

Opera suspicionată (OS)
Suspicious work**Opera autentică (OA)**
Authentic work

OS	Mang, I., Mang, E., Public-key cryptosystem based on the diophantine equations, <i>Journal of Computer Science and Control Systems</i> , Vol.1 Nr.1, p.58-61, 2008. Disponibil la: http :// electroinf . uoradea . ro / reviste %20 CSCS/documente / JCSCS 2008 / JCSCS 2008 11 Mangl 1 . pdf .
OA	Lin, C.H. Chang, C.C. Lee, R.C.T., „A New Public-Key Cipher System Based Upon the Diophantine Equations”, <i>IEEE Trans. on Computers</i> , vol. 44, no. 1, p. 13-19, Jan. 1995.

Incidența minimă a suspiciunii / Minimum incidence of suspicion

p.58: 9s – p.60:18d

p.13 - 12d - p.15:47s

Fișa întocmită pentru includerea suspiciunii în Indexul Operelor Plagiate în România de la
www.plagiate.ro

PUBLIC-KEY CRYPTOSYSTEM BASED ON THE DIOPHANTINE EQUATIONS

Ioan Mang, Erica Mang

Department of Computers,

University of Oradea, Faculty of Electrical Engineering and Information Technology,
1, Universitatii St., 410087 Oradea, Romania, E-mail: emang@keysys.ro

Abstract – This study analyses the mathematical aspects of diophantine equations and the potential of using them in cipher public-key systems. There are also presented the algorithms written in C language that were used for implementing such a system

Keywords: public-key algorithms, Diophantine equation, cryptosystem, encryption.

I. INTRODUCTION

In this paper, a new public-key cipher scheme is proposed. By the use of our scheme, the generating steps of keys are simple. Both the encryption and decryption procedures can be completed efficiently. Our cipher scheme is based upon the Diophantine equations.

In general, a Diophantine equation is defined as follows: We are given a polynomial equation $f(x_1, x_2, \dots, x_n) = 0$ with integer coefficients and we are asked to find rational or integral solutions [6].

Throughout this paper, we shall assume that the solutions are nonnegative. For instance, consider the following equation:

$$3x_1 + 4x_2 + 7x_3 + 5x_4 = 78. \quad (1)$$

The above equation is a Diophantine equation if we have to find a nonnegative solution for this equation. In fact, our solution is

$$(x_1, x_2, x_3, x_4) = (2, 5, 1, 9). \quad (2)$$

A famous Diophantine equation problem is Hilbert's tenth problem, which is defined as follows: Given a system of polynomials $P_i(x_1, x_2, \dots, x_n)$, $1 \leq i \leq m$, with integer coefficients, determine whether it has a nonnegative integer solution or not. In and, it was shown that the Hilbert problem is undecidable for polynomials with degree 4.

It was shown in that the Hilbert problem is undecidable for polynomials with 13 variables [1]. Gurari and Ibarra also proved that several Diophantine equations are in NP-complete class.

II. THE UNDERLYING MATHEMATICS

Let w be some positive integer and the domain D be a set of positive integers in the range of $[0, w]$. Let $w = 2^b - 1$, where b is some positive integer. Assume that a sending message M with length NB bits is broken up into n pieces of submessages, namely m_1, m_2, \dots, m_n . Each submessage is of length b bits. In other words, we can represent each submessage by a decimal number m_i and m_i in D .

Suppose that n pairs of integers $(q_1, k_1), (q_2, k_2), \dots$ and (q_n, k_n) are chosen such that the following conditions hold:

1) q_i 's are pairwise relative primes; i.e.

1. $(q_i, q_j) = 1$ for $i \neq j$.
2. $k_i > w$ for $i = 1, 2, \dots, n$.
3. $q_i > k_i w (q_i \bmod k_i)$, and $q_i \bmod k_i \neq 0$, for $i = 1, 2, \dots, n$.

