Вестник Сыктывкарского университета.
Сер.1. Вып.16.2012

УДК 513.88

AN EFFECTIVE ALGORITHM TO PRIVATE-KEY IN THE RSA CRYPTOSYSTEM

A. Grytczuk

In this paper we give an effective algorithm for determinaion in explicit form of the inverse element in private-key in the RSA cryptosystem under the condition when we known the value of the Euler's totient function .Moreover, we present some estimates for the function $\varphi(n)$ for the case when the natural number n is the product of two primes p, q, so $n = pq$ and this result can be applied in RSA cryptosystem. The main theoretical idea is contained in our papers [1].
2000AMS Subject Classification: 11B50,11T71.
Ключевые слова: криптография, криптосистемы RSA, последовательности.

1. Description of the classical algorithm.

We remember that Rivest, Shamir and Adleman in the paper [5] give a very important cryptosystem called as RSA cryptosystem. In the first steep in this cryptosystem we select two different primes p, q.Let $n = p \cdot q$, then we have $\varphi(n) = (p-1) \cdot (q-1)$, where φ is the well-known Euler's function. Next, we select a number k such that $1 < k < \varphi(n)$ .and $\gcd(k, \varphi(n)) = 1$, where $\gcd(x, y)$ denotes the grand common divisor of the integer numbers x, y. Then the pair $\langle k, n \rangle$ is called as public-key of the RSA cryptosystem. The inverse element with respect to k in the multiplicative group Z_m^*, where $m = \varphi(n)$, we denote by l. Then the pair $\langle l, n \rangle$ is called as private-key of the RSA. The determination of the element l in private-key cryptosystem by known classical technique has the following procedure. In the first steep we use classical Euler's theorem:

(1.1) If $(k, m) = 1$ then $k^{\varphi(m)} \equiv 1 \pmod{m}$.

Relation $a \equiv b\,(\bmod m)$ is equivalent to divisibility relation $m \mid a-b$,so denote that there is integer q such that $a-b=mq$,hence $a=mq+b$. On the other hand we known that the element l is inverse to k in the group Z_m^* hence

(1.2) $l \cdot k \equiv 1\,(\bmod m)\,.$

By (1.1), (1.2) and well-known properties of the congruence relation $(\bmod m)$ it follows that

(1.3) $l \equiv k^{\varphi(m)-1}\,(\bmod m)\,.$

From (1.3) we obtain that the element l is the residue of the divisilibity the number $k^{\varphi(m)-1}$ by m.

2. Algorithm based on continued simple finite fractions.

Let $m \geq 2$ be fixed integer and let Z be the ring of all integers. Moreover, let

(2.1) $Z_m^* = \{x \in Z; 1 \leq x \leq m, (x,m)=1\}\,,$

and let $x, y \in Z_m^*$ and " $\circ$" be the following operation in the set (2.1):

(2.2) $x \circ y = r = (x \cdot y)_m\,.$

Element r is the residue which we obtain dividing the product $x \cdot y$ by m.

In our papers [1] have been proved that the set Z_m^* defined by (2.1) with the operation (2.2) is a commutative group with effective and explicit form of the inverse elements.

Now, we give short method for determination such inverse element.

Let $k \in Z_m^*$ and let x be an inverse element to k. Then by (2.2) it follows that there is an integer y such that $k \cdot x = m \cdot y + 1$, hence,

(2.3) $m \cdot y - k \cdot x = -1.$

Since m, k are given integers then we can expanded the rational number $\frac{m}{k}$ on the simple finite continued fraction:

(2.4) $\frac{m}{k} = [q_0; q_1, q_2, ..., q_s]$.

Let $R_j = \frac{P_j}{Q_j}$ be $j - th$ convergent of the fraction (2.4), then $m = P_s, k = Q_s$, and

(2.5) $P_{j-1} \cdot Q_j - P_j \cdot Q_{j-1} = (-1)^j$; $2 \leq j \leq s$.

For $j = s$ by (2.5) it follows that

(2.6) $P_s \cdot Q_{s-1} - Q_s \cdot P_{s-1} = (-1)^{s+1}$.

