Asian Journal of Information Technology 15 (13): 2248-2251, 2016
ISSN: 1682-3915


# Evolutionary Data Encryption as a Primitive Cryptography

[1]Aleksey I. Titov, [1]Nikolai I. Korsunov, [1]Vladimir V. Krasilnikov and [2]Vladimir I. Rakov
[1]Belgorod State University, Pobedy St., 85, 308015 Belgorod, Russia
[2]Orel State University, Komsomolskaya St., 95, 302026 Orel, Russia

**Abstract:** The study gives examples of encryption algorithms and their models in interpret the evolutionary method of data encryption. Considered 5 stages processing open text data unit for converting the closed text. Illustrated examples of the encoding and decoding algorithms. The application mutation of a descendant and the method of decoding messages after mutations with using Hamming codes.

**Key words:** Evolutionary method, mutation, Hamming code, parent, descendant, encoding, decoding

## INTRODUCTION

To consider the evolutionary method of encoding data (Titov and Korsunov, 2012) its positive aspects and drawbacks must be disassembled into its component method:

- Stage 1: the choice of parents
- Stage 2: crossing
- Stage 3: the formation of offspring
- Stage 4: the mutation
- Stage 5: breeding offspring

The first three stages are not new (Koops, 1999) and are present in the existing methods of cryptography has long. Accordingly, in one form or another by changing the sequence of stages and the selection criteria at each stage, we can get any of the existing symmetric ciphers.

To form a multi-lingual encryption systems, we use the 1-3 stage care with well-defined parameters at each stage:

- Stage 1: the choice of parents
- Options
- 1 parent ith, the letter of the plaintext (1 byte messages)
- 2 parent ith the letter key (key 1 byte)
- If i>lengkey then (i mod lengkey)
- Stage 2: the crossing of parents Vizhinera table or algorithm (Titov and Korsunov, 2011)
- Stage 3: the result of crossing directly recorded in the offspring

## MATERIALS AND METHODS

Algorithm GOST 28147-89 (1989) can also be represented as a special case of evolutionary encoding. In the algorithm used by 1, 2, 5 stage:

- Step 1: select the parent 1 L = 32-bit
- Select of 2 parent R = 32 bits

The parents in this case, the left and right parts 64-bit block.

- Stage 2: the crossing can be described as follows:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

- Stage 5: standard algorithm selection for selecting a descendant used 32 times iterative execution of the second stage, after which the descendant is written in a closed text

Rijndael algorithm is more sophisticated (Daemen and Rijmen, 2001) but describable model of the evolutionary method. Considering adopted as the standard algorithm with a block dimension of 128 bits select the following:

- Stage 1: select the parent is dependent on the stage of a message block+key or message block+block messages sampling of messages is carried out in a direct manner
- Stage 2: the crossing is made with the use of S-box (corresponds to the replacement of the multilingual systems) and modulo key
- Stage 3: for greater distribution in the process of forming a descendant laid shift blocks and mixing
- Stage 5: selection of offspring produced at 10, 12 or 14-round encryption, depending on the length of the key. It has no attachment but for all message the selection will be on concrete stage

**Corresponding Author:** Aleksey I. Titov, Belgorod State University, Pobedy St., 85, 308015 Belgorod, Russia

## RESULTS AND DISCUSSION

Evolutionary data encoding method can be considered a generalized method for all symmetric algorithms. From the five-step method described above in existing systems, there are various steps in a different order sequence, except step mutation.

The term "mutation" was introduced by one of the scientists who rediscovered Mendel's laws Hugo de Vries in 1901 (from the Latin Mutati Change, change). This term means the newly emerged, without crosses heritable changes. Mutations are divided into gene mutations, chromosomal mutations and genomic mutation. In the evolutionary coding occupies a special place gene mutations. When you move the definition of gene mutation in the coding of the data we obtain the following definition: genetic mutation is a mutation in which the number of changes and the importance of chromosomes or chromosome sets, without crossing.

Based on the proposed evolutionary coding models, algorithms and software for safety in case of unauthorized access. Encryption history shows us simple technology for improving the reliability.

Strengthening the DES algorithm by introducing into it the triple iteration, resulting in improved more resistant TREE DES. Here, the introduction of iterations can be compared with step #5 evolutionary method.

