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>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

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

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

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

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

and consequently

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

Furthermore, using (3) we obtain

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

which implies

$$|y_i| < M/2 \quad \text{for} \quad i = 0, 1, \dots, n-1 \quad (8)$$

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

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 $\operatorname{char}(\mathbf{A}) = t^n + a_{n-1}t^{n-1} + \dots + a_1 t + a_0, \operatorname{char}(\mathbf{B}) = t^n + b_{n-1}t^{n-1} + \dots + b_1 t + b_0$ be their characteristic polynomials. If $\mathbf{A} \sim \mathbf{B} \pmod{m}$, then*

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

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

$$\widehat{\mathbf{x}}_i \equiv \widehat{\mathbf{x}}_{i-1}\mathbf{A} \pmod{M} \quad \text{for} \quad i = 1, 2, \dots, L, \quad (9)$$

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

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

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

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 $\mathbf{A}_0 \equiv \mathbf{C}^{-1}\mathbf{GC} \pmod{M}$, 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

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

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 $(y_0, \ldots, y_{n-1}) = T(0 \ldots 0 w_0 \ldots w_l)$ we get $0 \ldots 0 w_0 \ldots w_l$ 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.