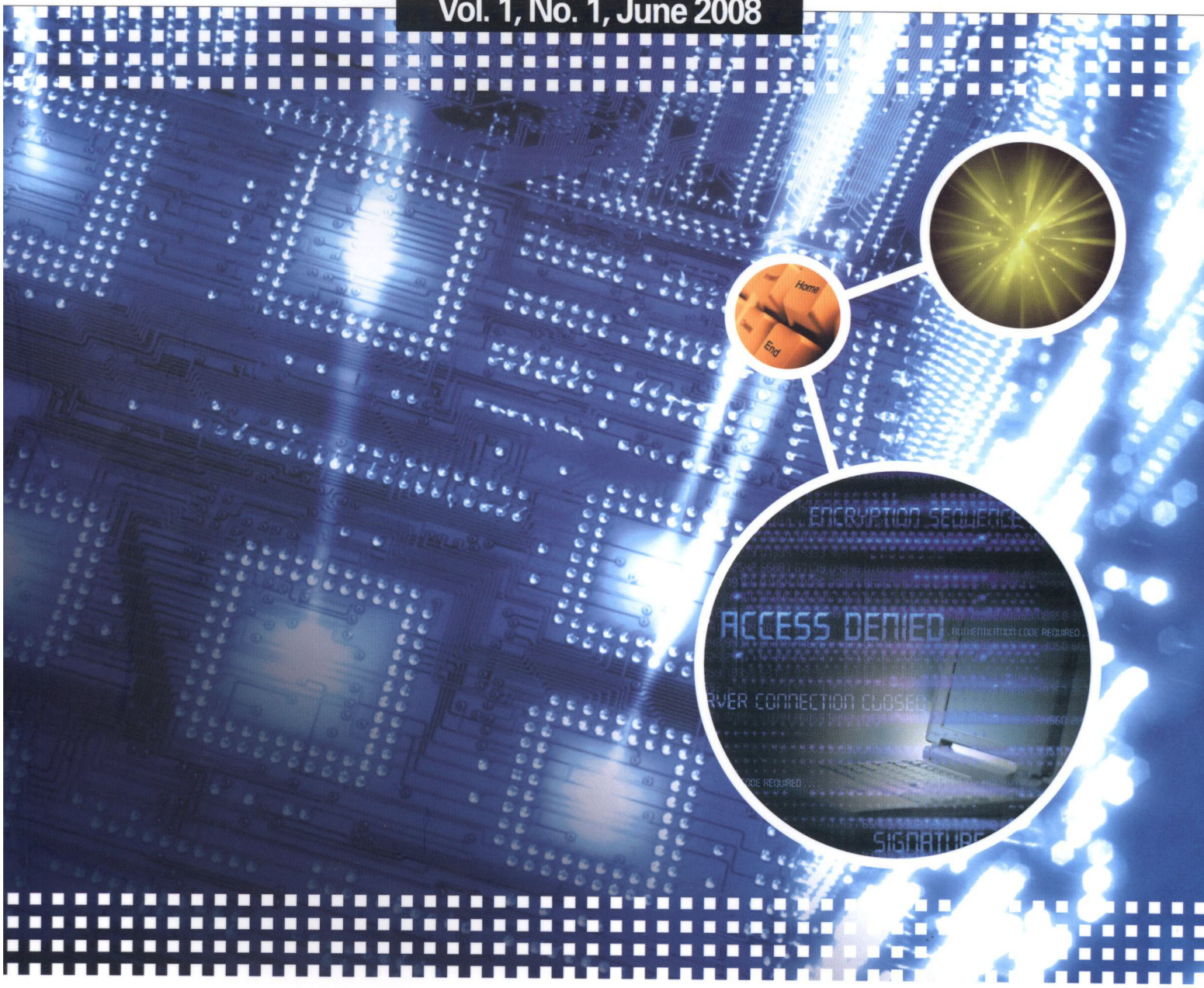
ISSN : 2005-1182

International Journal of Ubiquitous Computing and Internationalization

Vol. 1, No. 1, June 2008



Information Technology Internationalization Research Center
ITIRC

International Journal of Ubiquitous Computing and Internationalization

Vol. 1, No. 1, June 2008

C/O/N/T/E/N/T/S

ITIRC

Information Technology
Internationalization Research Center
ITIRC

International Journal of Ubiquitous Computing and Internationalization
Vol. 1, No. 1, June 2008, pp. 13-16

