Using the Solution of System of Linear Equations as a Key Generator of Crypto-System

Awni M. Gaftan[1] , Mizal H. Alobaidi[1] , Nihad Sh. Khalaf[2]

[1]*Dept. of Mathematics, College of comp and math. Sciences ,Tikrit University ,Tikrit , Iraq*

[2]*Dept. of Mathematics, College of education for women , Tikrit University ,Tikrit, Iraq*

(Received: 9 / 12 / 2013---- Accepted: 5 / 1 / 2014)

Abstract

In this article we used the results of mathematical model which was built as a cipher keys by transforming these results to the binary numbers to obtain a sequence of 0's and 1's and test them by standard statistic tests to guarantee a required random for this sequence .

The goal of Article

The goal of this article is to obtain a sequence of cipher keys which pass all statistic tests with good random .

Introduction

After the enormous and accelerated development in the communications equipment and means of tapping, the carrier of information became capable to penetrating especially that the physical protection become unable to prevent such instructions [5] .

Also refer to the old ways (relying on trusted correspondents) became impractical because of their Sluggishness and high cost. So there is an urgent need to use new and modern methods to ensure high security for these transmissions especially when such information has special importance. As a result of these reasons have been resorting to the use of new style ensures converting clear and understandable information (readable) to information that is understood only by the parties to the transmitter [4] .Let us define some terms before we introducing the mathematical model [2].

Plain text

Is the original intelligible text or data that is fed into the algorithm as input [2] .

Secret key

Is a code or group of codes (numbers, Character or mixture of them) are treated with the plain text using a mathematical function to obtain a cipher text , this operation called encryption or conversely treat it with the cipher text to obtain a clear text and this operation is called decryption [1] .

Cipher text

Is the scrambled message produced as output , it depends on plantext and the secret key. For a given message, two different keys will produce two different ciphertext [1]. Cryptography has great development and over in different stages, it was used initially simple encryption systems, substitution and transposition which called a hand-styled systems, it was followed by mechanical encryption stage and finally the use of electronic devices stage which opened new horizons in the use of more complicated mathematical functions. This leads to more complexity of encryption algorithms and increased the degree of security of messages.

Encryption goals

There are four goals of encryption:[3],[2].

Confidentiality

which deals with maintain the security of the information from intrusion of unauthorized people

Integrity which deals with protection of information from alteration or addition by people not authorized to do so.

Non-repudiation

It means prevent people from denying Messaging .

Authentication

Is the process of determining the identification of a user .

Cryptosystem must satisfy three general requirements

1. The enciphering and deciphering transformation must be efficient for all keys .
2. The system must be easy to use .
3. The security of the system should depend only on the secrecy of the keys and not depend on the secrecy of the algorithms .

Mathematical Model

It's possible to build a mathematical model in the following general formula [7] :

1. We are take a linear equation system in the form :

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1$$

$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2$$

.....

$$a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n$$

Then the matrix of equations of such system will be :

$$A = \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix}$$

2. Now we calculate the inverse of $(I - A)$ where $I -$ is the unit matrix .
3. We define the matrix X as:

$$X = (I - A)^{-1} B \text{ , where } B = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

4. After we found a variables values $x_1, x_2, \cdots, x_n$ we change such values to the binary representation [8] .

Thus, by changing the matrix of equations A each time we obtain new values, and continuing this process until we receive a chain of bits $(0,1)$ which represents the key.

This key must have the same length of cipher-text if we want to decrypt text or clear-text if we want to encryption.

Practical example .

Suppose that we have the following equation system:

$0.2x_{11} + 0.3x_{12} + 0.2x_{13} = 10$

$0.4x_{21} + 0.1x_{22} + 0.2x_{23} = 5$

$0.1x_{31} + 0.3x_{32} + 0.2x_{33} = 6$

Which represents a production functions in three different sectors .

Solution

We determine a matrix A

$$A = \begin{bmatrix} 0.2 & 0.3 & 0.2 \\ 0.4 & 0.1 & 0.2 \\ 0.1 & 0.3 & 0.3 \end{bmatrix}$$

Now we calculate the matrix $(I - A)$

$$I - A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 0.2 & 0.3 & 0.2 \\ 0.4 & 0.1 & 0.2 \\ 0.1 & 0.3 & 0.3 \end{bmatrix} = \begin{bmatrix} 0.8 & -0.3 & -0.2 \\ -0.4 & 0.9 & -0.2 \\ -0.1 & -0.3 & 0.8 \end{bmatrix}$$

$|I - A| = 0.384$, and notice that the determinant must not equal to zero (in such case we must choice new values to the matrix A) .

