Private box algorithm

Rustam Kh. Khamdamov, Tashkent University of Information Technology (TUIT),
r.hamdamov@msu.uz

Nodir Kh. Qodirov, Tashkent University of Information Technology (TUIT),
nodir_qodirov@yahoo.com

Abstract. In this paper, we propose new form of crypto algorithm, which based on rucksack problem. On this algorithm special way to generate private keys is explained and shown with an example. Algorithm is supposed to use in payment systems, data security and some more problems of e-Commerce.

Keywords. Cryptography, rucksack problems, pseudorandom sequence, superincreasing rucksack.

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 saperately by each abonent on the basis of private paramater. The name «*private box algorithm»* is follwed from it. *Pseudorandom* numbers are used to generate private keys, which have predefined pattern /2/.

Private Box Algorithm. Assume, *A* and *B* abonents want to exchange with messages. Abonent *A* is – sender, and abonent *B* – is reciever 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.
2. For ciphering open message $X = \{x_1, x_2, \dots, x_l\}$, which contains letters of Z - alphabet, abonent *B* generates n - elements of private box $K^Z = \{k_1^Z, k_2^Z, \dots, k_n^Z\}$ on the based on private parameter e^Z , using generator of *superincreasing pseudorandom numbers* [1] . After it codes of letters of open text - $X = \{x_1, x_2, \dots, x_l\}$ 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*,

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

where each block has length n . By scalar multiplication of modified open text X' and K^Z we take integer cipher $S = \{s_1, s_2, \dots, s_m\}$.

$$X' = \{1 \quad 1 \quad \dots \quad 0 \quad 1 \quad 0 \quad \dots \quad 1 \quad \dots \quad 0 \quad 1 \quad \dots \quad 1\}$$
$$X' = \{x'_{11} \quad x'_{12} \quad \dots \quad x'_{1n} \quad x'_{21} \quad x'_{22} \quad \dots \quad x'_{2n} \quad \dots \quad x'_{m1} \quad x'_{m2} \quad \dots \quad x'_{mn}\}$$
$$K^Z = \{k_1^Z \quad k_2^Z \quad \dots \quad k_n^Z \quad k_1^Z \quad k_2^Z \quad \dots \quad k_n^Z \quad \dots \quad k_1^Z \quad k_2^Z \quad \dots \quad k_n^Z\}$$
$$S = \{x'_{11} \cdot e_1 + \dots + x'_{1n} \cdot e_n = s_1 \quad x'_{21} \cdot e_1 + \dots + x'_{2n} \cdot e_n = s_2 \quad \dots \quad x'_{m1} \cdot e_1 + \dots + x'_{mn} \cdot e_n = s_m\}$$

And we send it to *A* abonent.

[1] Method of generating described below

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

For getting modified open text

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

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

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

condition is checked. Here if condition $\mathrm{S_j} \ge k_i^Z$ is true (it means, on formation of the cipher $S_j = \{s_1, s_2, \dots, s_m\}, \quad j = 1,2,\dots,m$ - k_i^Z was used), we have to put '1' in appropriate index of $X'_j, \quad j = 1,2,\dots,m$, alternatively we have to put '0'. Repeating this cycle for each element of $S_j = \{s_1, s_2, \dots, s_m\}, \quad j = 1,2,\dots,m$ we have modified open text, where length of them equals to n. Collecting on sequence all items of modified text $X'_j, \quad j = 1,2,\dots,m$ 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 $X = \{x_1, x_2, \dots, x_l\}$.

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 $e^Z \le 2^n, \quad n > 0$.

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,

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

Following instruction will be taken for generation of such vector. On the base on private parameter – e^Z pseudorandom sequence

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

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

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

condition.

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

Using induction method, assume for the sequence

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

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

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

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 $k_i^Z \quad i = 1..n$ 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 $K^Z = \left\{k_1^Z, k_2^Z, \ldots, k_n^Z\right\}$ with the element n.

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 of letters are given below.

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

Here, binary 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

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

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

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

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

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

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

we can compute remained elements $K^Z = \left\{4, 9, 20, 43, 89\right\}$ base on pseudorandom number sequence $t_j, \quad j = 1,2,\ldots,r$.

Binary representation of message $X =$ "*algoritm*"

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

$X =$"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 $S_j = \{s_1, s_2, \ldots, s_m\}, \quad j = 1,2,\ldots,m$.

$X^{'} = \{\ 0\ \ 0\ \ 0\ \ 0\ \ 1 \qquad 0\ \ 1\ \ 1\ \ 0\ \ 0 \qquad 0\ \ 0\ \ 1\ \ 1\ \ 1 \quad \ldots \quad 0\ \ 1\ \ 1\ \ 0\ \ 1\ \}$

$K^{Z} = \{4\ \ 9\ \ 20\ \ 43\ \ 89 \qquad 4\ \ 9\ \ 20\ \ 43\ \ 89 \qquad 4\ \ 9\ \ 20\ \ 43\ \ 89 \quad \ldots \quad 4\ \ 9\ \ 20\ \ 43\ \ 89\}$

$S = \{4\cdot 0 + \ldots + 89\cdot 1 = 89 \qquad 4\cdot 0 + \ldots + 89\cdot 0 = 29 \qquad 4\cdot 0 + \ldots + 89\cdot 1 = 152 \ldots\ 4\cdot 0 + \ldots + 89\cdot 1 = 118\}$

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 $K^{Z} = \{4, 9, 20, 43, 89\}$. For getting modified open text

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

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

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

right to left, i.e. for each element of $S_j = \{s_1, s_2, \ldots, s_m\}, \quad j = 1,2,\ldots,m$. In case of the last element $s_8 = 118$, at first $x_1^{'} =$"" and after

$s_8 \geq k_5^{Z}\ (118 \geq 89) \quad x_1^{'} =$"1" $\quad s_8 = 118 - 89 = 29;$

$s_8 < k_4^{Z}\ (29 < 43) \quad x_1^{'} =$"01" $\quad s_8 = 29;$

$s_8 \geq k_3^{Z}\ (29 \geq 20) \quad x_1^{'} =$"101" $\quad s_8 = 29 - 20 = 9;$

$s_8 \geq k_2^{Z}\ (9 \geq 9) \quad x_1^{'} =$"1101" $\quad s_8 = 9 - 9 = 0;$

$s_8 < k_1^{Z}\ (0 < 4) \quad x_1^{'} =$"01101" $\quad s_8 = 0;$

calculations we have

$X^{'} =$"00001 01100 00111 01111 10010 01001 10100 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*".

Conclusion: We propose use Private Box Algorithm in Enterprise Business Application or in data security problems with an embedded private key generation device or as software. For apply it on Web based systems algorithm has to be realized via web technology languages for instance Java™.

References:

1. Bruce Schneier: *Applied Cryptography*, John Wiley & Sons, New York, 1994
2. Khamdamov R.Kh., Ergashev A.K.: *Решение задачи о рюкзаке методом обобщенных неравенств*, Сб. научных трудов ТашГТУ, 1993.
3. A. Salomaa: *Public-Key Cryptography*, Springer-Verlag, 1990
4. S. Barichev: Криптография без секретов.