Hybrid cryptosystem based on Private Box Algorithm in vital electronic information exchange

Khamdomov Rustam Khamdamovich*, Kodirov Nodir Khomidjonovich
Tashkent University of Information Technology (TUIT)

(Received September 25, 2007 : accepted March 12, 2008)

Abstract

In this paper we propose new hybrid cryptosystem, which based on Private Box Algorithm, where actual structure of this algorithm includes asymmetric key agreement crypto protocoland symmetric binary information encryption algorithm. On this algorithm special way of generating encryption keys, based on pre-agreed key and using it as a seed parameter, is explained step-by-step within real example. Crypto system is supposed to use in secure electronic document exchange systems, vital information storage and mobile payment systems.

Keyword : Cryptography, rucksack problems, pseudorandom sequence, superincreasing rucksack

1. Introduction

Private box algorithm based on rucksack problems, which were first offered in 1979 by Ralph Marklin and Martin Hellman. That algorithm was one of algorithms which used rucksack systems and exchanged by elements through public channel after using modular arithmetic calculation for each element /1/. In suggested algorithm rucksack elements generate separately by each abonent on the basis of private parameter. The name «*private box algorithm*» is followed from it. *Pseudorandom* numbers are used to generate private keys, which have predefined pattern /2/.

2. Private Box Algorithm

Assume, A and B abonents want to exchange with messages. A bonent A is - sender, and abonent B - is receiver here. To exchange by messages they follow these calculating steps.

1. Both abonents generate common private parameter $e_A^Z = e_B^Z = e^Z$ via some kind of key generating algorithms, such as Diffie-Hellman.

For ciphering open message

$X = \{x_1, x_2, \cdots, x_l\}$

which contains letters of Z-alphabet, abonent B generates n-elements of private box

$$K^Z = \left\{k_1^Z, k_2^Z, \ldots, k_n^Z\right\}$$

on the based on private parameter e^z, using generator of superincreasing *pseudorandom numbers*[1]. After it codes of letters of open text - $X = \{x_1, x_2, \cdots, x_l\}$ will be taken, where length of each binary code equals to d. Merging binary code of characters to one sequence and divide it into m blocks we have *modified open text*,

$$X' = \left\{ x_{11}', x_{12}', \ldots, x_{1n}' \quad x_{21}', x_{22}', \ldots, x_{2n}' \quad \cdots \quad x_{m1}', x_{m2}', \ldots, x_{mn}' \right\}$$

where each block has length n. By scalar multiplication of modified open text X' and K^z we take integer cipher $S = \{S_1, S_2, \cdots, S_m\}$.

$$X' = \{1\ 1\ \cdots\ 0\ 1\ 1\ \cdots\ 1\ 0\ 1\ \cdots\ 1\}$$
$$X' = \left\{x_{11}'\ x_{12}'\ \cdots\ x_{1n}'\ x_{21}'\ x_{22}'\ \cdots\ x_{2n}'\ \cdots\ x_{m1}'\ x_{m2}'\ \cdots\ x_{mn}'\right\}$$
$$K^z = \left\{k_1^z\ k_2^z\ \cdots\ k_n^z\ k_1^z\ k_2^z\ \cdots\ k_n^z\ k_1^z\ k_2^z\ \cdots\ k_n^z\right\}$$
$$\mathrm{S} = \{x_{11}' \cdot e_1 + \cdots + x_{1n}' \cdot e_n = S_1\ \ x_{21}' \cdot e_1 + \cdots\ x_{2n}' \cdot e_n = S_2 \cdots$$
$$x_{m1}' \cdot e_1 + \cdots\ x_{mn}' \cdot e_n = S_m\}$$

and we send it to A abonent.

2. Maintaining foregoing scheme abonent A also generates n elements of superincreasing private box via $K^z = \left\{k_1^z, k_2^z, \cdots, k_n^z\right\}$ his private parameter e_A^Z.

