Journal of Universal Computer Science, vol. 12, no. 9 (2006), 1215-1228
submitted: 31/12/05, accepted: 12/5/06, appeared: 28/9/06 © J.UCS

The Number of the Modulo n Roots of the Polynomial $x^v - x^u$ and the RSA

János Gonda
(Eötvös University Budapest, Hungary
andog@compalg.inf.elte.hu)

Abstract: RSA is one of the oldest and until now one of the most widely used public key cryptographic systems, which is based on the modular raising to power. In this article it is pointed out that most of the essential properties of the RSA can be read out from the number of the modulo n roots of the polynomial mentioned in the title of this article. The results explain almost all of the properties taken into account at the choice of the parameters of the RSA. By the help of the polynomial it is pointed out how the modulus and the exponent must be chosen so that the modular raising to power realizes a secure cryptosystem. The article investigates also the role of the choice of the parameters related to the success of the cycling attack. The article conveys a unified point of view for the examination of a lot of the number theoretic problems arising with respect to the RSA.

Keywords: modulo n roots, RSA, cycling attack
Category: E.3

1 Introduction

In this article $\mathbf{N}$ denotes the nonnegative integers and $\mathbf{N}^+$ the positive ones and (a,b) denotes the greatest common divisor of the integers a and b.

1.1 On the RSA

RSA is the most frequently applied and best tried public key cryptographic algorithm, which was examined by many experts very thoroughly, and which is practically unbreakable without the trapdoor information – at least by the publicly known information – if the parameters are chosen with the appropriate care. As it is well-known the algorithm itself is the following [Rivest, Shamir, Adleman (78)]. Let Alice be a participant of the cryptosystem. She chooses two different odd prime numbers, p and q, and a positive integer e relatively prime to $\varphi(n)$, where $n = pq$ and φ is the Eulerian totient function and determines the solution d of the congruence $ex \equiv 1 \pmod{\varphi(n)}$. Then $M = \{m \in \mathbf{N} \mid m < n\} = C$ is the set of the plaintexts and the ciphertexts, (e,n) is the public and d is the private key of Alice, and $c = m^e \bmod n$ is the ciphertext corresponding to the plaintext $m \in M$. As Alice knows d, she regains easily the original message m from c as $m = c^d \bmod n$. If somebody knows the factors of n then this person is able to determine d and then similarly to Alice he can easily deci-

pher the message, but by our present knowledge without knowing the factors of n it is practically impossible to decrypt the encrypted message.

Theoretically, there are other possibilities for deciphering a message encrypted by the RSA. One of these possibilities is the , the cycling attack [Simmons, Norris (77)]. Let $c \in M$, then there is such a positive integer k that $c^{e^k} \mod n = c$. As the mapping $m \mapsto c = m^e \mod n$ is injective on M, $c^{e^{k-1}} \mod n = m$ with the previous k, and for the decryption we applied only publicly known information.

1.2 The Number of the modulo n Roots of a Polynomial with Integer Coefficients

Let f be a polynomial over the ring of integers and let n be a positive integer greater than 1. $u \in \mathbf{Z}$ is a modulo n root of f if $f(u) \equiv 0 \pmod{n}$. If $n = \prod_{i=1}^{s} p_i^{r_i}$ is the canonical form of n, that is, the p_i -s are pairwise different prime numbers and the r_i -s are positive integers then

$$f(u) \equiv 0 \pmod{n} \Leftrightarrow \forall\left(s \geq i \in \mathbf{N}^+\right): f(u) \equiv 0 \pmod{p_i^{r_i}} \qquad (1)$$

and then – by the Chinese Remainder Theorem – the number of the modulo n roots of f is equal to the product of the number of the modulo $p_i^{r_i}$ roots of the polynomial. Two modulo n roots of the polynomial are different if and only if they are incongruent modulo n so the number of the modulo n roots of the polynomial is the number of the pairwise incongruent modulo n roots of the polynomial.

1.3 The modulo n Primitive Root

Let n be an integer greater than 1. The modulo n order of $u \in \mathbf{Z}$ is the least positive integer t with the property that $u^t \equiv 1 \pmod{n}$, and u is a modulo n primitive root if the modulo n order of u is equal to $\varphi(n)$ where φ is the Eulerian totient function. The modulo n order of u exists if and only if u is relatively prime to n. By a very nice theorem the necessary and sufficient condition for the existence of a modulo n primitive root is that n is equal to either 2 or 4 or n is a power of an odd prime number with a positive exponent or the double of such a prime power.

