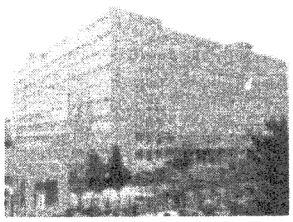
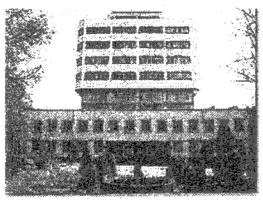
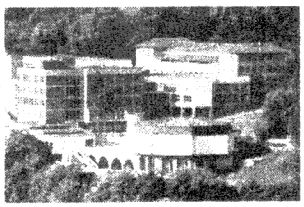
BAKU STATE UNIVERSITY

VINNYTSIA NATIONAL TECHNICAL UNIVERSITY

St. CYRIL and St. METHODIUS UNIVERSITY of VELIKO TURNOVO

Proceedings of the Forth International Conference

INTERNET EDUCATION SCIENCE

IES-2004

Volume 2

NEW INFORMATIONAL AND COMPUTER TECHNOLOGIES IN EDUCATION AND SCIENCE

AZERBAIJAN – UKRAINE – BULGARIA

September 28 – October 16, 2004

УДК 378 + 681.324
І73

Друкується за рішенням Ученої ради Вінницького національного технічного університету Міністерства освіти і науки України

Відповідальний за випуск *В. В. Грабко*

Підготовлено до друку: *В. В. Грабко, В. І. Месюра, І. Р. Арсенюк, В. В. Седлецький, О. А. Дячок*

І73 **«ІНТЕРНЕТ — ОСВІТА — НАУКА — 2004», четверта міжнародна конференція ІОН — 2002**, 28 вересня — 16 жовтня, 2004 р. Збірник матеріалів конференції. Том 2. — Вінниця: УНІВЕРСУМ-Вінниця, 2004. — 380 с.

ISBN 966-641-104-0 (том 2)

Четверта міжнародна конференція «ІНТЕРНЕТ — ОСВІТА — НАУКА — 2004» (ІОН — 2004) присвячена обговоренню питань застосування в освіті та наукових дослідженнях нових інформаційних технологій, що спираються на можливості Інтернет.

УДК 378 + 681.324

Доповіді у збірнику згруповані по секціях, відповідно до основних напрямків конференції:

Том1:

- **A** Інтернет та інформаційні технології в освіті та наукових дослідженнях
- **B** Методологія та практика дистанційної освіти
- **C** Соціальні та психологічні аспекти використання інформаційних технологій

Том 2:

- **D** Корпоративні мережі і розподілені системи керування
- **E** Інтелектуальні комп'ютерні системи
- **F** Телекомунікаційні технології для Інтернет

Матеріали доповідей представлені також на Web-сайті конференції (http:/www.vstu.vinnica.ua/ies2004), що містить електронну версію даного збірника доповнену наданими авторами перекладами окремих доповідей, і базу даних з відомостями про учасників конференції.

Тексти доповідей друкуються в авторській редакції.

ISBN 966-641-102-4 (загальний)
ISBN 966-641-104-0 (том 2)

BLOCK CIPHER BASED ON BIT INTERCHANGE

Volodymyr Luzhetsky, Vitaliy Davydyuk

Vinnytsia National Technical University
Khmelnytske Shose, 95, Vinnytsia 21021, Ukraine

Abstract

In the given report a block cipher is regarded the main feature of which is using only of interchange operation while encryption. The model of elements interchange is Rubik's cube.

In the process of encryption an information block of 512 bits is considered as a cube with the dimensions of 8x8x8.

A process of encryption lies in carrying out of consequence of such actions: transformation of one-dimensional array into three-dimensional array, interchange and transformation of three-dimensional array into one-dimensional array. Interchanges are realized in this way. A slice parallel to some plane is chosen and a rotation clockwise is done, and at this slice elements shift to new positions in the array, in other words interchange within the slice is done. For realization of the interchange 16 different slices are chosen within the whole array.

The length of private key is 124 orders.

Introduction

A great progress has been noticed last years in the branch of creation of reliable block ciphers. One of the directions is the creation of ciphers using Feistale's network. Another direction is concerned to usage of different set of mathematical operations [1]. However, even Shannon showed [2] that block ciphers can be constructed using only two main operations: substitution or replacement, or interchange. In modern ciphers, as a rule, a combination of these operations is used.