*Corresponding author: r.hamdamov@msu.uz

1. Method of generating described below.

To obtain modified open text

$$X' = \{x'_{11}\ x'_{12}\ \cdots\ x'_{1n}\ x'_{21}\ x'_{22}\ \cdots\ x'_{2n}\ \cdots\ x'_{m1}\ x'_{m2}\ \cdots\ x'_{mn}\}$$

from cipher $S=\{S_1,S_2,\cdots,S_m\}$ abonent A analysis once $K^Z=\{k_1^Z,k_2^Z,\cdots,k_n^Z\}$ right to left, i.e. for each element of $S_j=\{s_1,s_2,\cdots,s_m\}$, $j=1,2,\cdots,m$

$$S_j=\begin{cases} S_j, & \text{if } S_j < k_i^Z \\ S_j - k_i^Z, & \text{if } S_j \geq k_i^Z, \quad i=1,2,\ldots,n; \quad j=1,2,\ldots,m \end{cases}$$

condition is checked. Here if condition $S_j \geq k_i^z$ is true (it means, on formation of the cipher $S_j=\{s_1,s_2,\cdots,s_m\}$, $j=1,2,\cdots,m$ - K_i^Z was used), we have to put '1' in appropriate index of X'_j, $j=1,2,\cdots,m$ alternatively we have to put '0'. Repeating this cycle for each element of $S_j=\{s_1,s_2,\cdots,s_m\}$, $j=1,2,\cdots,m$ we have modified open text, where length of them equals to n. Collecting on sequence all items of modified text X'_j, $j=1,2,\cdots,m$ we have full present of open text $-X$. We divide it to parts where the length is the same as length of binary presentation of letter in Z alphabet. After putting them on appropriate succession we will restore open text $X=\{x_1, x_2,\cdots,x_l\}$.

3. The generating of box elements on the base of private parameter

For determination of number of box elements $-n$ binary length of e^z is taken, i.e. the minimum number n, which is response for condition $e^z \leq 2^n$.

Box's elements are superincreasing, i.e. the value of next element is greater than total sum of all previous. We can express such condition by following,

$$e_j > \sum_{i=1}^{j-1} e_i, \quad j=2,3,\ldots,n.$$

Following instructions will be taken for generation of such vector. On the base on private parameter $-\ e^Z$ pseudo-random sequence

$$T=\{t_1,t_2,\ldots,t_r\}$$

with the $r-$number of elements is generated and sorted in increasing order. The first element of classified vector is taken as the first box element, i.e. $k_1^z = t_1$. For the next element $-\ k_2^z$, we take such t_j, which responsible to

$$t_j > 2\cdot k_1^Z, \quad j=2,3,\ldots,r$$

condition.

Proof. It must be proved, that the clause $t_j > 2\cdot k_1^z$, $j=2,3,\cdots,r$ provides superincreasing characteristics, that is $k_{i+1}^Z > \sum_{j=1}^{j=i} k_j^Z$.

Using induction method, assume for the sequence

$$K^Z=\{k_1^Z,k_2^Z,\ldots,k_{i-1}^Z,k_i^Z,k_{i+1}^Z,\ldots,k_n^Z\}$$

is done the condition $k_i^Z > \sum_{j=1}^{j=i-1} k_j^Z$, then

$$k_{i+1}^Z > 2\cdot k_i^Z \Rightarrow k_{i+1}^Z = k_i^Z + k_i^Z > k_i^Z + \sum_{j=1}^{j=i-1} k_j^Z = \sum_{j=1}^{j=i} k_j^Z$$

$$\Rightarrow k_{i+1}^Z > \sum_{j=1}^{j=i} k_j^Z$$

from it feasibility of $k_{i+1}^Z > \sum_{j=1}^{j=i} k_j^Z$ is correct, which required to prove.

Thus, if the elements are taken from condition $k_{i+1}^Z > 2\cdot k_i^Z$, they become superincreasing. Keeping on this way, instead of k_i^Z i = 1..n we should take t_j, for which the condition

$$t_j > 2\cdot k_i^Z, \quad j=1,2,\ldots,r; \ i=1,2,\ldots,n$$

is done, once we have superincreasing box

$$K^Z=\{k_1^Z,k_2^Z,\ldots,k_n^Z\}$$

with the element n.

4. The example of crypto algorithm

Cryptosystem has two public parameters $q=71$ and $p=89$, which are available for everybody and used for generation of shared private parameter with the Diffie-Hellman key generation algorithm. Latin alphabet is used for exchange message. Appropriate codes and binary present

a	b	c	d
1=00001	2=00010	3=00011	4=00100
e	f	g	h
5=00101	6=00110	7=00111	8=01000
i	j	k	l
9=01001	10=01010	11=01011	12=01100
m	n	o	p
13=01101	14=01110	15=01111	16=10000
q	r	s	t
17=10001	18=10010	19=10011	20=10100
u	v	w	x
21=10101	22=10110	23=10111	24=11000
y	z		
25=11001	26=11010		

of letters are given below. In this example binary length of characters equals to 5, however in real applications it can be longer, for instance in web applications which use ASCII character encoding bit length equals to 8 and in international UNICODE encoding character bit length equals to 16.