In the following parts of this article we investigate that $m \mapsto m^e \mod n$ where n and e are arbitrary positive integers and m is a nonnegative integer less than n on what conditions realizes an encryption, and point out some considerations for the best choice of the parameters.

In Subsection 2.1 we deal with the number of the modulo n roots of the polynomial $x^v - x^u$ and we examine how these results are related to the choice of the parameters of the RSA.

With the results achieved in Subsection 2.1, in Subsection 2.2 we investigate the well-known attack on the RSA applying repeated raising to the power of the ciphertext.

Not the results but the approach explaining the choice of the parameters is new in this article. The article tries to give a unified frame for explaining and handling problems arising in connection with the RSA.

2 Results

2.1 The Number of the modulo *n* Roots of the Polynomial $x^v - x^u$

Lemma 1. *Let n be an odd integer greater than 1, let* $n = \prod_{i=1}^{s} p_i^{r_i}$ *be the canonical form of n, let u be a nonnegative and w a positive integer and let v be an integer greater than u. If* $N_u^{(n)}$ *and* $N_{v,u}^{(n)}$ *denotes the number of the modulo n roots of the polynomials* x^u *and* $x^v - x^u$*, respectively, then*

$$\begin{aligned} N_u^{(n)} &= \prod_{i=1}^{s} p_i^{r_i - \left\lceil \frac{r_i}{u} \right\rceil} \\ N_{w,0}^{(n)} &= \prod_{i=1}^{s} \left(w, \varphi\left(p_i^{r_i}\right)\right) \\ N_{v,u}^{(n)} &= \prod_{i=1}^{s} \left(N_u^{\left(p_i^{r_i}\right)} + N_{v-u,0}^{\left(p_i^{r_i}\right)}\right). \end{aligned} \tag{2}$$

Proof.
As $x^v - x^u = x^u\left(x^{v-u} - x^0\right)$ and $\left(a^u, a^{v-u} - 1\right) = 1$ for any $a \in \mathbf{Z}$, so

$$N_{v,u}^{(n)} = \prod_{i=1}^{s} \left(N_u^{\left(p_i^{r_i}\right)} + N_{v-u,0}^{\left(p_i^{r_i}\right)}\right). \tag{3}$$

If $u = 0$ then $m^u = 1$ for any nonnegative integer *m*. As $r > 0$ so $p^r > 1$ and $p^r \nmid m^0$. From this follows that $N_0^{\left(p^r\right)} = 0 = p^{-\infty} = p^{r - \left\lceil \frac{r}{0} \right\rceil}$, if $\left\lceil \frac{r}{0} \right\rceil = \infty$ and $p^{-\infty} = 0$. If $u > 0$, then let $m = kp^l$ so that *p* doesn't divide *k*. Then $m^u = k'p^{ul}$, and m^u can be divided by p^r if and only if $ul \geq r$ that is, if $l \geq \left\lceil \frac{r}{u} \right\rceil$ as *l* is an integer. In other words m^u is divisible by p^r if and only if *m* is divisible by $p^{\left\lceil \frac{r}{u} \right\rceil}$ that is, if

$m = m'p^{\left\lceil \frac{r}{u} \right\rceil}$. If $0 \le m'p^{\left\lceil \frac{r}{u} \right\rceil} < p^r$ then $0 \le m' < p^{r-\left\lceil \frac{r}{u} \right\rceil}$ and then the number of the modulo p^r roots of the polynomial x^u is equal to $p^{r-\left\lceil \frac{r}{u} \right\rceil}$, that is,

$$N_u^{(p^r)} = p^{r-\left\lceil \frac{r}{u} \right\rceil} \tag{4}$$

for any nonnegative integer *u*.