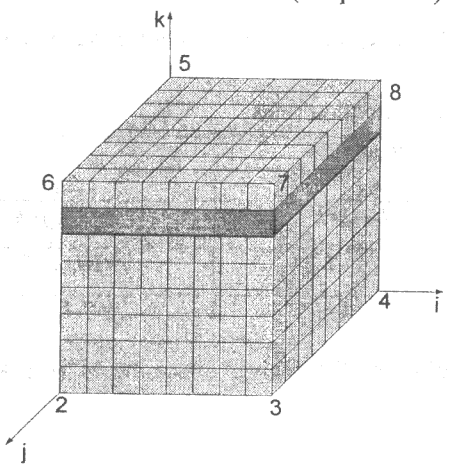
The report is regarded to a block cipher, which is suggested to realize using only interchange operations. Interchange of all symbols is possible to achieve using the procedure describing Hamilton's cycle, but it is difficult from the practical point of view.

It is proposed here to realize the interchange based on the idea of Rubik's cube.

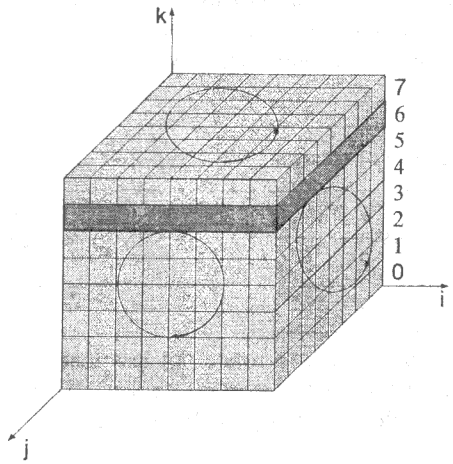
The description of the cipher

A message to be encrypted is divided into blocks of 512 bits. If the last block has a smaller size, zeroes are added to it until it has 512 bits.

In the process of encryption each block (one-dimensional array M[l], l=1,2…512) is considered as a cube with the dimensions of 8x8x8 (three-dimensional array M[i, j, k], i, j, k =0,1…7). Since the cube has eight corners, there are eight possible variants of the beginning of forming of three-dimensional array from one-dimensional (picture 1). That is assigned by original $i_П$, $j_П$, $k_П$ and finite $i_К$, $j_К$, $k_К$ coordinate values. Correspondence of number of cube corners (see picture 1) to coordinate values is shown in the table 1.



Picture 1. Three-dimensional array



Picture 2. Chosen plane in the three-dimensional array

Besides, at the process of forming of three-dimensional array a different order of coordinate change (P) is used. For example, if the P_{ijk} order is chosen, that means that first the i coordinate runs values from $i_П$ to $i_К$, and then j – from $j_П$ to $j_К$, and at last k – from $k_П$ to $k_К$. Considering this, the reflection is described by the formulas given in the table 2.

So there are 8x6=48 variants of forming of a M[i, j, k] three-dimensional array, which are assigned by the set of codes K_1K_2 taken from the table 1 and table 2.

Table 1 – Coordinate values for cube corners

Corners	$i_П$	$i_К$	$j_П$	$j_К$	$k_П$	$k_К$	Code $К_1$
1	0	7	0	7	0	7	001
2	0	7	7	0	0	7	010
3	7	0	7	0	0	7	011
4	7	0	0	7	0	7	100
5	0	7	0	7	7	0	101
6	0	7	7	0	7	0	110
7	7	0	7	0	7	0	111
8	7	0	0	7	7	0	000

Table 2 – The rules of reflection M[*l*] → M[*i, j, k*]

Coordinates change order	Code $К_2$	Formula for calculation of *l*	Coordinates change order	Code $К_2$	Formula for calculation of *l*
P_{ijk}	001	$1+i+8j+64k$	P_{jki}	100	$1+j+8k+64i$
P_{ikj}	010	$1+i+8k+64j$	P_{kij}	101	$1+k+8i+64j$
P_{jik}	011	$1+j+8i+64k$	P_{kji}	110	$1+k+8j+64i$

The model by which the interchange of elements in the M[i, j, k] array is done is the model of Rubik's cube. Interchanges are realized in this way. A slice parallel to some plane is chosen and a rotation clockwise is done, and at this slice elements shift to new positions in the array, in other words interchange within the slice is done. For realization of the interchange 16 different slices are chosen within the whole array.

Chosen slices are parallel to three planes. They are and. The number of slices parallel to every plane is 8.

Slice rotation can be realized only clockwise or only counter-clockwise, or both clockwise and counter-clockwise. In the first two cases the number of possible rotations is 3. Four rotations don't change the position of elements in a slice. In the third case there are such equivalent rotations:

1 rotation clockwise ~ 3 rotations counter-clockwise;
2 rotations clockwise ~ 2 rotations counter-clockwise;
3 rotations clockwise ~ 1 rotation counter-clockwise.

