Astérisque

MORISLAV LASSAK

Some remarks on the Pethő public key cryptosystem

Astérisque, tome 209 (1992), p. 257-264

<http://www.numdam.org/item?id=AST_1992__209__257_0>

Some remarks on the Pethő public key cryptosystem

Miroslav Laššák, Bratislava

In [1] Pethő introduced a public key cryptosystem. In its definition (see below for more details) an essential role is played by a monic polynomial $g(t)$ of degree n and a modulus M, which belong to the nonpublic part of this cryptosystem. The aim of this note is to show that if the greatest common divisor of the nth power of the constant term of g and M is too "small", then the cryptosystem can be broken in polynomial time. The crucial role in our cryptoanalysis is played by a system of congruences (9) whose solution can be found under the above mentioned condition.

1 Pethő public key cryptosystem

For the convenience of the reader, we describe in this section the main ingredients of the public key cryptosystem suggested by A. Pethő in [1].

Let $g(t) = t^n + g_{n-1}t^{n-1} + \cdots + g_1 t + g_0 \in \mathcal{Z}[t]$, where $\mathcal{Z}$ denotes the ring of integers and $\mathbf{G}$ the companion matrix of the polynomial $g(t)$. Further, let $\mathbf{x}_i \in \mathcal{Z}^n$ for $i \geq 0$ be the sequence of vectors defined by

$$\begin{aligned} \mathbf{x}_0 &= (1, 0, \ldots, 0) \\ \mathbf{x}_{i+1} &= \mathbf{x}_i \mathbf{G} \quad \text{for} \quad i \geq 0. \end{aligned} \tag{1}$$

Given a finite subset $\mathcal{N}$ of $\mathcal{Z}$, $\mathcal{A}_{\mathcal{N}}$ will denote the set of all finite words over $\mathcal{N}$ satisfying the property that if $0 \in \mathcal{N}$ and $l > 0$ then $w_l \neq 0$. If $l(w) = l + 1$ denotes the length of the word $w = w_0 w_1 \ldots w_l$, then $\mathcal{A}_{\mathcal{N}}^L$ will denote the set of all words of $\mathcal{A}_{\mathcal{N}}$ of length not exceeding $L + 1$.

DEFINITION 1.1 *A pair* $\{g(t), \mathcal{N}\}$ *is called a* weak number system *if the map* $T : \mathcal{A}_{\mathcal{N}} \to \mathcal{Z}^n$ *defined by*

$$T(w_0 \ldots w_l) = w_0 \mathbf{x}_0 + \cdots + w_l \mathbf{x}_l \tag{2}$$

is injective.

One sufficient condition for weak number systems is contained in the next result [1]:

PROPOSITION 1.1 *If* $|g_0| \geq 2$ *and* $\mathcal{N}$ *consists of pairwise incongruent integers modulo* g_0, *then the pair* $\{g(t), \mathcal{N}\}$ *is a weak number system.*

This weak number system enables us to construct a private key cryptosystem. To do this take $g(t) = t^n + g_{n-1}t^{n-1} + \cdots + g_1 t + g_0 \in \mathcal{Z}[t]$ with $|g_0| \geq 2$ and a set $\mathcal{N}$ of pairwise incongruent integers modulo g_0.

For encryption of a plaintext $w = w_0 \dots w_r \in \mathcal{A}_{\mathcal{N}}$ choose integers $l_1, l_2, \dots, l_h$ with $l_1 + l_2 + \cdots + l_h = r + 1$. Then cut the word w into subwords $W_1, \dots, W_h$ of $\mathcal{A}_{\mathcal{N}}$ in such a way that $w = W_1 \dots W_h$ and $l(W_i) = l_i$. Then application of the map T gives the cryptogram $Y_1, \dots, Y_h \in \mathcal{Z}^n$, where $Y_i = T(W_i)$ for $i = 1, \dots, h$. The knowledge of the corresponding secret keys $g(t)$ and $\mathcal{N}$ may be used to decrypt the received message. For more details about the corresponding algorithm consult [1].

Unfortunately, this cryptosystem cannot be used as the public key cryptosystem, therefore Pethő suggested the following modification:

Let $\{g(t), \mathcal{N}\}$ be a weak number system constructed by proposition 1.1 such that $0 \in \mathcal{N}$.

