**International Journal of Pure and Applied Mathematics**

**Volume 5 No. 2 2003, 135-140**

# A PUBLIC-KEY CRYPTOSYSTEM BASED ON DIOPHANTINE EQUATIONS

Mohammad Bagheri[1] §, Nader Dastranj[2], Gholamreza Jandaghi[1]

[1]Department of Mathematics
Imam Hossein University
P.O. Box 16895/198, Tehran, IRAN

[2]Payame-Noor University
Orumieh, IRAN

**Abstract:** The classical cryptography has been replaced by Public-Key cryptography since the past two decades. One of the most poular system proposed by Merkle and Helman named as the Knapsack-Public-Key-Encryption in 1978 [1]. This system of cryptography is based on the concept that if $C$ is a known number, how we can choose some numbers from a set so that they are summed up to $C$ in mode $M$. This system was broken by Shamir [2] six years after its genesis. In this paper, we present a new Public-Key cryptosystem. In this system, the equation $\sum_{i=1}^{n} a_i x_i = C$ is solved in mode $M$, in which $C$ and $a_i$ are known and $x_i \in \{0, 1, 2\}$. It can be simply seen that in general case we need to investigate $2^n$ combinations, while in our system, one needs to examine $3^n$ combinations which means that the security of the new system is higher than that of Merkle's.

**AMS Subject Classification:** 94A60
**Key Words:** Public-Key, cryptosystem, Diophantine equations

## 1. Introduction

The security of a message has been always based on encrypting and hiding it by transforming the message to a cipher text. Progress in sciences, especially

Received: December 22, 2002


§Correspondence author

in the area of computing, caused the classical cryptography not to be able to remain safe and have a risk of breakdown in a short amount of time. Since the begining of 80's, this question was arised, that whether we can find an algorithm in which the encryption operation can be done easily, so that each person can encrypt their message based on the algorithm but when enciphered, anybody even the sender can not decode it and only the person, who receives the code, is able to decode. In fact, the number of operations needed to decode a message must be so large that can not be reached in a short amount of time even with the aid of computers. Cryptography based on this idea has been named the Public-Key cryptosystems one of which is based on the Knapsack-Problem.

## 2. Cryptography Based on Knapsack-Problem

Before presenting our new cryptosystem, we go back to the Knapsack-Problem. Let $S$ be a known positive integer and $a_1, a_2, \cdots, a_n$ representing length of segments of a wire. How can we choose some of these segments such that their sum be $S$? It is obvious that the solution needs to investigate $2^n$ different combinations. When $n$ gets larger, this inspection needs a considerable amount of time even with the aid of computers. But if $a_1, a_2, \cdots, a_n$ be a superincreasing sequence, the inspection can be done easily and we do not need to consider $2^n$ combinations.

**Definition 1.** The sequence $a_1, a_2, \cdots, a_n$ is called superincreasing if for any $j = 2, 3, \cdots$ we have $\sum_{i=1}^{j-1} a_i < a_j$.

The solution of the Knapsack-Problem is to find a vector $X = (x_1, x_2, \cdots, x_n)$ such that the inner-product $a.X$ is equal to $S$ in which $x_i \in \{0, 1\}$. It is proved that we can find such $X$ based on the following algorithm.

If $a_n < S$, we set $x_n = 1$ otherwise $x_n = 0$. To find $x_{n-1}, x_{n-2}, \cdots, x_2, x_1$, we use the following formula:

$$x_j = \begin{cases} 1 & a_j \leq (S - \sum_{k=j+1}^{n} a_k x_k), \\ 0 & \text{otherwise.} \end{cases}$$

Now, we come back to the Helman-Merkle cryptosystem:

- Assign a number to each letter and transfer it into a base-2 number and form the message in $n$-tuple vectors.

- Each member of the communication network chooses a superincreasing sequence $(a_1, a_2, \cdots, a_n)$, as their specific key.
- Choose $M$ such that $\sum_{i=1}^{n} a_i < M$ and a $W$ such that $(W, M) = 1$ and find $W^{-1}$ (the multiplication inverse of $W$ in mode $M$) as the other part of the specific key.
- set $W(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n)$ as Public-Key.
- Let $P$ be the main message. Each letter in $P$, is replaced by its base-2 number equivalent and the message is formed in $n$-tuple vectors with 0 and 1 components ($n$ must be a multiple of $S$). Multiplying these vectors by the Public-Key encodes, the message comes into the integers $S_1, S_2, \cdots, S_k$. The one, who receives the message, multiplies each $S_i$ by $W^{-1}$ in mode $M$ to find $s_1, s_2, \cdots, s_k$ which satisfies $s_j = W^{-1}S_j$ in mode $M$. Now only the one, who has the specific key, can simply solve $k$ Knapsack problems to decode the message.