Now let's consider the polynomial $x^w - 1$. If *m* is a modulo p^r root of that polynomial then $m^w \equiv 1 \pmod{p^r}$. If *p* is an odd prime number and *r* is a positive integer then there exist modulo p^r primitive roots. Let α be one of them, then there is a uniquely determined nonnegative integer *k* less than $\varphi(p^r)$ with the property that $\alpha^k \equiv m \pmod{p^r}$. Then

$$\alpha^{kw} = (\alpha^k)^w = m^w \equiv 1 = \alpha^0 \pmod{p^r}. \tag{5}$$

As α is a modulo p^r primitive root so (5) is equivalent to the congruence

$$kw \equiv 0 \pmod{\varphi(p^r)} \tag{6}$$

and this congruence is true if and only if $\varphi(p^r) \mid kw$, or, dividing by the greatest common divisor of *w* and $\varphi(p^r)$, if and only if $\frac{\varphi(p^r)}{(w, \varphi(p^r))} \mid k$. This means that *k* is a multiple of $\frac{\varphi(p^r)}{(w, \varphi(p^r))}$ that is, $k = l\frac{\varphi(p^r)}{(w, \varphi(p^r))}$ with an integer *l*. But $\varphi(p^r) > k \in \mathbf{N}$ and then $0 \le l < (w, \varphi(p^r))$ so

$$N_{w,0}^{(p^r)} = (w, \varphi(p^r)). \tag{7}$$

□

As a special case we get that if $u = 1$ then

$$N_{v,1}^{(n)} = \prod_{i=1}^{s} (1 + (v - 1, \varphi(p_i^{r_i}))). \tag{8}$$

From these results we get the following properties introducing t as the least common multiple of the $\varphi\left(p_i^{r_i}\right)$-s.

Proposition 1. *Let n be an odd integer greater than 1, where $n=\prod_{i=1}^{s} p_i^{r_i}$ is the canonical form of n, let u be a nonnegative integer and v an integer greater than u. Then*

1. $0 \le N_u^{(n)} \le \prod_{i=1}^{s} p_i^{r_i-1}$;
   a) $N_u^{(n)}=0$ *if and only if* $u=0$;
   b) $N_u^{(n)}=1$ *if and only if* $u=1$, *or* $r_i=1$ *for every* $s \ge i \in \mathbf{N}^+$, *that is, if n is square free;*
   c) $N_u^{(n)}=\prod_{i=1}^{s} p_i^{r_i-1}$ *if and only if* $u \ge \max\left\{r_i \,\middle|\, s \ge i \in \mathbf{N}^+\right\}$;

2. $1 \le N_{v,0}^{(n)} \le \varphi(n)$;
   a) $N_{v,0}^{(n)}=1$ *if and only if* $(v,\varphi(n))=1$;
   b) $N_{v,0}^{(n)}=\varphi(n)$ *if and only if* $t \mid v$, *and* $N_{\varphi(n),0}^{(n)}=\varphi(n)$ *(this is the Euler-Fermat theorem);*

3. *if* $u \ge 1$ *then* $2^s \le N_{v,u}^{(n)} \le n$ *and*
   a) $N_{v,u}^{(n)}=2^s$ *if and only if* $u=1$ *or n is square free, and* $(v-u,\varphi(n))=1$;
   b) $N_{v,u}^{(n)}=n$ *if and only if* $u \ge \max\left\{r_i \,\middle|\, s \ge i \in \mathbf{N}^+\right\}$ *and* $t \mid v-u$;
   c) *if* $v-u$ *is even then* $N_{v,u}^{(n)} \ge 3^s$;

4.
   a) $N_{v,1}^{(n)}=2^s$ *if and only if* $v-1$ *and* $\varphi(n)$ *are coprimes;*
   b) *if* v *is odd then* $N_{v,1}^{(n)} \ge 3^s$;
   c) $N_{v,1}^{(n)}=n$ *if and only if n is square free and* $t \mid v-1$;
   d) *if n is a square free integer then* $m^{1+k\varphi(n)} \equiv m \pmod{n}$ *for every integer m and nonnegative integer k;*

5. *if n is square free, k is a positive integer and e is a positive integer relatively prime to kt then for an arbitrary positive integer j relatively prime to e and positive integer d satisfying the congruence* $ed \equiv 1 \pmod{jt}$ *it is true for any integer m that* $\left(m^e\right)^d \equiv m \pmod{n}$; *as a special case the previous statement is true if* $(e,\varphi(n))=1$ *and* $ed \equiv 1 \pmod{\varphi(n)}$;

6. *if n is square free,* $n=\prod_{i=1}^{s'}u_i$ *where every* u_i *is an integer greater than* 1, $t'=\prod_{i=1}^{s'}(u_i-1)$, *e is a positive integer relatively prime to* t' *and d is such a positive integer that* $ed\equiv 1 \pmod{t'}$ *then*

   a) $(m^e)^d \equiv m \pmod{n}$ *for every integer m if and only if t divides* $ed-1$;

   b) 6.a) is true for any e possible if and only if $t \mid t'$.