From (2.6) and (2.3) immediately follows that if $s = 2t$ then

(2.7) $x = P_{s-1} = P_{2t-1}$.

If $s = 2t + 1$ then we obtain

(2.8) $x = m - P_{s-1} = m - P_{2t}$.

By (2.7) and (2.8) it follows that the inverse element x is determined in explicit form.■

3. Application to RSA cryptosystem.

For application of this algorithm to determination of the element l in private-key of RSA cryptosystem it suffices to consider the case when $m = \varphi(n)$. Consider the following example:

Example 1. Let $p = 13, q = 31$. Then we have $n = p \cdot q = 13 \cdot 31 = 403$ and consequently $\varphi(n) = \varphi(p \cdot q) = (p - 1) \cdot (q - 1) = 12 \cdot 30 = 360$. Now, we select in public-key the number $k = 157$,which satisfied the condition $1 < 157 < 360$ and $\gcd(157, 360) = 1$. Then by application to numbers 360 and 157 of the Euclide's algorithm we obtain:

(3.1) $360 = 157 \cdot 2 + 46$; $q_0 = 2$
$157 = 46 \cdot 3 + 19$; $q_1 = 3$
$46 = 19 \cdot 2 + 8$; $q_2 = 2$
$19 = 8 \cdot 2 + 3$; $q_3 = 2$
$8 = 3 \cdot 2 + 2$; $q_4 = 2$
$3 = 2 \cdot 1 + 1$; $q_5 = 1$

$2 = 1 \cdot 2$; $\quad q_6 = 2.$

From (3.1) we have the following form of simple finite continued fraction for rational number $\frac{360}{157}$:

(3.2) $\frac{360}{157} = [2; 3, 2, 2, 2, 1, 2]$.

Using the following formulas for the reducts $R_j = \frac{P_j}{Q_j}; 0 \leq j \leq s$, from the theory of simple finite continued fractions:

(3.3) $P_0 = q_0, Q_0 = 1 : P_1 = q_0 \cdot q_1 + 1, Q_1 = q_1,$

(3.4) $P_j = q_j \cdot P_{j-1} + P_{j-2}, Q_j = q_j \cdot Q_{j-1} + Q_{j-2}$, for all j, such that $2 \leq j \leq s$;

by (3.1),(3.3) and (3.4) we obtain

(3.5) $P_0 = 2, P_1 = 2 \cdot 3 + 1 = 7, P_2 = 2 \cdot 7 + 2 = 16,\ P_3 = 2 \cdot 16 + 7 = 39, P_4 = 2 \cdot 39 + 16 = 94, P_5 = 1 \cdot 94 + 39 = 133, P_6 = 2 \cdot 133 + 94 = 360 = \varphi(n)$

(3.6) $Q_0 = 1, Q_1 = 3, Q_2 = 2 \cdot 3 + 1 = 7, Q_3 = 2 \cdot 7 + 3 = 17, Q_4 = 2 \cdot 17 + 7 = 41, Q_5 = 1 \cdot 41 + 17 = 58, Q_6 = 2 \cdot 58 + 41 = 157 = k.$

Since $s = 6 = 2 \cdot 3$, is even , then by (2.7) and (3.5) it follows that $l = P_{s-1} = P_5 = 133$. ■

Example 2. Let $p = 13, q = 31$ be the same prime numbers as in the **Example 1**, but we select in public-key the number $k = 257$. Then applying similar procedure as in the **Example 1** we obtain

(3.7) $\frac{360}{257} = [1; 2, 2, 51]$, $q_0 = 1, q_1 = 2, q_2 = 2, q_3 = 51.$

By (3.7), (3.3) and (3.4) it follows that

(3.8) $P_0 = 1, P_1 = 3, P_2 = 7, P_3 = 360$

(3.9) $Q_0 = 1, Q_1 = 2, Q_2 = 5, Q_3 = 257.$

Since $s = 3 = 2 \cdot 1 + 1$, is odd, then from (3.8) and (2.8) we have that $l = m - P_{s-1} = \varphi(n) - P_2 = 360 - 7 = 353$.■

Example 3. Now we can compare the classical and our algorithm. In **Example 1** we have $m = \varphi(n) = 360$,hence $\varphi(m) = \varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = \varphi(2^3) \cdot \varphi(3^2) \cdot \varphi(5) = 4 \cdot 6 \cdot 4 = 96$. By (1.3) we have

(3.10) $l \equiv 157^{95}\,(\bmod 360)$,

so denote that for determination in explicit form of the element l in private - key of RSA cryptosystem we must calculate of the value power 157^{95} and next dividing by 360 we obtain the number $l = 133$.

