Столыпинский
вестник

Научная статья
Original article
УДК 004.056.55

SPECIAL CODING METHOD TO INCREASE INFORMATION RELIABILITY

СПЕЦИАЛЬНЫЙ МЕТОД КОДИРОВАНИЯ ДЛЯ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ИНФОРМАЦИИ

Salmanov V.I., Ph.D, assoc. professor, Department of Informatics The Nakhchivan State University Azerbaijan Republic, Nakhchivan city, e-mail: vuqars69@mail.ru

Салманов В.И., доктор философии по математике, доцент, Кафедра информатики Нахчыванского государственного университета, Азербайджанская Республика, город Нахчыван, e-mail: vuqars69@mail.ru

Abstract

The quality of the processes of receiving, storing, processing and transmitting information is achieved by solving the problems of data management and software or hardware, security and backup. At this time, information support includes the following elements: information ring, information circulation path, information carriers, technical means of information processing. Thus, information security is a combination of a unified data coding system, unified documentation systems and data flow schemes.

Existing coding methods have some disadvantages. Among them, the reversibility of encoding, low performance, the presence of a repetition period. The

use of traditional coding algorithms leads to the complication of coding structures, and at the same time is characterized by high computational complexity. And this result, at any rate, hinders its use under conditions of serious "real" time constraints. The article is devoted to the analysis of the main problems in the field of increasing the reliability of information.

Аннотация

Качество процессов приема, хранения, обработки и передачи информации достигается за счет решения задач управления данными и программным или аппаратным обеспечением, безопасности и резервного копирования. В это время информационное обеспечение включает в себя следующие элементы: информационное кольцо, путь циркуляции информации, носители информации, технические средства обработки информации. Таким образом, информационная безопасность представляет собой сочетание единой системы кодирования данных, единых систем документации и схем потоков данных.

Существующие методы кодирования имеют некоторые недостатки. Среди них обратимость кодирования, низкая производительность, наличие периода повторения. Использование традиционных алгоритмов кодирования приводит к усложнению кодирующих структур, и в то же время характеризуется высокой вычислительной сложностью. А этот результат при всяком препятствует его использование в условиях серьезных «реальных» временных ограничений. Статья посвящена анализу основных проблем в области повышения достоверности информации.

Keywords: information, trigonometric coding, encryption, decryption

Ключевые слова: информация, тригонометрическое кодирование, шифрование, дешифрование

The transition to the construction of modern test automation systems is characterized by high intensity and instability of the data flow, high requirements for the accuracy and reliability of tests.

The high quality of information transfer, storage and processing processes is achieved by solving the problems of data and software management, security and backup.

At the same time, information support is a structural set of all documents and data (information elements) stored and circulating in an automated system.

In other words, information security is a combination of a unified data classification and coding system, unified documentation systems, data flow schemes, and at the same time a database construction methodology.

The reliability of modern encryption systems is determined, as a rule, from several main positions: a theoretical study of the properties of the crypto scheme, the study of the resulting cipher text for the presence of statistical patterns in it, the resistance of the cipher to various types of crypto attacks.

At present, there are a number of fairly reliable cryptographic protocols, the strength of which is justified formally and tested in practice.

This article discusses one of these new algorithms proposed by V.P. Sizov [4]

The cipher developed by Vladimir Sizov [4] is classified as a simple substitution stream cipher using a private symmetric key. The encryption is based on the use of periodic functions continuous over the entire numerical interval. In the simplest version, y = cos(x) and the corresponding wave equation $y = \cos(x + n\Delta x)$ are considered.

In this case, encryption is performed according to the formula

$$y = x + N \cdot [\cos(z + n\Delta x)] \pmod{N} \qquad (1)$$

For decryption, the same formula (1) is used, expressed in terms of x:

$$x = y - N \cdot [\cos(z + n\Delta x)] \pmod{N} \qquad (2)$$

Below we consider one of the possible approaches to solving the problem formulated above - the creation of a special coding method oriented to use in "real" time sources.

The trigonometric coding method is implemented by using periodic functions of the type $y = \cos(x)$ and the "wave" equation, that is $y = \cos(x + \Delta x)$. The wave equation $y = \cos(x + n\Delta x)$ is an example of one of many functions that have a constant amplitude and are continuous over the entire interval $x \in (-\infty, +\infty)$. The important point is that if for $y = \cos(x + \Delta x)$ the parameter Δx is not equal to $-\frac{2\pi}{N}$, where N is any integer, then the scaling period of this particular function is infinite.

As an example, let's encrypt the text "ABC" in the 32-letter Azerbaijani alphabet. Let us set the values z = 0,5, Δx = 12 as the key. Each character of the alphabet is assigned a half-interval: $A \to [0..1)$, $B \to [1..2)$, $C \to [2..3)$...

$$y_1 = 0{,}5 + 32 \cdot [\cos(0{,}5 + 1 \cdot 12)] + 32 = 63{,}74,$$
$$y_2 = 0{,}5 + 32 \cdot [\cos(0{,}5 + 1 \cdot 12)] = 31{,}7,$$
$$y_3 = 0{,}5 + 32 \cdot [\cos(0{,}5 + 1 \cdot 12)] - 32 = -0{,}25.$$

Of the three values y_1, y_2, y_3, we choose y_2, since it fell into the range from 0 to 32, and round the value of y_2 to a larger integer y_2=32 (Z). We encode the second character of the plaintext:

$$y_1 = 1{,}5 + 32 \cdot [\cos(0{,}5 + 2 \cdot 12)] + 32 = 62{,}61,$$
$$y_2 = 1{,}5 + 32 \cdot [\cos(0{,}5 + 2 \cdot 12)] = 30{,}61,$$
$$y_3 = 1{,}5 + 32 \cdot [\cos(0{,}5 + 2 \cdot 12)] - 32 = -1{,}38.$$

In the encoded text, respectively, we write y_2 = 31 (Y).