These n integer pairs (q_i, k_i) 's will be kept secret and used to decrypt messages. For convenience, we name the above three conditions the DK-conditions since they will be used as deciphering keys. Note that for the generating of pairwise relatively primes, one can consult. Furthermore, the following numbers are computed.

First, compute $R_i = q_i \bmod k_i$ and compute P_i 's such that two conditions are satisfied:

- 1) $P_i \bmod q_i = R_i$, and
- 2) $P_j \bmod q_i = 0$ if $i \neq j$.

Since q_i 's are pairwise relatively primes, one solution for P_i 's satisfying the above two conditions is that $P_i = Q_i b_i$ with

$$Q_i = \prod_{j \neq i} q_j$$

and b_i is chosen such that $Q_i b_i \bmod q_i = R_i$. Since Q_i and q_i are relatively prime, b_i 's can be found by using the extended Euclid's algorithm. Note that the average number of divisions performed by the extended Euclid's algorithm for finding b_i is approximately 0.843. In $(q_i) + 1.47$. Secondly, compute

$$N_i = \overline{q_i / (k_i R_i)} \quad \text{for } i = 1, 2, \dots, n.$$

Finally, compute

$$s_i = P_i N_i \bmod Q \quad \text{where } Q = \prod_{i=1}^n q_i \quad (3)$$

That is, we have a vector $S = (s_1, s_2, \dots, s_n)$ with each component computed as above. After this, S can be used as the enciphering key for encrypting messages. By conducting a vector product between $M = (m_1, m_2, \dots, m_n)$ and $S = (s_1, s_2, \dots, s_n)$; i.e.,

$$C = E(S, M) = M * S = \sum_{i=1}^n m_i s_i \quad (4)$$

a message M is transformed to its ciphertext C , where $*$ denotes the vector product operation. Conversely, the i th component m_i in M can be revealed by the following operation:

$$m_i = D((q_i, k_i), C) = \overline{k_i C / q_i} \quad \text{for } i = 1, 2, \dots, n \quad (5)$$

Theorem 2.1 shows that (5) is the inverse function of (4). The following lemmas are helpful in the proof of the theorem.

Lemma 2.1:

Let a and b be some positive integers where $b > a$. Then for all x , $a \overline{x/b} < x$ if $x \geq ab/(b-a)$.

Proof: Let $\overline{x/b} = c$ for some integer c .

Then $x/b \leq c < (x/b + 1)$. We have

$$ac < ax/(b+a) \quad (6)$$

On the other hand, if $x \geq ab/(b-a)$, then $(b-a)x \geq ab$; that is,

$$(ax/b + a) \leq x. \quad (7)$$

Combining (6) and (7), we have that

$$a \overline{x/b} < x \quad \text{if } x \geq ab/(b-a). \quad (8)$$

Lemma 2.2:

Let $R_i \equiv q_i \bmod k_i$. Then

$$k_i R_i m_i \overline{q_i / (k_i R_i)} \bmod k_i q_i \equiv k_i R_i m_i \overline{q_i / (k_i R_i)} \quad (9)$$

Proof: Let $a \equiv R_i m_i$, $b \equiv k_i R_i$, and $x \equiv q_i$. Since $q_i > k_i R_i$, we know that $q_i > k_i R_i 2 m_i / (R_i (k_i - m_i))$.

That is, $x \geq ab/(b-a)$ is satisfied. By applying Lemma 2.1, it can be seen that $R_i m_i \overline{q_i / (k_i R_i)} < q_i$. Therefore,

$$k_i R_i m_i \overline{q_i / (k_i R_i)} \bmod k_i q_i \equiv k_i R_i m_i \overline{q_i / (k_i R_i)} \quad (10)$$

Lemma 2.3:

Let m_i 's, k_i 's and q_i 's be chosen such that the DK-conditions are satisfied. Let $R_i \equiv q_i \bmod k_i$. Then

$$\overline{k_i R_i m_i \overline{q_i / (k_i R_i)}} \bmod q_i = m_i. \quad (11)$$

Proof:

