Code 004.9

NEW BLOCK ENCRYPTION ALGORITHM

Kochladze Zurab[1], Beselia Lali[2]

[1] Ivane Javakhishvili Tbilisi State University Faculty of Exact and Natural Sciences, Department of Computer Science

[2] Sokhumi State University, Faculty of Mathematics and Computer Sciences

Abstract

This paper describes a new block encryption algorithm that uses the Hill's modified algorithm for faster efficiency process. This allows us to increase the encryption and decryption speeds so as not to reduce the algorithm's resistance to cryptanalytic attacks.

Анотація

В этом документе описывается новый алгоритм шифрования блоков, который использует модифицированный алгоритм Хилла для ускорения процесса эффективности. Это позволяет увеличить скорость шифрования и дешифрования, чтобы не уменьшать устойчивость алгоритма к криптоаналитическим атакам.

Introduction

Modern block algorithms are very often very substantially different from each other [1, 2] in both, architecture and the number of operations and rounds, but the outcome of their work is always the same. The starting line is a binary string with the length of n , whose structure is defined by the open text, by the key of length k and the use of certain operations, after the multiple iterations goes back to the n length pseudo-random bit string. In fact, any block algorithm mathematically can be imagined as function of two variables

$$E:\{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n ,$$

where $(0,1)^l$ notes bit string of l length, and k and n values depend on the specific of encryption algorithm. In practice, this means that for each fixed $K \in \{0,1\}^k$ encryption function is a replacement on $\{0,1\}^n$ bit string [3, 4]. Obviously, the received function can't be absolutely random, since the transfer is done with the determinant algorithm. This means that any such algorithm can theoretically be broken, and it can be only computationally protected against the cryptanalytic attacks. In order to prevent an opponent with limited computational resources from breaking the algorithm, it is essential that the binary string that is encrypted by encryption algorithm, will be near with a random binary string.

As it is well known, C. Shannon in his fundamental work [5] showed that to achieve this goalit is necessary, that maximal number of open-text symbols to take part in getting one symbol of cipher-text. To achieve this goal, modern bloc ciphers use several Iterations, i.e. the same block is encoded several times using different keys. Obviously, repeatting the same procedure increases the encryption time. Thus, it is better that the operations used in the rounds are more effective in this regard.

Description of algorithm

In 1930, the American mathematician L.S. Hill developed the previously existing bigram and trigram ciphers and introduced a n -gram encryption using a linear algebra [6]. The essence of the algorithm is that as it is obtained in the classical cryptography, the letters of the encrypted text will be transferred to the numbers. Then these numbers are divided into vectors of length and are multiplied to a $n \times n$ square matrix by module n , where n is the number of characters in the language on which the open text is drawn. The matrix that represents the key of this algorithm musthave a reverse matrix. It is not easy to use only crypto-text to attack the

algorithm, but it is easy to attack using open-text, because the conversion is a straight line, and if the size of the matrix is $n \times n$, then only the linear n^2 equation system is needed to accurately calculate the key. Because of these reasons, the long-term algorithm was no longer used in computer cryptography, although the multiplication operation on the matrix has a very high efficiency of diffusion. In recent years the works [7,8,9,10] have been published, the authors of which are still trying to use different options of the Hill's Algorithm due to the quality.

In the articles [11,12], the author describes Hill's modified algorithm that can be used in cipher in which the encrypted block can be viewed as a matrix of the condition (for example AES standard [13]).

Description of the algorithm: the size of the block is 128 bits. Two keys are used for encryption, each of them is 128 bits long. The open text will be viewed as ASP-II codes in binary string and will be divided into 128 bit length blocks. Before the open text will enter in first round, it gathers with the 128-bit first key with the xor operation. Each round consists with three operations: multiplication on the self-reversible matrix, shifting the bytes in matrix and gathering with the round key. The result of first operation will be divided by 16 bits (16 bytes) and will be written as a square matrix (4×4). Recording from left to right and down from the top. Bytes will be transferred in decimal systems. Received matrix is multiplied by the self-reversible matrix by mod256. In received matrix, the bytes are shifted to left by strings by one byte. The bits string will be transformed into a matrix and will enter the second round matrix will be transfer on bit string and we gather it with the second key by xor operation. The gathered bits string will be transformed into a matrix and will enter the second round. After four rounds, we get an encrypted text.

References:

1. B. Schneier. Applied cryptography, John Wiley & Sons, Inc. 1996.
2. M. Mogollon. Cryptography and Security Services. Cybertech Publishing 2007
3. R. Oppilger. Contemporary Cryptography Artech House Boston/ London 2005.
4. M. Bellare, P. Rogaway. Introduction to Modern Cryptography. -UCSD CSE 207, 2005.
5. C. Shannon. Communication theory of secrecy systems. Bell System tech. J., 28, #4 (1949), 656-715.
6. Lester S. Hill. Cryptography in an algebraic alphabet. //The American Mathematical Monthly, vol.56, #6, 1929, pp. 306-312.
7. Bibhudendra Acharya, Sarojkumar Panigrahy, Saratkumar Patra, Canapsti Panda. Image Encryption Using Advanced Hill Cipher Algorithm. // International Journal of Recent Trends in Engineering, May 2009, vol.1, No.1, pp.663-667.
8. Bibhudendra Acharya, SarojkumarPanigrahy, SaratkumarPatra, and Canapsti Panda. Image Encryption Using Advanced Hill Cipher Algorithm. International Journal of Recent Trends in Engineering. Vol.1, No.1, May 2009. pp.663-667.
9. M. Farmanbar, A.G. Chefranov. Investigation of Hill Cipher Modifications Based on Permutation and Iteration. (IJCSIS) International Journal of Computer Science and Information Security. Vol.10, No9, September, 2012. pp.1-7.
10. V.U.K.Sastry, A.Varanasi and S.U. Kumar. A Modern Advanced Hill Cipher Involving a Permuted Key and Modular Arithmetic Addition Operation
11. Z. Kochladze. Modified Version of the Hill's Algorithm. GESJ: Computer Science and Telecommunication No3 (43) 2014.
12. Georgian engineering innovations, No.1 (vol.73), 2015, pp.50. In Georgian.
13. J. Daemen, V. Rijmen The Decign of Rijndael: AES – The Advanced Encryption Standard. Springer, 2002.