Here, key bit length $d = 5$.

1. Abonent A chooses $\alpha = 131$ and B $\beta = 37$ as private parameter, which used for generation of common private parameter $e_A^Z = e_B^Z = e^Z = 24$ via Diffie-Hellman algorithm. Presenting private parameter $e^Z = 24_{10} = 11000_2$ on binary view we have amount of box elements $n = 5$ and this is the minimum number which holds

$$e^Z \le 2^n \quad n > 0 \quad 26 \le 2^5 \quad \Leftrightarrow \quad 26 \le 32 \quad n > 0$$

clause.

For cipher message $X =$ "*algoritm*" abonent B generates $r = 15$ pseudorandom number sequence

$$T = \{t_1, t_2, \cdots, t_r\}$$
$$= \{17,6,4,13,9,37,20,22,49,62,43,75,93,89,95\}$$

on the base of private parameter $e^z = 24$.

To obtain superincreasing box elements, pseudorandom number sequence had to be sorted on increasing order

$$T' = \{t_1, t_2, \cdots, t_r\}$$
$$= \{4,6,9,13,17,20,22,37,43,49,62,75,89,93,95\}$$

from here $k_1^Z = t_1 \Rightarrow k_1^Z = 4$. Ongoing such way and keeping request

$$k_i^Z > 2 \cdot k_{i-1}^Z, \quad i = 2,3,\ldots,n$$

we can compute remained elements

$$K^Z = \{4,9,20,43,89\}$$

base on pseudorandom number sequence t_j, $j = 1,2,\cdots,r$.

Binary representation of message $X =$ "algoritm"

$$a = 00001 \quad l = 01100 \quad g = 00111 \quad o = 01111$$
$$r = 10010 \quad i = 01001 \quad t = 10100 \quad m = 01101$$
$$X = \text{"0000101100001110111110010010011010001101"}$$

divided to $m = 8$ blocks, where each block has same length as binary presentation of letter in Z alphabet $n = 5$ and there we obtain modified open text. Here '0' is set on unfilled places. By scalar multiplication X' and K^Z we take integer cipher $S_j = \{s_1, s_2, \cdots, s_m\}$, $j = 1,2,\cdots,m$.

$X' = \{0\,0\,0\,0\,1 \quad 0\,1\,1\,0\,0 \quad 0\,0\,1\,1\,1 \cdots 0\,1\,1\,0\,1\}$
$K^Z = \{4\,9\,20\,43\,89 \quad 4\,9\,20\,43\,89 \quad 4\,9\,20\,43\,89 \quad \cdots \quad 4\,9\,43\,89\}$
$S = \{4{\cdot}0+\cdots+89{\cdot}0=89 \quad 4{\cdot}0+\cdots+89.0=29 \quad 4{\cdot}0+\cdots+89.1=152\cdots \quad 4{\cdot}0+\cdots+89.1=118\}$

Cipher $S = \{89,29,152,161,47,98,24,118\}$ is send to abonent A.

2. Maintaining foregoing scheme abonent A also generates $n = 5$ and $K^Z = \{4,9,20,43,89\}$. To obtain modified open text

$$X' = \{x'_{11}, x'_{12}, \cdots, x'_{1n} \; x'_{21}, x'_{22}, \cdots, x'_{2n} \; \cdots \; x'_{m1}, x'_{m2}, \cdots, x'_{mn}\}$$

from cipher $S = \{89,29,152,161,47,98,24,118\}$ abonent A analysis once

$$K^Z = \{k_1^Z, k_2^Z, \cdots, k_n^Z\}$$

right to left, i.e. for each element of $S_j = \{s_1, s_2, \cdots, s_m\}$, $j = 1, 2, \cdots, m$. In case of the last element $S_8 = 118$, at first $x'_1 =$ "" and after