Let the height $m(w)$ of the word $w \in \mathcal{A}_{\mathcal{N}}$ be defined by

$$m(w) = \max\{|y_0|, \dots, |y_{n-1}|\},$$

where $T(w) = (y_0, \dots, y_{n-1}) \in \mathcal{Z}^n$. Then take an integer M such that

$$M > 2 \max\{m(w) : w \in \mathcal{A}_{\mathcal{N}}^{n+L}\} \tag{3}$$

and a regular matrix $\mathbf{C}$ over $\mathcal{Z}_M$ satisfying

$$\mathbf{CG} \neq \mathbf{GC} \quad \text{over } \mathcal{Z}_M. \tag{4}$$

Finally, define the vectors $\widehat{\mathbf{x}}_i$ for $i = 0, 1, \dots, L$ by

$$\widehat{\mathbf{x}}_i \equiv \mathbf{x}_{n+i}\mathbf{C} \pmod{M} \tag{5}$$

and the map $\widehat{T} : \mathcal{A}_{\mathcal{N}}^L \to \mathcal{Z}^n$ by

$$\widehat{T}(w_0 \dots w_l) = w_0 \widehat{\mathbf{x}}_0 + \cdots + w_l \widehat{\mathbf{x}}_l \quad \text{for} \quad l \leq L. \tag{6}$$

The public part of the Pethő public key cryptosystem consists of the chosen weak number system, $\mathcal{N}$ and vectors $\widehat{\mathbf{x}}_0, \widehat{\mathbf{x}}_1, \dots, \widehat{\mathbf{x}}_L$. To encrypt a plaintext $w = w_0 \dots w_i$ an analogous algorithm can be used, but based on $\widehat{T}(w_0 \dots w_i)$ instead on $T(w_0 \dots w_i)$.

Knowing the secret keys $\mathbf{C}, M$ one can determine the matrix $\mathbf{C}^{-1}$ over $\mathcal{Z}_M$. We have

$$\widehat{T}(w_0 \ldots w_l) = w_0\widehat{\mathbf{x}}_0 + \cdots + w_l\widehat{\mathbf{x}}_l \equiv (w_0\mathbf{x}_n + \cdots + w_l\mathbf{x}_{n+l})\mathbf{C} \pmod M$$

and consequently

$$(y_0, \ldots, y_{n-1}) = T(\underbrace{0 \ldots 0}_{n} w_0 \ldots w_l) \equiv \widehat{T}(w_0 \ldots w_l)\mathbf{C}^{-1} \pmod M. \tag{7}$$

Furthermore, using (3) we obtain

$$2|y_i| \le 2m(\underbrace{0 \ldots 0}_{n} w_0 \ldots w_l) < M,$$

which implies

$$|y_i| < M/2 \ \text{ for } \ i = 0, 1, \ldots, n-1 \tag{8}$$

and $y_0, \ldots, y_{n-1}$ are uniquely determined. Using the algorithm for decryption (see [1]) we get $0 \ldots 0 w_0 \ldots w_l$ and then $w_0 \ldots w_l$.

This cryptosystem is correct in the sense that the plaintext may be uniquely determined from the encrypted text.

2 A possibility of decryption

We write $\mathbf{A} \equiv \mathbf{B} \pmod m$ or $\mathbf{A} \overset{(m)}{\equiv} \mathbf{B}$ for the matrices $\mathbf{A}, \mathbf{B}$ congruent modulo m.

DEFINITION 2.1 *The square matrices* $\mathbf{A}, \mathbf{B}$ *of order* n *are called* similar modulo m *if there exist two square matrices* $\mathbf{P}, \mathbf{Q}$ *of order* n *such that* $\mathbf{PQ} \overset{(m)}{\equiv} \mathbf{QP} \overset{(m)}{\equiv} \mathbf{I}$ *and* $\mathbf{B} \equiv \mathbf{PAQ} \pmod m$. *We write* $\mathbf{A} \sim \mathbf{B} \pmod m$.

PROPOSITION 2.1 *Let* $\mathbf{A}, \mathbf{B}$ *be square matrices of order* n *and* $\operatorname{char}(\mathbf{A}) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0, \operatorname{char}(\mathbf{B}) = t^n + b_{n-1}t^{n-1} + \cdots + b_1 t + b_0$ *be their characteristic polynomials. If* $\mathbf{A} \sim \mathbf{B} \pmod m$, *then*

$$a_i \equiv b_i \pmod m \ \ \textit{for } i = 0, 1, \ldots, n-1.$$

Now we return to the Pethő public key cryptosystem. Consider the following system of congruences

$$\widehat{\mathbf{x}}_i \equiv \widehat{\mathbf{x}}_{i-1}\mathbf{A} \pmod M \ \text{ for } \ i = 1, 2, \ldots, L, \tag{9}$$

where $\mathbf{A}$ is a (unknown) matrix of order n and M, $\widehat{\mathbf{x}}_0, \widehat{\mathbf{x}}_1, \ldots, \widehat{\mathbf{x}}_L$ are public keys.