Let $\delta = \overline{k_i R_i m_i \overline{q_i / (k_i R_i)}} \bmod q_i = m_i$. It can be easily seen that the following two inequalities hold:

$$\delta < \overline{k_i R_i m_i (q_i / (k_i R_i) + 1)} / q_i = m_i \quad (12)$$

and

$$\delta \geq \overline{k_i R_i m_i (q_i / (k_i R_i))} / q_i = m_i. \quad (13)$$

Furthermore, the right-hand side of (13) is identical to m_i and that of (12) is $\overline{m_i + k_i R_i m_i / q_i}$. On the other hand, since m_i is an integer and $k_i R_i m_i / q_i < 1$, the right-hand side in (12) becomes

$$\overline{m_i + k_i R_i m_i / q_i} = m_i. \quad (14)$$

Combining these two inequalities, we obtain that $m_i \leq \delta \leq m_i$. Finally, we have $\delta = m_i$, since δ is an integer.

Theorem 2.1: Let $(q_1, k_1), (q_2, k_2), \dots$, and (q_n, k_n) be n pairs of positive integers satisfying the DK-conditions. Let the vector S be computed by applying (1). Then (3) is the inverse function of (2). That is, a message enciphered by (2) can be decrypted by (3).

Proof: Let us prove the theorem by the following two steps. First, from (1), define $s_i = P_i N_i$ we have a vector

$$s = (s_1, s_2, \dots, s_n); \text{ i.e., } s_i = s_i \bmod Q, \text{ for } i = 1, 2, \dots, n.$$

Let

$$C' = M * S = \sum_{i=1}^m m_i s_i = \sum_{i=1}^m m_i P_i N_i. \quad (15)$$

Since P_i 's satisfy the following two conditions:

- 1) $P_i \bmod q_i = q_i \bmod k_i = R_i$; and
- 2) $P_j \bmod q_i = 0$ if $i \neq j$,

$$k_i C' \bmod k_i q_i = (k_i \sum_{i=1}^n m_i P_i N_i) \bmod k_i q_i = k_i m_i R_i \overline{q_i / (k_i R_i)} \bmod k_i q_i. \quad (16)$$

Furthermore, by Lemma 2.2,

$$k_i m_i R_i \overline{q_i / (k_i R_i)} \bmod k_i q_i = k_i m_i R_i \overline{q_i / (k_i R_i)} \quad (17)$$

That is, $k_i C' \bmod k_i q_i = k_i m_i R_i \overline{q_i / (k_i R_i)}$ for $i=1, 2, \dots, n$. In other words,

$$k_i C' = y_i k_i q_i + k_i m_i R_i \overline{q_i / (k_i R_i)}. \quad (18)$$

for some integers y_i .
Moreover,

$$k_i C' / q_i = y_i k_i + k_i m_i R_i \left[q_i / (k_i R_i) \right]^{-1} / q_i. \quad (19)$$

Hence

$$\begin{aligned} \left[k_i C' / q_i \right]^{-1} &= \left[y_i k_i + k_i m_i R_i \left[q_i / (k_i R_i) \right]^{-1} / q_i \right]^{-1} \\ &= y_i k_i + \left[k_i m_i R_i \left[q_i / (k_i R_i) \right]^{-1} / q_i \right]^{-1} \end{aligned} \quad (20)$$

By applying Lemma 2.3, we have

$$\left[k_i C' / q_i \right]^{-1} = y_i k_i + m_i. \quad (21)$$

Thus

$$m_i = \left[k_i C' / q_i \right]^{-1} \pmod{k_i}. \quad (22)$$

Second, let

$$Q = \prod_{i=1}^n q_i. \quad (23)$$

then

$$\begin{aligned} C' \pmod{Q} &= \left(\sum_{i=1}^n m_i s_i \right) \pmod{Q} = ((m_1 s_1 \pmod{Q}) + \dots \\ &+ (m_n s_n \pmod{Q})) \pmod{Q} = (m_1 (s_1 \pmod{Q}) + \dots \\ &+ m_n (s_n \pmod{Q})) \pmod{Q} = \left(\sum_{i=1}^n m_i s_i \right) \pmod{Q} = C \pmod{Q}. \end{aligned}$$

That is, $C' = C \pmod{Q}$.