Proof.

1. If $u=0$ then $a^u=1$ for any integer *a* and $n \nmid 1$ as $n>1$. Conversely, if $u>0$ then for instance $0^u=0$ and $n \mid 0$, so there is at least one modulo *n* root of the polynomial x^u.

Now let's suppose $u>0$, that is, $u\geq 1$ as *u* is an integer. $\prod_{i=1}^{s} p_i^{r_i-\left\lceil \frac{r_i}{u} \right\rceil}=N_u^{(n)}=1$ if and only if $r_i-\left\lceil \frac{r_i}{u} \right\rceil=0$, that is, if $r_i=\left\lceil \frac{r_i}{u} \right\rceil$ for every index $s\geq i\in \mathbf{N}^+$. As $u\geq 1$, so $\frac{r_i}{u}\leq r_i$ and then $\left\lceil \frac{r_i}{u} \right\rceil \leq r_i$, that is, $r_i=\left\lceil \frac{r_i}{u} \right\rceil$ if and only if $r_i \leq \left\lceil \frac{r_i}{u} \right\rceil$, and this relation is equivalent to $r_i-1<\frac{r_i}{u}$. From the last inequality we get that $(u-1)(r_i-1)<1$ and then $u=1$ or $r_i=1$ for every *i* as both *u* and the r_i-s are positive integers.

As $r_i>0$ and *u* is positive so $\frac{r_i}{u}$ is a positive real number and then $\left\lceil \frac{r_i}{u} \right\rceil \geq 1$. $p_i^{r_i-\left\lceil \frac{r_i}{u} \right\rceil}$ is a monotone increasing function of *u* and it reaches its maximum when $\left\lceil \frac{r_i}{u} \right\rceil=1$ and this is true with the fixed r_i if and only if $u\geq r_i$.

2. $N_{v,0}^{(n)}=1$ if and only if *v* is relatively prime to every $\varphi(p_i^{r_i})$ and this is true exactly when *v* is relatively prime to the product of the $\varphi(p_i^{r_i})$-s, that is, to $\varphi(n)$.

$\varphi(p_i^{r_i})>0$, so $(v,\varphi(p_i^{r_i}))\leq \varphi(p_i^{r_i})$ and the equality is true if and only if $\varphi(p_i^{r_i}) \mid v$ for every index, that is, if the least common multiple of the $\varphi(p_i^{r_i})$-s divides *v*. The special case is obvious as the least common multiple divides the product of the members of the least common multiple.

3. $N_{v,u}^{(n)}$ is minimal if and only if every factor of the product is minimal. The factors of the product are sums of two positive integers. These factors are minimal if all of these positive integers have the least values possible. From the previous results we get

that the least values are 1 so the minimal value of every factor of the product is equal to 2. As the number of the factors is *s* so the minimal value of $N_{v,u}^{(n)}$ is equal to 2^s and it is easy to read out from the previous section the conditions for this result. If $v-u$ is even then $\left(v-u,\varphi\left(p_i^{r_i}\right)\right)\geq 2$ as $\varphi\left(p_i^{r_i}\right)$ is always even if p_i is odd.

Similarly to the minimal value, the maximum of $N_{v,u}^{(n)}$ is reached if and only if all of the factors in the expression are maximal. As $\varphi\left(p_i^{r_i}\right)=p_i^{r_i}-p_i^{r_i-1}$, so this maximum is $p_i^{r_i}$ and then $\max\left(N_{v,u}^{(n)}\right)=n$. We get this value if and only if $p_i^{r_i-\left\lceil\frac{r_i}{u}\right\rceil}=p_i^{r_i-1}$ and $\left(v-u,\varphi\left(p_i^{r_i}\right)\right)=\varphi\left(p_i^{r_i}\right)$ for every index $1\leq i\leq s$, that is, if and only if $u\geq\max\left\{r_i\,\middle|\,s\geq i\in\mathbf{N}^+\right\}$ and $t\,|\,v-u$.

4. These results are special cases of the previous results in 3. For now $u=1$ so $u\geq\max\left\{r_i\,\middle|\,s\geq i\in\mathbf{N}^+\right\}$ is the same condition as *n* is square free, and since $t\,|\,\varphi(n)$ so $t\,|\,(1+k\varphi(n))-1$.