## 3. Cryptography Based on Diophantine Equations

It is obvious that the solution of the Diophantine equation:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = S\,,$$

in which $S$ and $a_i$'s are known, in general case needs examining $3^n$ combinations. But under some condition on $a_i$, it can be solved simply.

**Definition 2.** The finite sequence of natural numbers $a_1, a_2, \cdots, a_n$ is called second order superincreasing if for any $j = 2, 3, \cdots$ we have $2\sum_{i=1}^{j-1} a_i < a_j$.

Now, suppose the sequence $a_1, a_2, \cdots, a_n$ be a second order superincreasing sequence. To find the solution of the equation:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = S\,,$$

first we find $x_n$ based on the following formula:

$$x_n = \begin{cases} 2 & 2a_n \le S, \\ 1 & a_n \le S < 2a_n, \\ 0 & S < a_n. \end{cases}$$

Then $x_1, x_2, \cdots, x_{n-1}$ is obtained recursively from the following equation:

$$x_j = \begin{cases} 2 & S - \sum_{i=j+1}^{n} a_i x_i > 2a_j\,, \\ 1 & a_j \le S - \sum_{i=j+1}^{n} a_i x_i < 2a_j\,, \\ 0 & a_j < S - \sum_{i=j+1}^{n} a_i x_i\,. \end{cases}$$

### 3.1. The New Cryptosystem

Suppose $A$ is a member of the communication network. At first, $A$ chooses a second order superincreasing sequence like $a_1, a_2, \cdots, a_n$ and a natural number $M$ such that $M > 2\sum_{i=1}^{n} a_i$. Then he chooses $W$ such that $(W, M) = 1$ and computes $W^{-1}$(the multiplication inverse of $W$ in mode $M$) and calculates $b_i = Wa_i$ as the Public-Key. He keeps $W$, $W^{-1}$, $M$ and the superincreasing sequence as the specific key. Now to send a message to $A$, each person must transform the message into $n$-tuple vectors in base-3.

Let $(x_1, x_2, \cdots, x_n)$ be one of the vectors. Its cipher will be $C = \sum_{i=1}^{n} b_i x_i$. To decode the ciphered message, the person $A$ first computes $W^{-1}C = S$ and solve the equations $\sum i = 1^n a_i x_i = S$.

### 3.2. Example

Suppose we have a second order superincreasing sequence $(a_1, a_2, \cdots, a_n)$ $= (1, 3, 9, 27, 82, 245, 750, 2300)$ and choose $M = 7001$. Note that we must have $M > 2\sum_{i=1}^{n} a_i$. We set $W = 345$. So, $W^{-1} = 6169$ in mode $M$. Now we apply the equation $b_i = Wa_i$ in mode $M$ to have

$$b_1 = 345 \times 1 = 345\,,$$

$$b_2 = 345 \times 3 = 1035\,,$$

$$b_3 = 345 \times 9 = 3105\,,$$

$$b_4 = 345 \times 27 = 2314\,,$$

$$b_5 = 345 \times 82 = 286\,,$$

$$b_6 = 345 \times 245 = 513\,,$$

$$b_7 = 345 \times 750 = 6714\,.$$

$$b_8 = 345 \times 2300 = 2387\,.$$

So, $B = (b_1, b_2, \cdots, b_n) = (345, 1035, 3105, 2314, 286, 513, 6714, 2387)$ , $W$, $W^{-1}$ and $M$ are the specific key. To encode the word $HEALTH$, we assign numbers 0 to 25 to English alphabet to have the $H = 7$, $E = 4$, $A = 0$, $L = 11$, $T = 19$ and $H = 7$. Taking these numbers into base 3, we will have: $H = 7 = (0021)$, $E = 4 = (0011)$, $A = 0 = (0000)$, $L = 11 = (0102)$, $T = 19 = (0201)$ and $H = 7 = (0021)$. Then we form the word "HEALTH" in 8-tuple vectors:

$$X_1 = (0, 0, 2, 1, 0, 0, 1, 1)\,,$$

$$X_2 = (0, 0, 0, 0, 0, 1, 0, 2)\,,$$

$$X_3 = (0, 2, 0, 1, 0, 0, 2, 1)\,.$$

Now we send the message in the following form:

$$C = \begin{bmatrix} 0 & 0 & 2 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 2 & 0 & 1 & 0 & 0 & 2 & 1 \end{bmatrix} \begin{bmatrix} 345 \\ 1035 \\ 3105 \\ 2314 \\ 286 \\ 513 \\ 6714 \\ 2387 \end{bmatrix} = \begin{bmatrix} 17625 & 5287 & 20199 \end{bmatrix}.$$