It is not hard to see that the matrix $\mathbf{C}^{-1}\mathbf{G}\mathbf{C}$ is a solution of the system of congruences (9) for

$$\begin{aligned}\widehat{\mathbf{x}}_i &\overset{(M)}{\equiv} \mathbf{x}_{n+i}\mathbf{C} = \mathbf{x}_{n+i-1}\mathbf{G}\mathbf{C}\\ &\overset{(M)}{\equiv} \mathbf{x}_{n+i-1}\mathbf{C}\mathbf{C}^{-1}\mathbf{G}\mathbf{C} \overset{(M)}{\equiv} \widehat{\mathbf{x}}_{i-1}(\mathbf{C}^{-1}\mathbf{G}\mathbf{C}) \quad \text{for } i = 1, 2, \ldots, L.\end{aligned}$$

In the rest of the paper we shall find conditions under which it is possible to find M and a solution matrix $\mathbf{A}_0$ of the system (9). The following observations show that this is sufficient to break the Pethő cryptosystem in polynomial time. To see this note:

1. If $\mathbf{A}_0 \equiv \mathbf{C}^{-1}\mathbf{G}\mathbf{C} \pmod{M}$, then by definition 2.1 the matrices $\mathbf{A}_0$ and $\mathbf{G}$ are similar modulo M. Therefore, if $\operatorname{char}(\mathbf{A}_0) = t^n + g'_{n-1}t^{n-1} + \cdots + g'_1 t + g'_0$ is the characteristic polynomial of the matrix $\mathbf{A}_0$, then by proposition 2.1 we have

$$g'_i \equiv g_i \pmod{M}. \tag{10}$$

Furthermore, we have

$$M > 2|g_i| \cdot |w'| \geq 2|g_i|, \tag{11}$$

where w' is a nonzero element of $\mathcal{N}$, since $\mathbf{x}_n = (-g_0, \ldots, -g_{n-1})$. Consequently, $|g_i| < M/2$ for $i = 0, 1, \ldots, n-1$ and this together with (10) implies that the coefficients $g_0, g_1, \ldots, g_{n-1}$ of the polynomial $g(t)$ are uniquely determined. Thus we can derive the polynomial $g(t)$, the matrix $\mathbf{G}$ and the vectors $\mathbf{x}_i$ $(i = 0, 1, \ldots, n+L)$ from knowledge of M and $\mathbf{A}_0$.

2. Let $\mathbf{R}_0$ be an arbitrary solution of the system of congruences

$$\widehat{\mathbf{x}}_i\mathbf{R} \equiv \mathbf{x}_{n+i} \pmod{M} \quad \text{for } i = 0, 1, \ldots, L \tag{12}$$

with an unknown matrix $\mathbf{R}$. This system is solvable, because $\mathbf{C}^{-1}$ solves it. But it is not necessary to find just the matrix $\mathbf{C}^{-1}$, because any solution matrix $\mathbf{R}_0$ can be used for determining $y_0, \ldots, y_{n-1}$ since

$$\begin{aligned}\widehat{T}(w_0 \ldots w_l)\mathbf{R}_0 &= (w_0\widehat{\mathbf{x}}_0 + \cdots + w_l\widehat{\mathbf{x}}_l)\mathbf{R}_0\\ &\overset{(M)}{\equiv} w_0\mathbf{x}_n + \cdots + w_l\mathbf{x}_{n+l}\\ &= T(0\ldots 0w_0 \ldots w_l) = (y_0, \ldots, y_{n-1})\end{aligned}$$

Due to (8) the numbers $y_0, \ldots, y_{n-1}$ are uniquely determined. Now we know all that is necessary for decryption. Applying the decryption algorithm to $(y_0, \ldots, y_{n-1}) = T(0\ldots 0w_0 \ldots w_l)$ we get $0\ldots 0w_0 \ldots w_l$ and consequently $w_0 \ldots w_l$.