5. If $(e,kt)=1$ then *e* and *t* are coprimes, too. Similarly, if both *t* and *j* are relatively primes to *e*, then also their product, *jt* is relatively prime to *e*, and then there exists such a positive integer *d* that $ed\equiv 1\pmod{jt}$. Then $t\,|\,ed-1$ and $N_{v,1}^{(n)}=n$ as *n* is square free. The special case is true, too, as $t\,|\,\varphi(n)$.

6. 6.a) is a simple consequence of 4.

If $t\,|\,t'$ then $t\,|\,ed-1$. Conversely, if 6.a) is true for any positive integer *e* relatively prime to t' then let *k* be such a positive integer that $(k,t)=1$ and let $ed=1+kt'$. It is easy to see that there is such a *k* that *ed* is a composite number. Now $t\,|\,ed-1=kt'$ and then $t\,|\,t'$ as *t* and *k* are coprimes.

□

An encryption is decipherable only if the encrypting rule is injective (it is true in the case of the homophonic enciphering with the appropriate meaning). From the previous results, we can read out the following consequences.

Corollary 1. *Let* $1<n\in\mathbf{N}^+$, $n=\prod_{i=1}^{s}p_i^{r_i}$ *with parwise distinct odd prime factors,* $1<e\in\mathbf{N}^+$, *and let* $f:m\mapsto m^e \bmod n$ *be a mapping of* $M^{(n)}$ *into itself. Then this mapping has* $\prod_{i=1}^{s}\left(1+\left(e-1,\varphi\left(p_i^{r_i}\right)\right)\right)$ *fixed points. f is injective if and only if n is square free and e is relatively prime to* $\varphi(n)$ *and then the number of the fixed points is equal to* $\prod_{i=1}^{s}\left(1+\left(e-1,p_i-1\right)\right)$.

Remark 1. *As* $M^{(n)}$ *is a finite set so if f is injective then it is bijective, too.*

Remark 2. If $e=1$ *then* $m^e \bmod n = m$ *for every* $m \in M^{(n)}$ *and then the ciphertext is equal to the plaintext which is not a real encryption.*

Proof.
m is a fixed point of the mapping if and only if $m = f(m) = m^e \bmod n$, that is, if and only if m is a modulo n root of the polynomial $x^e - x$ and then the number of the fixed points is equal to the number of the modulo n roots of the polynomial. This number is $N_{e,1} = \prod_{i=1}^{s} \left(1 + \left(e-1, \varphi\left(p_i^{r_i}\right)\right)\right)$ by the equation (8).

Let e and $\varphi(n)$ be coprimes, then there exists such a positive integer d that $ed \equiv 1 \pmod{\varphi(n)}$, that is, $\varphi(n) \mid ed-1$ and then $t \mid ed-1$. If n is square free then the number of the modulo n roots of the polynomial $x^{ed} - x$ is equal to n, that is, $m^{ed} \bmod n = m$ for every nonnegative integer less than n. This means that $h : m \mapsto m^{ed} \bmod n$ is the identical mapping of $M^{(n)}$ into itself and then h is a bijective mapping. But

$$h(m) = m^{ed} \bmod n = \left(m^e \bmod n\right)^d \bmod n = g(f(m)) = (gf)(m) \qquad (9)$$

where both f and g are mappings of $M^{(n)}$ into itself and $f : m \mapsto m^e \bmod n$. As h is a bijective mapping, and then it is injective, so f is injective, too.

On the other hand, if n is not square free, then, because of $e > 1$, the polynomial x^e has more than one modulo n root (see 1.b)), so f is not injective. Similarly, if e is not relatively prime to $\varphi(n)$, then the polynomial $x^e - 1$ has more than one modulo n root (see 2.a)), and f is not injective again.

Finally, if n is a square free integer, then $\varphi\left(p_i^{r_i}\right) = \varphi(p_i) = p_i - 1$ and in this case $\prod_{i=1}^{s} \left(1 + \left(e-1, \varphi\left(p_i^{r_i}\right)\right)\right) = \prod_{i=1}^{s} \left(1 + \left(e-1, p_i - 1\right)\right)$.

□

Some further properties are true, too. As 5. shows if somebody knows d then this person easily regains the plaintext from the ciphertext encrypted by the corresponding e. It can be seen, too, that if $n = pq$ with the odd and distinct p and q, and at least one of them is not square free or the two numbers are not coprimes (the latter property is easy to be checked but the first one is not) then surely there is such a plaintext m that $\left(m^e \bmod n\right)^d \bmod n \neq m$. Last but not least if $n = pq$ is square free but at least one of the two factors is a composed number but we think they are primes and we treat them as prime numbers, and we calculate d so that $ed \equiv 1 \pmod{(p-1)(q-1)}$ is

fulfilled then by 6.a) we can decipher all of the ciphertexts error free if and only if $ed \equiv 1 \pmod{t}$ is fulfilled, too.