Let $C' = C + zQ$, for some positive integer z .

We have

$$\begin{aligned} \left[k_i C' / q_i \right]^{-1} \pmod{k_i} &= \left[k_i (C' - zQ) / q_i \right]^{-1} \pmod{k_i} \\ &= \left(\left[k_i C' / q_i \right]^{-1} - k_i z Q_i \right) \pmod{k_i} = \left[k_i C' / q_i \right]^{-1} \pmod{k_i} \end{aligned} \quad (24)$$

In other words, $m_i = \left[k_i C' / q_i \right]^{-1} \pmod{k_i}$.

III. THE CONSTRUCTION OF THE CRYPTOSYSTEM

In this section, the algorithms for constructing the cryptosystem, encrypting messages, respectively, are presented.

First, each user picks n pairs of parameters $(q_1, k_1), (q_2, k_2), \dots,$ and (q_n, k_n) such that the DK-conditions are satisfied. Afterward,

$$Q = \prod_{j \neq i} q_j \quad (25)$$

and

$$N_i = \left[q_i / (k_i (q_i \pmod{k_i})) \right]^{-1} \quad (26)$$

are computed, and b_i 's are integers chosen such that $Q_i b_i \pmod{q_i} \equiv q_i \pmod{k_i}$, for $i = 1, 2, \dots, n$.

Let $P_i \equiv Q_i b_i$ and $s_i \equiv P_i N_i \pmod{Q}$, for $i = 1, 2, \dots, n$, where

$$Q = \prod_{i=1}^n q_i \quad (27)$$

Therefore, a vector

$$S = (s_1, s_2, \dots, s_n)$$

is obtained. There the n -tuple S of integers is published and used as the public key of the cryptosystem for enciphering messages.

The chosen parameters $(q_1, k_1), (q_2, k_2), \dots, (q_n, k_n)$ are kept and used as the private key to decipher messages received. Specifically, let user A be the sender and user B be the receiver, and let A be sending a message represented by

$$M = (m_1, m_2, \dots, m_n),$$

where m_i is a b -bits submessage represented by a decimal number in the range of $[0, 2^b - 1]$.

Then (m_1, m_2, \dots, m_n) is enciphered by (4) into an integer C . Afterward, the integer C is sent to user B as the ciphertext of the original message M . On the receiving of integer C user B is able to convert C into (m_1, m_2, \dots, m_n) by applying (5).

IV. CONCLUSION AND DISCUSSION

A new public-key cryptosystem is investigated in this paper. The motivation of this attempt is trying to use real numbers for its dense property. However, if real numbers are used as keys, several disturbing problems, such as representation and precision will be encountered. With the help of integer functions, the possibility of using an integer as a key is increased significantly. That is, for a cryptanalyst who tries to break the cipher, he has to conduct an exhaustive search on a long list of integer numbers.

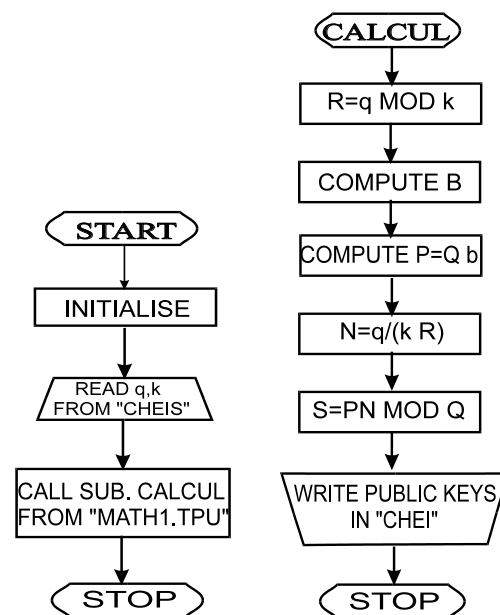


Fig. 1. Key Generating for Each User