$$adj(I - A) = \begin{bmatrix} 0.66 & 0.30 & 0.24 \\ 0.34 & 0.62 & 0.24 \\ 0.21 & 0.27 & 0.60 \end{bmatrix}$$

$$(I - A)^{-1} = \frac{1}{|I - A|} adj(I - A)$$,then

$$(I - A)^{-1} = \frac{1}{0.384} \begin{bmatrix} 0.66 & 0.30 & 0.24 \\ 0.34 & 0.62 & 0.24 \\ 0.21 & 0.27 & 0.60 \end{bmatrix}$$

Next step is to find the matrix X , where $X = (I - A)^{-1} B$

1.
$$X = \begin{bmatrix} \frac{0.66}{0.384} & \frac{0.30}{0.384} & \frac{0.24}{0.384} \\ \frac{0.34}{0.384} & \frac{0.62}{0.384} & \frac{0.24}{0.384} \\ \frac{0.21}{0.384} & \frac{0.27}{0.384} & \frac{0.60}{0.384} \end{bmatrix} \begin{bmatrix} 10 \\ 5 \\ 6 \end{bmatrix} = \begin{bmatrix} 24.84 \\ 20.68 \\ 18.36 \end{bmatrix}$$

2. And the last step ,transform each value of elements the matrix X to the binary form :

We obtained 100110110100, 1000000010100, by putting these binary numbers each beside the other and repeating this process we obtained a chain of binary numbers which is the required key.

Statistic Tests

Now we must apply the statistic tests to the obtained chain, to see if it pass these tests.[6],[7]

1. Frequency Test

This test can be done by the following mathematical relation :

$X_1 = (n_0 - n_1) * 2 / N$,where N -the chain length, n_0 the number of 0s in the chain and n_1 - the number of 1s in the chain .

Let N=75***(passed)***

2. Serial Test

Suppose that we have:

$n_{00} = 6, \quad n_{01} = 6, \quad n_{10} = 8, \quad n_{11} = 8$; where :

n_{00} - present the chain type 0 0

n_{01} - present the chain type 0 1

n_{10} - present the chain type 1 0

n_{11} - present the chain type 1 1

Then we do this test by the following relation :

$$X_2 = (4/30)(36+36+64+64) - 2/31((15)2+(16)2)+1 = 0.3680 < 5.99 \textbf{(passed)}$$

Poker Test

Let

$n_0 = 0, \quad n_1 = 1, \quad n_2 = 2, \quad n_3 = 1, \quad n_4 = 2, \quad n_5 = 0$

; where n_0 - present the (block) which contain 1 and so for $n_1 \ldots, n_5$, then we obtain the result of test by the following formula :

$X_3 = (32/6)(0+1+4+1+4+0) - 6 < 0.5$

(the length of seq.) ***(passed)***

Conclusion

Using the solution of system of linear equations as a key generator of Crypto-System is a one of the non-traditional method which verifies the basis of the encryption process , and the treatment of the solutions of these systems to obtain stream of bits which pass all standard statistic tests makes this method as a new to build a cypher-keys .

Reference

1. Golek, (key generator system) Rotary Institute, Beograd , 2002.

2. Omnisec, (Solution to the correlation problem in Bruer: threshold – generator and pless- generator), Omnesic company for cryptography Equipment's. 1994.

3. Brainer K. Miladin D., (Roots of stream Cipher), Beograd, 2001.

4. Hongjun W., (A new stream cipher HC-256), Institute of infocmm research , Singapure, 2004.

5. Martin B. and others , (Rabbit: anew high–performance stream cipher) CRYPTICO A/S , Copenhagen , 2001.

6. Awney M. Kaftan and Nazar H. , (A new treatment of the attack by using correlation ship), Tikrit journal for economic and management sciences , v.4,no. 11, Tikrit, Iraq,2008.

7. Coutinho S.C. , (The mathematics of cipher , number theory and RSA cryptography), Natik Massachusetts, 2nd ed. ,2009.

8. Douglas S. , (Cryptography : Theory and practice), CRC press LLC, 3d edition , 2000.

إستخدام حل نظام من المعادلات الخطية كمفتاح توليد لنظام تشفير

عوني محمد كفطان ، مزعل حمد ذاوي ، نهاد شريف خلف

[1] *قسم الرياضيات ، كلية علوم الحاسوب والرياضيات ، جامعة تكريت ، تكريت ، العراق*

[2] *قسم الرياضيات ، كلية التربية للبنات ، جامعة تكريت ، تكريت ، العراق*

(تاريخ الاستلام: 9 / 12 / 2013 ---- تاريخ القبول: 5 / 1 / 2014)

الملخص

تم في هذا البحث استخدام نتائج حل نظام من المعادلات الخطية لتوليد نظام تشفير ، حيث تم بناء نموذج رياضي بتحويل هذه الحلول الى سلسلة من الأصفار والواحدات . كما تم اختبار هذه الطريقة بتطبيق الاختبارات الاحصائية القياسية عليها ، وقد اجتازت جميع الاختبارات .