Thus knowing M and the matrix $\mathbf{A}_0$ we are able to decrypt intercepted messages in polynomial time.

3 How to solve system (9)

Put

$$\mathbf{X} = \begin{pmatrix} \widehat{\mathbf{x}}_0 \\ \vdots \\ \widehat{\mathbf{x}}_{L-1} \end{pmatrix}, \quad \mathbf{Y} = \begin{pmatrix} \widehat{\mathbf{x}}_1 \\ \vdots \\ \widehat{\mathbf{x}}_L \end{pmatrix}$$

and rewrite the system of congruences (9) into the matrix form

$$\mathbf{XA} \equiv \mathbf{Y} \pmod{M}. \tag{13}$$

We can suppose $L \geq n$. In the opposite case (i. e. if $L < n$) this system would reduce to a system of equations, which is easy to solve and we immediately obtain the plaintext.

Reduce the matrix $\mathbf{X}$ of order $L \times n$ over $\mathcal{Z}$ to Smith canonical form. Then we obtain invertible matrices $\mathbf{P}, \mathbf{Q}$ over $\mathcal{Z}$ such that

$$\mathbf{PXQ} = \mathbf{D},$$

where $\mathbf{D} = \mathrm{diag}_{L,n}(a_0, \dots, a_{n-1})$ is the matrix of order $L \times n$ with $a_0, \dots, a_{n-1}$ on the main diagonal and $a_i | a_j$ for $i < j$. We may suppose that $a_i \geq 0$ for $i = 0, 1, \dots, n-1$ (in the opposite case multiply the row by -1).

The system (13) can be equivalently rewritten into the form

$$\mathbf{DB} = \mathbf{PXQB} \equiv \mathbf{PY} \pmod{M}, \tag{14}$$

with an unknown matrix $\mathbf{B}$ such that $\mathbf{A} = \mathbf{QB}$.

Note that we do not need to know M in order to be able to reduce the matrix $\mathbf{X}$ to Smith canonical form.

If $\mathbf{B} = \|y_{ij}\|$ and $\mathbf{PY} = \|b_{ij}\|$, then the system (14) can be replaced by two systems

$$\begin{aligned} a_0 y_{0,j} &\equiv b_{0,j} \pmod{M} \\ &\vdots \\ a_{n-1} y_{n-1,j} &\equiv b_{n-1,j} \pmod{M} \quad \text{for} \quad j = 0, \dots, n-1 \end{aligned} \tag{15}$$

and

$$\begin{aligned} 0 &\equiv b_{n,j} \pmod{M} \\ &\vdots \\ 0 &\equiv b_{L-1,j} \pmod{M} \quad \text{for} \quad j = 0, \dots, n-1. \end{aligned} \tag{16}$$

System (16) is solvable, because e. g. the matrix $\mathbf{Q}^{-1}\mathbf{C}^{-1}\mathbf{GC}$ is its solution. Thus the following condition must be true:

$$M | b_{k,j} \quad \text{for} \quad k = n, \dots, L-1; j = 0, \dots, n-1.$$

If we write d for the greatest common divisor of $b_{k,j}$ for all $k = n, \ldots, L-1$; $j = 0, \ldots, n-1$, then $M|d$.

Similarly, system (15) has also a solution, therefore

$$(a_i, M) = (a_i, M, b_{i,j}) \quad \text{for} \quad i = 0, \ldots, n-1; j = 0, \ldots, n-1$$

and this gives a further restriction on M of the type $M|d'$, where $d' \leq d$.

Now we may gradually substitute for M divisors of d'. However, this is possible only provided $d \neq 0$, otherwise the congruences (5) become equalities, i. e. $\widehat{\mathbf{x}}_i = \mathbf{x}_{n+i}\mathbf{C}$ for $i = 0, \ldots, L$.

Now we suppose that we know M. Put $d_i = (a_i, M)$, $m_i = M/d_i$ for $i = 0, 1, \ldots, n-1$. Since $a_i|a_j$ for $i < j$, we have $d_i|d_j$ and $m_j|m_i$ for $i < j$.

The congruence $a_i y_{ij} \equiv b_{ij} \pmod{m_i}$ has exactly d_i solutions incongruent modulo M for all $i, j \in \{0, \ldots, n-1\}$. Therefore there are $d_0^n d_1^n \cdots d_{n-1}^n$ solutions incongruent modulo M of the system (14) and also the same number of the system (13).

4 Conclusions

Now we prove the following theorem.