Therefore, there are two variants of sets of rotations:

the first – 1 and 2 rotations clockwise and 1 rotation counter-clockwise;
the second – 1 and 2 rotations counter-clockwise and 1 rotation clockwise.

However, the first variant is equivalent to 1, 2, and 3 rotations clockwise, and the second one – to 1, 2, and 3 rotations counter-clockwise. Therefore, any of them can be chosen for the realization. We will choose a set of 1, 2, and 3 rotations clockwise for distinctness.

The rules, according to which new coordinates of the M*[i, j, k] array elements after corresponding slice rotation are determined, are given in the table 3.

Table 3 – Coordinates transformation rules

Number of rotations	Plane		
	S_{ij}	S_{ik}	S_{jk}
1	$i=7-j, j=i$	$k=7-i, i=k$	$k=7-j, j=k$
2	$j=7-j, i=7-i$	$i=7-i, k=7-k$	$j=7-j, k=7-k$
3	$j=7-i, i=j$	$i=7-k, k=i$	$j=7-k, k=j$

It is recommended to rotate not less than 16 slices. After rotation of all the given slices the M*[i, j, k] three-dimensional array transforms into the M[l] onedimensional array.

So the following equality has place:

$$f = p \circ g \circ h.$$

The decryption function f^{-1}: $M^*[l] \to M[l]$ is a composition of such reflections:
h^{-1}: $M^*[l] \to M^*[i, j, k]$ – transformation of a one-dimensional array into three-dimensional one;
g^{-1}: $M^*[i, j, k] \to M[i, j, k]$ – additional rotations of slices;
p^{-1}: $M[i, j, k] \to M[l]$ – transformation of a three-dimensional array into one-dimensional one.
That is

$$f^{-1}=p^{-1}\circ g^{-1}\circ h^{-1}.$$

To set a p function we are to point out the number of an n_B cube corners, a P order of coordinates change, and choose a corresponding function from the table 2.

A g function is set by a collection of {S} plains, to which the chosen slices are parallel, a set of $\{n_3\}$ numbers of slices, a set of $\{n_\Pi\}$ numbers of rotations, and formulas taken from the table 3.

To set an h function we are to point out the number of an n_B^* cube corner, a P* order of coordinates change, and to choose a corresponding formula from the table 2.

Therefore, the components of a private key are:

$$n_B,\ P,\ \{S\},\ \{n_3\},\ \{n_\Pi\},\ n_B^*,\ P^*.$$

Let us determine the length of the key. Three bit codes K1 and K1* given in the table 3 correspond to the n_B and n_B^*components. P and P* orders of coordinates change are set by K2 and K2* three-bit codes (see table 2). Each plain among the 16 plains of the {S} collection is set by a K3 two-bit code according to the table 3.

Table 3 – Plain codes.

Plain	K_3 code
S_{ij}	01
S_{ik}	10
S_{jk}	11

To each among the 16 slices from the $\{n_3\}$ set a K4 three-bit common binary code.

The number of rotations for every slice given in the $\{n_\Pi\}$ collection is set by a K5 two-bit common binary code.

Considering this we have such key structure for encoding:

$$K_1K_2K_{3,1}K_{4,1}K_{5,1}K_{3,2}K_{4,2}K_{5,2}...K_{3,16}\,K_{4,16}\,K_{5,16}K_1^*K_2^*$$

The key length is 124 bits. In the process of encryption key components are read starting from the left.

Three arrays are needed for program realization: one for storage of the key, the second for storage of a block with a message, and the third backup array.

For decryption the key components are to be read starting from the right and besides $K_{5,i}$ (i=1,2,...,16) codes are to be replaced by their supplements to 4.

For key generation any procedure of generation of a pseudorandom consequence can be used. But at this consequences meeting such conditions 0are to be discarded:

1) it has at least one $K_{3,i}$ (i=1,2,...,16) component encoded as 00;

2) it has eight or more $K_{5,i}$ encoded as 00;

3) $(K_{3,i} = K_{3,i+1}) \wedge (K_{4,i} = K_{4,i+1}) \wedge (K_{5,i} = (K_{5,i+1})_{доп})$;

4) $(K_{3,1} = K_{3,2} = \ldots = K_{3,16}) \wedge (K_{4,1} = K_{4,2} = \ldots = K_{4,16})$, where $(K_{5,i+1})_{доп}$ is a supplement to 4.

According to this method to encrypt and decrypt one bit from 16 to 32 operations are needed (depending on the key). This means that the encryption based on the given method can be realized more quickly than ones based on well-known block ciphers.

References:

[1] Chmora A. L. Modern applied cryptography.

[2] Schenon K. Information and cybernetics works.