 s.

3. The generating random sequences with the increased cryptographic strength / Volodymyr Korchynskyi, Vitalii Kildishev, Oleksandr Riabukha, Oleksandr Berdnikov // IAPGOS, 1/2020. 20–23.

4. Luntovskij A.O., Zaharchenko M.V., Semenko A.I. Multiservisni mobilni platform. K.: PVP «Zadruga», 2014. 214 s.

5. Metody i sredstva zashity informacii v kompyuternyh sistemah i setyah / M.A. Ivanov, A.V. Kovalev, N.A. Macuk, I.V. Chugunkov / pod red. M.A. Ivanova. M.: KUDIC-PRESS, 2009. 602 s.

6. Osnovy Kriptografii. 2-e izd. / A.P. Alfyorov, A.Yu. Zubov, A.S. Kuzmin, A.V. Cheryomushkin. M., 2002. 480 s.

7. Federal Information Processing Standards (FIPS) Publication 180-2, Secure Hash Standard (SHS), U.S. DoC/NIST, August 1. 2002.

8. Metody generacii i testirovaniya sluchajnyh posledovatelnostej / M.B. Budko, M.Yu. Budko, A.V. Girik, V.A. Grozov. SPb: Universitet ITMO, 2019. 70 s.

9. Mordashov A.S. Statisticheskoe testirovanie rossijskogo standarta funkcii heshirovaniya GOST 34.11-2012 («STRIBOG») // Voprosy kiberbezopasnosti. (2015), No 3 (11). S. 56–59.

10. Informacijni tehnologiyi. Kriptografichnij zahist informaciyi. Funkciya heshuvannya. DSTU 7564:2014. Kiyiv: Ukrayinskij naukovo-doslidnij i navchalnij centr problem standartizaciyi, sertifikaciyi ta yakosti, 2015.

ЛІТЕРАТУРА:

1. Шахтарин Б.И. Генераторы хаотических колебаний. М. : Гелиос АРВ, 2007. 248 с.

2. Кузнецов С.П. Динамический хаос. М. : Физматлит, 2006. 356 с.

3. The generating random sequences with the increased cryptographic strength / Volodymyr Korchynskyi, Vitalii Kildishev, Oleksandr Riabukha, Oleksandr Berdnikov // IAPGOS, 1/2020, 20–23.

4. Лунтовський А.О., Захарченко М.В., Семенко А.І. Мультисервісні мобільні платформи. К.: ПВП «Задруга», 2014. 214 с.

5. Методы и средства защиты информации в компьютерных системах и сетях / М.А. Иванов, А.В. Ковалев, Н.А. Мацук И.В. Чугунков / под ред. М.А. Иванова. М.:КУДИЦ-ПРЕСС, 2009. 602 с.

6. Основы Криптографии. 2-е изд. / А.П. Алфёров, А.Ю. Зубов, А.С. Кузьмин, А.В. Черёмушкин. М., 2002. 480 с.

7.Federal Information Processing Standards (FIPS) Publication 180-2, Secure Hash Standard (SHS), U.S. DoC/NIST, August 1. 2002.

8.Методы генерации и тестирования случайных последовательностей / М.Б. Будько, М.Ю. Будько, А.В. Гирик, В.А. Грозов. СПб.: Университет ИТМО, 2019. 70 с.

9.Мордашов А.С. Статистическое тестирование российского стандарта функции хэширования ГОСТ 34.11-2012 («СТРИБОГ») // Вопросы кибербезопасности. 2015, No 3 (11). С. 56–59.

10.Інформаційні технології. Криптографічний захист інформації. Функція хешування. ДСТУ 7564:2014. Київ: Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості, 2015.

DOI10.33243/2518-7139-2020-1-2-65-69