By optimizing algorithm Vizhinera we get the new code (Korsunov and Titov, 2010). The disadvantage of this method is the sequence of encryption and decryption. To overcome this limitation and conversion algorithm to the block structure will change (Titov and Korsunov, 2011).

The presented algorithm plays an important role during the encryption key. Even after the formation of the encryption mask can be situations that show compliance.

In the presence of an intruder large amount of decrypted and encrypted message, there is a possibility of selection of the encryption mask for messages of a particular length. Defining the encryption key, if there is an accurate mask encryption and file length of knowledge, carried out brute force.

In order to form a more stable algorithm will take the prototype current encryption standard GOST 28147-89. Its base crossing the left and right of the block and stream selection on 32th selection. In GOST 28147-89 phase selection is clearly established in the algorithm and can not be changed without the intervention of developers in the program code.

Avoid this drawback by introducing into the encryption key selection stage. In step 24, GOST 28147-89 goes direct interaction with the key and the last 8 with a reverse. This is possible due to its clearly defined number of iterations. In our algorithm, the next step is not explicitly defined, so the stage crossing will have the following representation:

**Data encryption:** Read the private key in the first and second bits. Depending on the values of the anchoring blocks of data "0" anchoring the first block of the word, "1" anchoring the second block of the word. Here, the first bit of information responsible for the first word, the second bit of the second word.

The remaining blocks are written from first word in the third position from the second word in the fourth position.

**Making the crossing C1 XOR C2 record the result in D1:** Read the private key is the 3rd bit, if:

- "0": take the last C1, C2 first (record in D2)
- "1": take the first C1, C2 last

If the number of generations that do not meet the criteria, then repeat step 1-3, wherein the encryption key moves further. An illustrative example of the encryption algorithm is shown in Fig. 1:

- Encryption key: 011100
- Input words: the first word (10001101) second word (10110110)

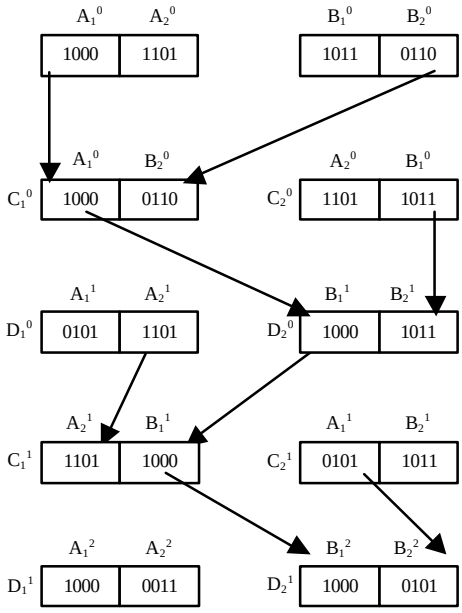


Fig. 1: The algorithm of data coding evolutionary methods

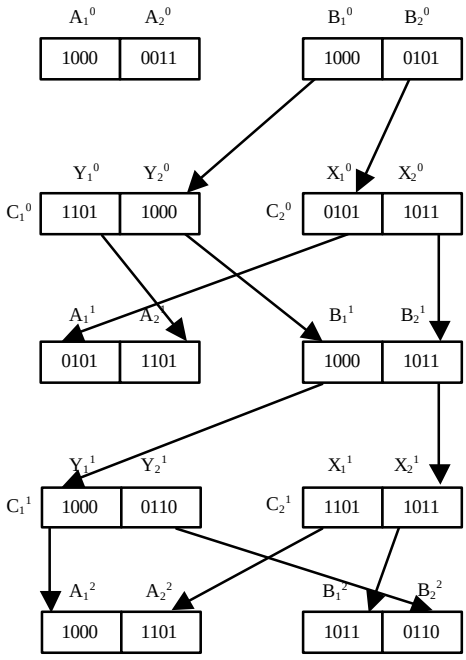


Fig. 2: Using of data decoding algorithm evolutionary methods

- The number of generations to achieve resistance: 2
- Decoding data requires a secret key used for encoding. Key exchange occurs on existing communication channels closed or during the "handshake" (Barichev *et al*., 2001)

**Decoding:** Read the key from the end. If the bit is set to "0" then $B_1^0$ in the second block word C1 ($Y_2$) and $B_2^0$ in the first block word C2 ($X_1$). If the bit is set to "1" then $B_1^0$ in the first block word C1 ($Y_1$) and $B_2^0$ in the second block word C2 ($X_2$).