To decode the message, from the equation $W^{-1}C = S$ we have:

$$S = \begin{bmatrix} 6169 \times 17625 \\ 6169 \times 5287 \\ 6169 \times 20199 \end{bmatrix} = \begin{bmatrix} 3095 \\ 4845 \\ 3833 \end{bmatrix},$$

in which "=" means "in mode $M = 7001$". Having $S = (S_1, S_2, S_3)$, we can find $X_1$, $X_2$ and $X_3$ as follows:

To find the components of $X_1$, since

$$3095 \geq a_8 = 2300 \;\text{ so }\; X_{18} = 1\,,$$

$$3095 - 2300 = 795 \geq a_7 = 750 \;\text{ so }\; X_{17} = 1\,,$$

$$795 - 750 = 45 < a_6 = 245 \;\text{ so }\; X_{16} = 0\,,$$

$$45 < a_5 = 82 \;\text{ so }\; X_{15} = 0\,,$$

$$45 > a_4 = 27 \;\text{ so }\; X_{14} = 1\,,$$

$$45 - 27 = 18 \geq 2a_3 = 18 \;\text{ so }\; X_{13} = 2\,,$$

$$18 - 18 = 0 < a_2 = 3 \ \text{ so } \ X_{12} = 0\,,$$
$$0 < a_1 = 1 \ \text{ so } \ X_{11} = 0\,,$$

which results in $X_1 = (0, 0, 2, 1, 0, 0, 1, 1)$.

To find the components of $X_2$, since

$$4845 \geq 2a_8 = 4600 \ \text{ so } \ X_{28} = 2\,,$$
$$4845 - 4600 = 245 < a_7 = 750 \ \text{ so } \ X_{27} = 0\,,$$
$$245 \geq a_6 = 245 \ \text{ so } \ X_{26} = 1\,,$$
$$245 - 245 = 0 < a_5 = 82 \ \text{ so } \ X_{25} = 0\,,$$
$$0 < a_4 = 27 \ \text{ so } \ X_{24} = 0\,,$$
$$0 < a_3 = 9 \ \text{ so } \ X_{23} = 0\,,$$
$$0 < a_2 = 3 \ \text{ so } \ X_{22} = 0\,,$$
$$0 < a_1 = 1 \ \text{ so } \ X_{21} = 0\,,$$

which results in $X_2 = (0, 0, 0, 0, 0, 1, 0, 2)$.

To find the components of $X_3$, since

$$3833 \geq a_8 = 2300 \ \text{ so } \ X_{38} = 1\,,$$
$$3833 - 2300 = 1533 \geq 2a_7 = 1500 \ \text{ so } \ X_{37} = 2\,,$$
$$1533 - 1500 = 33 < a_6 = 245 \ \text{ so } \ X_{36} = 0\,,$$
$$33 < a_5 = 82 \ \text{ so } \ X_{35} = 0\,,$$
$$33 \geq a_4 = 27 \ \text{ so } \ X_{34} = 1\,,$$
$$33 - 27 = 6 < a_3 = 9 \ \text{ so } \ X_{33} = 0\,,$$
$$6 \geq 2a_2 = 6 \ \text{ so } \ X_{32} = 2\,,$$
$$6 - 6 = 0 < a_1 = 1 \ \text{ so } \ X_{31} = 0\,,$$

which results in $X_3 = (0, 2, 0, 1, 0, 0, 2, 1)$.

## References

[1] R.C. Merkle, M.E. Helman, Hiding information and signatures in Trapdoor Knapsack, *IEEE Transactions on Information Theory*, **24** (1984), 525-530.

[2] A. Shamir, A polynomial-time algorithm for breaking the basic Merkle-Helman cryptosystem, *IEEE Transactions on Information Theory*, **30** (1984), 699-704.