We encode the second character of the plaintext:

$$y_1 = 2{,}5 + 32 \cdot [\cos(0{,}5 + 3 \cdot 12)] + 32 = 60{,}22,$$
$$y_2 = 2{,}5 + 32 \cdot [\cos(0{,}5 + 3 \cdot 12)] = 28{,}22,$$
$$y_3 = 2{,}5 + 32 \cdot [\cos(0{,}5 + 3 \cdot 12)] - 32 = -3{,}78.$$

In the encoded text, respectively, we write y_2 = 29 (Ü).

As a result, we have "ZYÜ". Decryption is performed according to the formula (2). From each value obtained 32; 30; 27 subtract 0.5. This is done so that values from the middle of the segment to which the given sign belongs are substituted into the formulas.

$$x_1 = 31{,}5 - 32 \cdot [\cos(0{,}5 + 1 \cdot 12)] + 32 = 32{,}25,$$
$$x_2 = 31{,}5 - 32 \cdot [\cos(0{,}5 + 1 \cdot 12)] = 0{,}26,$$
$$x_3 = 31{,}5 - 32 \cdot [\cos(0{,}5 + 1 \cdot 12)] - 32 = -31{,}74.$$

Since 0.26 belongs to the interval [0; 1), this number corresponds to the letter A.

Finding the second letter:

$$x_1 = 30{,}5 - 32 \cdot [\cos(0{,}5 + 2 \cdot 12)] + 32 = 33{,}38,$$
$$x_2 = 30{,}5 - 32 \cdot [\cos(0{,}5 + 2 \cdot 12)] = 1{,}38,$$
$$x_3 = 30{,}5 - 32 \cdot [\cos(0{,}5 + 2 \cdot 12)] - 32 = -30{,}61.$$

Since 1.38 belongs to the interval [1; 2), this number corresponds to the letter B.

Finding the second letter:

$$x_1 = 28{,}5 - 32 \cdot [\cos(0{,}5 + 3 \cdot 12)] + 32 = 34{,}77,$$
$$x_2 = 28{,}5 - 32 \cdot [\cos(0{,}5 + 3 \cdot 12)] = 2{,}78,$$
$$x_3 = 28{,}5 - 32 \cdot [\cos(0{,}5 + 3 \cdot 12)] - 32 = -29{,}22.$$

Since 2.38 belongs to the interval [2; 3), this number corresponds to the letter C.

Recall that cryptographic strength is provided only by the secret key - a pair of real numbers z and Δx.

We can say that this cipher is secure only with respect to direct enumeration. You can improve this cipher.

Instead of trigonometric functions, one can take any periodic continuous functions defined on the entire real line. You can choose a cosine having a period of 2π. Then the expression

$$\cos(z + N(\Delta x + 2\pi)) = \cos(z + N\Delta x)$$

is valid only for the integer N, which, generally speaking, holds. Thus, the problem has not one solution, but a whole set, each of which differs by 2π in any coordinate. This "vulnerability" is also true for other modifications of the crypto scheme - it is enough to know the period of the function.

As a solution, we can consider not a point (a pair of secret parameters), but some of its neighborhood.

Theoretically, the radius of such a neighborhood should be within 1/(2N) for the Z parameter and within 1/(2Nm) for the Δx parameter. For an alphabet of N= 256 characters and texts with a length of about m = 500 characters, these values are of the order of 10^{-4} and 10^{-6}, respectively. It is obvious that the longer the text length, the smaller the radius of the neighborhood is required for its correct decoding.

Thus, the use of the coding method proposed by Sizov [4] is based on the use of trigonometric functions, while the calculations of trigonometric functions in the processor hardware can be performed in various ways, depending on the implementation of the processor itself, and having different characteristics.

Using a function with a large period, this encryption algorithm can be improved, since the period affects the number of iterations of key options with the required accuracy. If the period of the function is kπ, then the number of key options is proportional to. For example: a function with a period of 8π will have 16 times more key options than a regular function $y = \cos(x + \Delta x)$.

References

1. Aho A., Hopkroft Dj.,Ul'man Dj. Construction and analysis of computational algorithms. – Moskow, « Book on Demand» 2013. - 534 p.

2. Introduction to cryptography / Ed. ed. V.V. Yashchenko - M.: MTSNMO: "CheRo", 2012. - 348 p.
3. Knut D. The art of programming. Volume 2. Derived algorithms. - M.: "Dialectics" 2019. - 832 p.
4. Sizov V.P. Cryptographic algorithms based on trigonometric functions. URL:http://www.ruscrypto.ru/sources/conference/rc2005/

Для цитирования: Salmanov V.I. SPECIAL CODING METHOD TO INCREASE INFORMATION RELIABILITY// Научный сетевой журнал «Столыпинский вестник» №4/2022