$$s_8 \ge k_5^Z (118 \ge 89) \quad x'_1 = \text{"1"} \quad s_8 = 118 - 89 = 29;$$
$$s_8 < k_4^Z (29 < 43) \quad x'_1 = \text{"01"} \quad s_8 = 29;$$
$$s_8 \ge k_3^Z (29 \ge 20) \quad x'_1 = \text{"101"} \quad s_8 = 29 - 20 = 9;$$
$$s_8 \ge k_2^Z (9 \ge 9) \quad x'_1 = \text{"1101"} \quad s_8 = 9 - 9 = 0;$$
$$s_8 < k_1^Z (0 < 4) \quad x'_1 = \text{"01101"} \quad s_8 = 0;$$

calculations we have

$$X' = \text{"00001 01100 00111 01111 10010 01001 10110 01101"}$$

modified open text. Dividing it to parts, which the length is the same as length of binary presentation of letter in Z alphabet $d = 5$,

$$00001 = a \;\; 01100 = l \;\; 00111 = g \;\; 01111 = o \;\; 10010 = r \;\; 01001 = i \;\; 10100 = t \;\; 01101 = m$$

and set them on appropriate sequence we restore open text $X =$ "algoritm".

5. Conclusion

While this cryptosystem is hybrid crypto system it includes asymmetric key exchange generating Diffie-Hellman algorithm and symmetric encryption algorithm for further information exchange, using previously generated key as a seed parameter of actual encryption keys. As robustness and length of cipher depends on key length, different key length can be used, according to security of information. For instance, in multi level management systems such as government administering, different key bit length can be used depending on priority of authority or in Bank transfer system key bit length should be used according to transfer amount.

Now authors of paper are working on implementations

of this algorithm in electronic document management system. Where this system enables secure exchange of electronic documents, using Private Box Algorithm and international encryption standards, like DES (Data Encryption Standard), TDES (DESede) GOST 28147-89 (Russian Encryption algorithm).

As we mentioned previously, cipher text length and robustness varies according to key bit length, while small bit length can be used in mobile devices. But specific requirements to key bit length and mobile device properties are subject to research.

References

[1] Bruce Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994.

[2] Khamdamov R.Kh., Ergashev A.K. Решение задачи о р юкзаке методом обобщенных неравенств, Сб. научн ых трудов ТашГТУ, 1993.

[3] A. Salomaa, Public-Key Cryptography, Springer-Verlag, 1990.

[4] S. Barichev, Криптография без секретов.

[5] "Handbook of Applied Cryptography," by Alfred J. Menezes, Paul C. van Oorschot, and Scott Vanstone. CRC Press; ISBN: 0-8493-8523-7.

[6] "A Course in Number Theory and Cryptography," by Neal Koblitz. Springer-Verlag; ISBN: 0-387-94293-9. An excellent graduate-level mathematics textbook on number theory and cryptography.

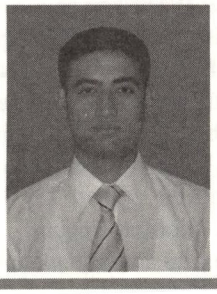
■ Authors ■

Khamdamov Rustam Khamdamovich (r.hamdamov@msu.uz)

Rustam Kh. Khamdamov was born in 1957. He received the B.E of applied mathematics from Tashkent State University at 1979. In 1984, he received Ph.D of technical science from Academy of Sciences of the Republic of Uzbekistan/Institute of Cybernetics/Uzbek scientific production company "Cybernetics". He also received Ph.D of technical science from Tashkent State Technical University at 1992.

He joined in the Academy of Sciences of the Republic of Uzbekistan, Institute of Cybernetics and Uzbek scientific production company "Cybernetics" from 1979 to 1990 as a scientist. He was consecutively vice-rector on information technologies, vice-rector of science, dean of faculty and chief of software solutions of computing machines and automatic systems department. From 2004 to 2005, he was a first deputy director of UzInfocom (Center of development and introduction of computer and information technologies) within Uzbek Agency of communications and information. At present, he is a vice-rector of Tashkent University of Information Technologies since 2004.

Kodirov Nodir Khomidjonovich (nodir_qodirov@yahoo.com)



Kodirov Nodir Khomidjonovich was born in Bukhara province of Uzbekistan in 1986. He received the B.E of e-Commerce from the department of Information Technology of TUIT (Tashkent University of Information Technologies) in 2008. He also completed the course of Young developers training and support center and Diploma in Web Technology from Jawaharlal Nehru Indo-Uzbek Centre for Information Technology. His interested fields are biological classification, physiology and logic.