As fixed points are not desirable, the fewer fixed points a cryptosystem has the better the system is. $\varphi(n)$ is even for an odd n so e is odd if it is relatively prime to $\varphi(n)$ and then the number of the fixed points is at least 3^s. We can reduce the number of the fixed points if the number of the factors of n is the smallest possible, that is, if n is the product of only two factors.

2.2 The Iterative Deciphering of the RSA and the Choice of the Parameters

Proposition 2. *Let* $1 < e \in \mathbf{N}$, $2 < n \in \mathbf{N}$, *and for* $m \in M^{(n)}$ *let* $c = m^e \bmod n$. *Then there exists such a* $k \in \mathbf{N}^+$ *that* $c^{e^{k-1}} \bmod n = m$ *for every* $m \in M^{(n)}$ *if and only if the mapping* $f : m \mapsto m^e \bmod n$ *is injective on* $M^{(n)}$, *and then* $k = o_t(e)$ *is the smallest such exponent.*

Remark 3. Let m and n be two positive integers. Then $o_n(m)$ denotes the modulo n multiplicative order of m, that is, $o_n(m) = \min\left\{k \in \mathbf{N}^+ \,\middle|\, m^k \equiv 1 \pmod{n}\right\}$.

Proof.

Let $n = \prod_{i=1}^{s} p_i^{r_i}$, where $s \in \mathbf{N}^+$, let the p_i-s be pairwise different prime numbers and the r_i-s positive integers, $u \in \mathbf{N}$, $u_1 \in \mathbf{N}$, $u_2 \in \mathbf{N}$ and $u < v \in \mathbf{N}$, $u_1 < v_1 \in \mathbf{N}$, $u_2 < v_2 \in \mathbf{N}$. If $u_1 \le u_2$ and $m \in M_{u_1}^{(n)}$, then $n \mid m^{u_1} \mid m^{u_2}$, that is, $m \in M_{u_2}^{(n)}$, so consequently $M_{u_1}^{(n)} \subseteq M_{u_2}^{(n)}$, and then $N_{u_1}^{(n)} \le N_{u_2}^{(n)}$. If $v_1 - u_1 \mid v_2 - u_2$ additionally to $u_1 \le u_2$, and $m \in M_{v_1,u_1}^{(n)}$, then

$$\begin{aligned} n \mid m^{v_1} - m^{u_1} &= m^{u_1}\left(m^{v_1-u_1} - 1\right) \\ m^{u_1}\left(m^{v_1-u_1} - 1\right) \mid m^{u_2}\left(m^{v_2-u_2} - 1\right) &= m^{v_2} - m^{u_2} \end{aligned} \tag{10}$$

that is, $m \in M_{v_2,u_2}^{(n)}$, and consequently $M_{v_1,u_1}^{(n)} \subseteq M_{v_2,u_2}^{(n)}$, as well as $N_{v_1,u_1}^{(n)} \le N_{v_2,u_2}^{(n)}$. If now $M_{v_1,u_1}^{(n)} \subseteq M_{v_2,u_2}^{(n)}$ and $N_{v_1,u_1}^{(n)} = N_{v_2,u_2}^{(n)}$, then we get that $M_{v_1,u_1}^{(n)} = M_{v_2,u_2}^{(n)}$, that is, in that case by increasing the exponents we don't get further modulo n roots of the polynomial $x^v - x^u$.

Now let $e \in \mathbf{N}^+$ and $k \in \mathbf{N}^+$. $c^{e^k} \bmod n = c$ is fulfilled for a $c \in M^{(n)}$ exactly in that case if $c \in M_{e^k,1}^{(n)}$, and the number of the messages decipherable by this exponent of k is $N_{e^k,1} = \prod_{i=1}^{s}\left(1 + \left(e^k - 1, \varphi\left(p_i^{r_i}\right)\right)\right)$. $M_{e^k,1}^{(n)} = M^{(n)}$ with a given e and k if and