THEOREM 4.1 *Let* $\mathbf{X}$ *be the matrix of order* $L \times n$ *defined in section 3 and* $L \geq n$. *Let the matrix* $\mathbf{D} = \mathrm{diag}_{L,n}(a_0, \ldots, a_{n-1})$ *be its Smith canonical form with* $a_i|a_j$ *for* $i < j$ *and* $a_i \geq 0$ *for* $i = 0, 1, \ldots, n-1$. *Then*

(a) $\quad (a_0, M) = d_0 = (M, g_0, \ldots, g_{n-1})$

(b) $\quad (a_0 \cdots a_{n-1}, M) = (M, g_0^n)$.

Proof: The following property of the Smith canonical form will be used.

Let $\Delta_k(\mathbf{A})$ be the greatest common divisor of all minors of k-th order of a matrix $\mathbf{A}$. Given a matrix $\mathbf{A}$ of order $l \times m$, write $\mathbf{D} = \mathrm{diag}_{l,m}(a_0, \ldots, a_{n-1})$ for its Smith canonical form. Then (see [2] chapter 16)

$$\begin{aligned} a_0 &= \Delta_1(\mathbf{A}) \\ a_0 a_1 &= \Delta_2(\mathbf{A}) \\ &\vdots \\ a_0 a_1 \cdots a_{n-1} &= \Delta_n(\mathbf{A}). \end{aligned} \tag{17}$$

(a) Put $s = (M, g_0, \ldots, g_{n-1})$. We show by induction on i that there is a vector $\mathbf{x}'_{n+i}$ such that $\mathbf{x}_{n+i} = s\mathbf{x}'_{n+i}$ for all $i = 0, 1, \ldots, L$. The case $i = 0$ is trivial, because $\mathbf{x}_n = (-g_0, \ldots, -g_{n-1})$. Suppose therefore that our assertion is true for $i-1$. The induction hypothesis implies $\mathbf{x}_{n+i} = \mathbf{x}_{n+i-1}\mathbf{G} = s\mathbf{x}'_{n+i-1}\mathbf{G} =$

$s\mathbf{x}'_{n+i}$. Furthermore, we have $\widehat{\mathbf{x}}_i \overset{(M)}{\equiv} \mathbf{x}_{n+i}\mathbf{C} = s\mathbf{x}'_{n+i}\mathbf{C}$. Since $s|M$, there exists a vector $\widehat{\mathbf{x}}'_i$ over $\mathcal{Z}$ such that $\widehat{\mathbf{x}}_i = s\mathbf{x}'_i$ for all $i = 0, 1, \dots, L$. Consequently $s|d_0$. There exists a vector $\widehat{\mathbf{x}}''_0$ over $\mathcal{Z}$ with $\mathbf{x}_n\mathbf{C} \overset{(M)}{\equiv} \widehat{\mathbf{x}}_0 = d_0\widehat{\mathbf{x}}''_0$. The matrix $\mathbf{C}$ is regular over $\mathcal{Z}_M$, $d_0|M$, thus necessarily there exists a vector $\mathbf{x}''_n$ such that $\mathbf{x}_n = d_0\mathbf{x}''_n$, i. e. $d_0|s$ as claimed.

(b) We have

$$\left|\begin{pmatrix} \widehat{\mathbf{x}}_0 \\ \vdots \\ \widehat{\mathbf{x}}_{n-1} \end{pmatrix}\right| \overset{(M)}{\equiv} \left|\begin{pmatrix} \mathbf{x}_n \\ \vdots \\ \mathbf{x}_{2n-1} \end{pmatrix}\mathbf{C}\right| =$$
$$= |\mathbf{I}\mathbf{G}^n\mathbf{C}| = |\mathbf{G}|^n|\mathbf{C}| = (-1)^n g_0^n|\mathbf{C}|.$$

Determine now the value of another minor of n-th order of the matrix $\mathbf{X}$. Let $0 \le i_0 < \cdots < i_{n-1} < L$, then

$$\left|\begin{pmatrix} \widehat{\mathbf{x}}_{i_0} \\ \vdots \\ \widehat{\mathbf{x}}_{i_{n-1}} \end{pmatrix}\right| \overset{(M)}{\equiv} \left|\begin{pmatrix} \mathbf{x}_{n+i_0} \\ \vdots \\ \mathbf{x}_{n+i_{n-1}} \end{pmatrix}\mathbf{C}\right| =$$
$$= \left|\begin{pmatrix} \mathbf{x}_{i_0} \\ \vdots \\ \mathbf{x}_{i_{n-1}} \end{pmatrix}\mathbf{G}^n\mathbf{C}\right| = \left|\begin{pmatrix} \mathbf{x}_{i_0} \\ \vdots \\ \mathbf{x}_{i_{n-1}} \end{pmatrix}\right|(-1)^n g_0^n|\mathbf{C}|.$$