In the **Example 2** we have

(3.11) $l \equiv 257^{95}\,(\bmod 360)$.

Therefore dividing the number 257^{95} by 360 we must obtain the number $l = 353$ which has been determined in **Example 2**.

Now, we give general procedure based on algoritm described in part 2.

We name of this algorithm in short form as:**algorithm of CSFF**

4. Determination of the element l in private-key of the RSA cryptosystem based on algorithm of CSFF

Let $n = p \cdot q$ and $\varphi(n) = (p-1) \cdot (q-1)$. Moreover, let $1 < k < \varphi(n)$,

$\gcd(k, \varphi(n)) = 1$. Then public-key is given by the pair $\langle k, n \rangle$. We determine the inverse element in private-key by the following process:

1^0. The rational number $\frac{\varphi(n)}{k}$ we expande on simple finite continued fraction by application well-known Euclide's algorithm,

(4.1) $\frac{\varphi(n)}{k} = [q_0; q_1, q_2, ..., q_s]$.

2^0. By applications of the formulas (3.3) and (3.4) we determinate P_{s-1}.

3^0. If $s = 2t$ then the inverse element l is given by the formula $l = P_{2t-1}$. If $s = 2t+1$ then $l = \varphi(n) - P_{2t}$.

5. Remark 1. The algorithm based on simple finite continued fraction described in part **4** give explicit form of the inverse element l in private-key $\langle l, n \rangle$ of the RSA cryptosystem but under the condition when we known the value of the Euler function $\varphi(n)$. Therefore in next part of this paper we give an estimate for the function $\varphi(n)$, which can be used in practice cryptography.

6. Estimate for the function $\varphi(n)$.

Since $n = p \cdot q$ then we have

(6.1) $\varphi(n) = (p-1) \cdot (q-1) = p \cdot q + 1 - (p+q) = n + 1 - (p+q)$.

Now,we remark that if x is a real positive number, then we have

(6.2) $x = [x] + \{x\}$,

where $[x]$ denote the integer part of x and $0 \leq \{x\} < 1$.

It is well-known classical inequality:

(6.3) $\frac{p+q}{2} \geq \sqrt{p \cdot q}$.

From (6.2), (6.3) and in virtue of $n = p \cdot q$ we obtain

(6.4) $p + q \geq 2\sqrt{n} \geq 2\left[\sqrt{n}\right]$.

By (6.1) and (6.4) it follows that

(6.5) $\varphi(n) \leq n + 1 - 2\left[\sqrt{n}\right]$.

For lower bound estimation we note that if $n = p \cdot q$ then we have: 1). $p > \sqrt{n}$ and $q \leq \sqrt{n}$ or 2). $q > \sqrt{n}$ and $p \leq \sqrt{n}$. By (6.1) it follows that

(6.6) $\varphi(n) = n \cdot \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right) = n \cdot \left[1 - \left(\frac{1}{p} + \frac{1}{q}\right) + \frac{1}{p \cdot q}\right]$.

Suppose that 1). holds and let $q \geq 11$. Then we have

(6.7) $\frac{1}{p} + \frac{1}{q} < \frac{1}{\sqrt{n}} + \frac{1}{11}$.

From (6.6) and (6.7) we get

(6.8) $\varphi(n) > n \cdot \left[1 - \frac{1}{11} - \frac{1}{\sqrt{n}} + \frac{1}{n}\right] = \frac{10}{11} \cdot n - \frac{n}{\sqrt{n}} + 1 = \frac{10}{11} \cdot n + 1 - \sqrt{n}$.

For $x = \sqrt{n}$ from (6.2) follows that

(.6.9) $\sqrt{n} = \left[\sqrt{n}\right] + \left\{\sqrt{n}\right\} < \left[\sqrt{n}\right] + 1$.