only if $N_{e^k,1} = n$. This equation is equivalent to the conditions that n is square free and $p_i - 1 \mid e^k - 1$ for every $s \geq i \in \mathbf{N}^+$. The latter condition can be fulfilled only if e is relatively prime to all of the $\varphi(p_i) = p_i - 1$-s, that is, to $\varphi(n)$. For each condition mentioned is fulfilled in an RSA system, so the ciphertexts encrypted by the rules of the RSA can be decrypted by repeated exponentiations with an appropriate exponent, too, as if the conditions are fulfilled then the mapping $m \mapsto m^e \bmod n$ is injective, and

$$\left(c^{e^{k-1}} \bmod n\right)^e \bmod n = c^{e^k} \bmod n = c = m^e \bmod n \qquad (11)$$

with the previous k, and then $m = c^{e^{k-1}} \bmod n$.

Let e be relatively prime to $\varphi(n)$. $p_i - 1 \mid e^k - 1$ is true exactly when $o_{p_i-1}(e) \mid k$, so $N_{e^k,1} = n$ with a given k is true if and only if $o \mid k$, where

$$o = lcm\left\{o_{p_i-1}(e) \,\middle|\, s \geq i \in \mathbf{N}^+\right\} \qquad (12)$$

and the minimal value of these k-s is precisely o. The previously mentioned possibility for the decryption is applicable in the practice only if either o is not a big number, or the greatest part of the messages can be decrypted by small exponents. Consequently, in a secure system the value of o is such a big number that practically this procedure of deciphering is impossible, and the proportion of the messages decipherable with exponents less than o is small. Of course the at least 3^s fixed points can be decrypted with $k = 1$. If $o_{p_i-1}(e) < o$ for every i (which is true in every normal case), then at least $3^{s-1} p_i$ messages are decipherable with the exponent of $o_{p_i-1}(e)$, so our expectation can only be that apart from the fixed points no other ciphertexts can be deciphered by an exponent less than the previously mentioned $o_{p_i-1}(e)$-s.

Big value for o can be achieved if $o_{p_i-1}(e)$ is as great as possible for every i, and $\left(o_{p_i-1}(e), o_{p_j-1}(e)\right)$ is the smallest value possible for all of the indices $i \neq j$.

$o_{p_i-1}(e) \mid \varphi(p_i - 1)$, so $\varphi(p_i - 1)$ is the greatest value possible for $o_{p_i-1}(e)$. Such an e exists if and only if the value of $p_i - 1$ is either 2, 4 or $2 p_i^{(1)r_i^{(1)}}$ (because $p_i - 1$ is even), where $p_i^{(1)}$ is an odd prime number and $r_i^{(1)} \in \mathbf{N}^+$, that is, in the case of an RSA exactly when $p_i - 1 = 2 p_i^{(1)r_i^{(1)}}$, as the small factors are easily discoverable. Thus let $p_i - 1 = 2 p_i^{(1)r_i^{(1)}}$, then $\varphi(p_i - 1) = p_i^{(1)r_i^{(1)}-1}\left(p_i^{(1)} - 1\right)$, and let e be a modulo $p_i - 1$

primitive root, that is, let $(e, p_i - 1) = 1$ and $o_{p_i - 1}(e) = \varphi(p_i - 1)$. If $(e, p_i - 1) = 1$ then also $\left(e, p_i^{(1)r_i^{(1)}-1}\right) = 1$. Then $e^{\varphi\left(2p_i^{(1)r_i^{(1)}-1}\right)} \equiv 1 \left(\bmod 2p_i^{(1)r_i^{(1)}-1}\right)$, so

$$2p_i^{(1)r_i^{(1)}-1} \left| \left(e^{\varphi\left(2p_i^{(1)r_i^{(1)}-1}\right)} - 1, 2p_i^{(1)r_i^{(1)}}\right)\right. \tag{13}$$

furthermore

$$\left(e^{\varphi\left(2p_i^{(1)r_i^{(1)}-1}\right)} - 1, 2p_i^{(1)r_i^{(1)}}\right) < 2p_i^{(1)r_i^{(1)}} \tag{14}$$

because $o_{p_i-1}(e) = \varphi\left(2p_i^{(1)r_i^{(1)}}\right)$, and finally

$$\left(e^{\varphi\left(2p_i^{(1)r_i^{(1)}-1}\right)} - 1, 2p_i^{(1)r_i^{(1)}}\right) \left| 2p_i^{(1)r_i^{(1)}}\right. . \tag{15}$$