This implies

$$a_0a_1\cdots a_{n-1} = \Delta_n(\mathbf{X}) = g_0^n|\mathbf{C}|,$$

and since the matrix $\mathbf{C}$ is regular over $\mathcal{Z}_M$ we have $(|\mathbf{C}|, M) = 1$ and in turn

$$(a_0a_1\cdots a_{n-1}, M) = (\Delta_n(\mathbf{X}), M) = (M, g_0^n)$$

and the proof is finished.

In section 3 we obtained $d_0^n d_1^n \cdots d_{n-1}^n$ solutions incongruent modulo M of the system (13). But we need one such $\mathbf{A}_0$ for which $\mathbf{A}_0 \equiv \mathbf{C}^{-1}\mathbf{G}\mathbf{C}$ (mod M). Thus we arrive at the problem to determine which one among the solutions of (13) satisfies this additional condition.

If $d_{n-1} = 1$, then the system (13) has only one solution and we are able to decrypt. Thus $d_{n-1} = 1$ is a sufficient condition for the determination of the matrix $\mathbf{A}_0$. But there is also a weaker condition for this conclusion.

All the solutions of the system (13) are congruent modulo m_{n-1}. Let $\mathbf{Z}$ be one of them, then $\mathbf{Z} \equiv \mathbf{C}^{-1}\mathbf{G}\mathbf{C} \pmod{m_{n-1}}$. Since $m_{n-1}|M$ and $\mathbf{C}\mathbf{C}^{-1} \overset{(M)}{\equiv} \mathbf{C}^{-1}\mathbf{C} \overset{(M)}{\equiv} \mathbf{I}$, we have $\mathbf{C}\mathbf{C}^{-1} \overset{(m_{n-1})}{\equiv} \mathbf{C}^{-1}\mathbf{C} \overset{(m_{n-1})}{\equiv} \mathbf{I}$. According to definition 2.1

we obtain $\mathbf{Z} \sim \mathbf{C}^{-1}\mathbf{G}\mathbf{C} \pmod{m_{n-1}}$. If $\mathrm{char}(\mathbf{Z}) = t^n + g'_{n-1}t^{n-1} + \cdots + g'_1 t + g'_0$ is the characteristic polynomial of the matrix $\mathbf{Z}$, then $g_i \equiv g'_i \pmod{m_{n-1}}$ for $i = 0, 1, \ldots n-1$ as proposition 2.1 shows. Put $k = \max\{|w| : w \in \mathcal{N}\}$, then we have $M > 2k|g_i|$ for $i = 0, \ldots, n-1$ by (11), whence

$$|g_i| < \frac{M/k}{2} \quad \text{for} \quad i = 0, 1, \ldots, n-1.$$

Thus if

$$m_{n-1} \geq M/k, \quad \text{resp.} \quad d_{n-1} \leq k, \tag{18}$$

then the coefficients of $g(t)$ are uniquely determined, since

$$|g_i| < \frac{M/k}{2} \leq \frac{m_{n-1}}{2} \quad \text{for} \quad i = 0, \ldots, n-1.$$

And now we can decrypt by the same way as in section 2.

According to assertion (b) of theorem 4.1 we have

$$d_{n-1} \leq (a_0 \cdots a_{n-1}, M) = (g_0^n, M).$$

Thus the Pethő public key cryptosystem cannot be used securely if $(g_0^n, M) \leq k$ and therefore it is necessary to choose M in such a way that (g_0^n, M) is sufficiently large.

References

[1] A. Pethő, *On a polynomial transformation to the construction of a public key cryptosystem*, Proceedings of the Colloquium on Computational Number Theory held at Kossuth Lajos University, Debrecen (Hungary), September 4-9, 1989.

[2] K. A. Rodosskij, *Euclid algorithm*, Moscow, Nauka, 1988 (in Russian).

Miroslav Laššák
Department of Algebra
and Number Theory
Faculty of Mathematics and Physics
Comenius University
Mlynská dolina
842 15 Bratislava
Czechoslovakia