By (6.8) and (6.9) it follows that

(6.10) $\varphi(n) > \frac{10}{11} \cdot n - [\sqrt{n}]$.

From (6.5) and (6.10) we obtain that for every odd primes p, q such that one of p or q is greater than 11 we have the following estimate for function $\varphi(n)$, when $n = p \cdot q$:

(*) $\frac{10}{11} \cdot n - [\sqrt{n}] < \varphi(n) \leq n + 1 - 2 \cdot [\sqrt{n}]$.

Now, we remark that we can obtained better lower bound than (6.1) using the following consideration. Suppose that we have the case 2). Then we have

(6.11) $q > \sqrt{n} = [\sqrt{n}] + \{\sqrt{n}\}, 0 \leq \{\sqrt{n}\} < 1$.

By (6.1) it follows that

(6.12) $q > [\sqrt{n}]$.

From (6.12) and the fundamental theorem of arithmetic we have

(6.13) $q = [\sqrt{n}] \cdot s + r$, where $0 \leq r < [\sqrt{n}], s \geq 1$.

Since from condition (2) we have that $p \leq \sqrt{n} = [\sqrt{n}] + \{\sqrt{n}\} < [\sqrt{n}] + 1$, then by (6.13) we get

(6.14) $p + q < [\sqrt{n}] + 1 + [\sqrt{n}] \cdot s + [\sqrt{n}] = (s + 2)[\sqrt{n}] + 1$.

By (6.14) and (6.1) it follows that

(6.15) $\varphi(n) = n + 1 - (p + q) > n + 1 - (s + 2)[\sqrt{n}] - 1 = n - (s + 2)[\sqrt{n}]$.

From (6.15) and (6.5) for $s = 1$ we obtain

(**) $n - 3[\sqrt{n}] < \varphi(n) < n + 1 - 2[\sqrt{n}]$.

We note that the lover bound estimation for the function φ given in **(**)** is better than **(*)** for all $n > 22^2$.

Example 4. Let $p = 13, q = 31$ as in **Example 1.** Then we have $n = 403, \varphi(n) = 360$. From (*) we obtain

(i) $\frac{10}{11} \cdot 403 - \left[\sqrt{403}\right] < \varphi(n) \leq 403 + 1 - 2 \cdot \left[\sqrt{403}\right]$, hence

(ii) $346 < \varphi(n) < 364.$

Remark 2. From the classical Rosser-Schonenfeld's inequality [6], (Cf.[4],p.169 and [2],p.70) it follows that for all $n \geq 3^9$ we have

(R-S) $\varphi(n) > \frac{n}{1.3e^{\gamma}\log\log n}.$

It is easy to see that the lower bound given by (*) is better for application than (R-S).Upper bound (*) for all composite n in the form: $\varphi(n) < n + 1 - 2 \cdot \sqrt{n}$ have been given in the paper [3].

References

1. **Grytczuk A.** Effective description of the group of reduced system of residues // *Dydaktyka Matematyki, 4 (2003), 17-22, (in Polish).*

2. **Grytczuk A.** Upper bound for sum of divisors function and the Riemann Hypothesis // *Tsukuba J.Math. 31.(2007),67-75.*

3. **Grytczuk A. and Wójtowicz M.** An application of the Minkowski inequality // *Int.J.Pure Appl.Math. 11 (2004), 311-314.*

4. **Ribenboim P.** The Little Book of Big Primes,Springer-Verlag, 1991 (Polish Edition WNT,1997).

5. **Rivest R. L., Shamir A., Adleman L. M.** A method for obtaining digital signatures and public-key cryptosystems // *Comm.ACM, 21 (1978), 120-126.*

6. **Rosser J. B. and Schoenfeld L.** Aproximate formulas for some functions of prime numbers // *Illinois J. Math. 6 (1962), 64-94.*

Summary

Grytczuk A. An effective algorithm to private-key in the RSA cryptosystem

Keywords: Sequences (modm),cryptograpphy,cryptosystem RSA.

University of Zielona Góra, Poland *Поступила 18.12.2012*