Depending on the value of the read bits of the key in the previous step, we perform the restoration ancestor genotype descendants:

- If "0" then $Y_1 = (A_1^0 \text{ XOR } X_1)$; $X_2 = (A_2^0 \text{ XOR } Y_2)$
- If "1" then $Y_2 = (A_2^0 \text{ XOR } X_2)$; $X_1 = (A_1^0 \text{ XOR } Y_1)$

Read the following two bit key, depending on their values change blocks of seats, like shown in Table 1.

If the number of generations that do not meet the criteria then repeat step 1-3, wherein the encryption key moves further. An illustrative example of the data decoding algorithm is shown in Fig. 2:

- Encryption key: 011100
- Input hidden words: the first word (10000011) second word (10000101)
- The number of generations to achieve resistance

Table 1: Crossing blocks

| The value of bit key | Recording information blocks 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 00 | $A_1 = Y_1$ | $A_2 = X_1$ | $B_1 = Y_2$ | $B_2 = X_2$ |
| 01 | $A_1 = Y_1$ | $A_2 = X_1$ | $B_1 = X_2$ | $B_2 = Y_2$ |
| 10 | $A_1 = X_1$ | $A_2 = Y_1$ | $B_1 = Y_2$ | $B_2 = X_2$ |
| 11 | $A_1 = X_1$ | $A_2 = Y_1$ | $B_1 = X_2$ | $B_2 = Y_2$ |

The best result and full compliance with the evolutionary model coding will the introduction of mutation.

The mutation will be based on the known method of error-correcting "Hamming cod". Since, the proposed crossing algorithm gives us the ability to change the value of the input data blocks without difficulty, then, accordingly, this value can be secret. The idea of the proposed method "Hamming cod" error-correcting coding as follows: all of the bits, the numbers of which have a power of 2 control and the rest the message bits. Each bit is responsible for controlling the amount of parity bits of a certain group. One bit may belong to different groups. To determine which control bits control bit in position k is necessary to expand the k in powers of two: if k = 11 = 8+2+1 then this bit refers to the three groups the group whose parity is calculated in the first bit, the group the second and a group of 8th bit.

## CONCLUSION

Previously only used RSG to generate the encryption key (Proakis and Salehi, 2007) and used in the block algorithm and have never been directly part of the data modification process.

Stage mutation seems like adding control bits in the offspring and the introduction of a single random error. Without knowledge of the value of the encryption bloks to determine the location of control bits can only be in first block. For errors in the introduction of mutations will use a Random Sequence Generator (RSG) ANSI X9.17.

## REFERENCES

Barichev, S.G., S.G. Barichev, V.V. Goncharov and O.E. Serov, 2001. Fundamentals of Modern Cryptography. Hotline Telecom, Moscow.

Daemen, J. and V. Rijmen, 2002. The Design of Rijndael: AES-the Advanced Encryption Standard. Springer-Verlag, Berlin.

GOST. 28147-89, 1989. Information processing systems. Protection crypto-graphic, cryptographic transformation algorithm, State Standard of the USSR, Moscow.

Koops, B.J., 1999. The Crypto Controversy: A Key Conflict in the Information Society. Kluwer Law International, Boston, London, ISBN-13: 9789041111432, Pages: 285.

Korsunov. N.I. and A.I. Titov, 2010. Further information protection efficiency modification cipher Vizhinera. Sci. Statements BSU., 7: 171-175.

Proakis, J. and M. Salehi, 2007. Digital Communications. 5th Edn., McGraw-Hill Science Engineering Math, New York, USA., Pages: 1150.

Titov, A.I. and N.I. Korsunov, 2012. Evolutionary methods of data encoding example of the encoding and decoding algorithms. Scientific Bulletin BSU 1(120).

Titov, A.I., and N.I. Korsunov, 2011. Modified data encryption algorithm. Inf. Syst. Technol., 2: 89-89.