From the three relations we get that

$$\left(e^{\varphi\left(2p_i^{(1)r_i^{(1)}-1}\right)} - 1, 2p_i^{(1)r_i^{(1)}}\right) = 2p_i^{(1)r_i^{(1)}-1} \tag{16}$$

and then in the case of $r_i^{(1)} > 1$ not only the fixed points can be deciphered by an exponent less than $o_{p_i-1}(e)$. For this reason let $r_i^{(1)} = 1$ for every $s \geq i \in \mathbf{N}^+$, in other words, let every prime factor of *n* be of the form $p_i = 2p_i^{(1)} + 1$ where $p_i^{(1)}$ is an odd prime number. Then

$$\left(e^k - 1, p_i - 1\right) = \begin{cases} 2 \\ p_i - 1 \end{cases} . \tag{17}$$

$e - 1 \left| e^k - 1 \right.$ with an arbitrary positive integer *k*, thus $M_{e,1}^{(p_i)} \subseteq M_{e^k,1}^{(p_i)}$, and if $N_{e^k,1}^{(p_i)} = 2$, then $M_{e,1}^{(p_i)} = M_{e^k,1}^{(p_i)}$, that is, with such a choice of the p_i-s only the fixed points can be decrypted with small exponents.

The modulo $p_i - 1$ order of e is equal to o_i if and only if $e^{o_i} \equiv 1 \pmod{p_i - 1}$ and $e^{\frac{o_i}{p}} \not\equiv 1 \pmod{p_i - 1}$ for every prime divisor p of o_i, and for the multiplicative order is always fulfilled that $o_i \mid \varphi(p_i - 1) = \varphi\left(p_i^{(1)}\right) = p_i^{(1)} - 1$. The number of the modulo $p_i - 1$ primitive roots is $\varphi\left(p_i^{(1)} - 1\right)$. $\varphi\left(p_i^{(1)} - 1\right) \le \frac{p_i^{(1)} - 1}{2}$, since $p_i^{(1)} - 1$ is an even number, and $\varphi\left(p_i^{(1)} - 1\right) < \frac{p_i^{(1)} - 1}{2}$ if $p_i^{(1)} - 1$ is not a power of 2. If $p_i^{(1)} - 1 = 2^l$ then $p_i^{(1)}$ is a Fermat-prime, and this case is very unlikely (perhaps impossible). Then $\varphi\left(p_i^{(1)} - 1\right) \le \frac{p_i^{(1)} - 1}{2} - 1$ and $\varphi\left(p_i^{(1)} - 1\right) = \frac{p_i^{(1)} - 1}{2} - 1$ if and only if $\frac{p_i^{(1)} - 1}{2} = p_i^{(2)}$ is a prime number, in other words, if $p_i^{(1)} = 2p_i^{(2)} + 1$ with a prime number $p_i^{(2)}$. Then on the one hand, the proportion of the primitive roots is

$$\begin{aligned} \frac{\varphi\left(p_i^{(1)} - 1\right)}{p_i} &= \frac{p_i^{(2)} - 1}{p_i} = \frac{\frac{p_i^{(1)} - 1}{2} - 1}{p_i} = \frac{p_i^{(1)} - 3}{2p_i} \\ &= \frac{\frac{p_i - 1}{2} - 3}{2p_i} = \frac{p_i - 7}{4p_i} \approx \frac{1}{4} \end{aligned} \tag{18}$$

so it is easy to hunt a primitive root, and on the other hand, in the case of an arbitrary positive integer k it is easy to check whether k is a primitive root as if $p_i - 1 \nmid k^2 - 1$ and $p_i - 1 \nmid k^{p_i^{(2)}} - 1$ then $o_{p_i - 1}(k) = \varphi(p_i - 1)$.

Finally, with the previous choice

$$\begin{aligned} o &= lcm\left\{o_i \mid s \ge i \in \mathbf{N}^+\right\} \\ &= lcm\left\{2p_i^{(2)} \mid s \ge i \in \mathbf{N}^+\right\} = 2\prod_{i=1}^{s} p_i^{(2)} \end{aligned} \tag{19}$$

and applying the previous result

$$\frac{o}{n} = \frac{2\prod_{i=1}^{s} p_i^{(2)}}{\prod_{i=1}^{s} p_i} \approx 2\prod_{i=1}^{s} \frac{1}{4} = 2^{-(2s-1)} \tag{20}$$

so the smaller the value of *s* is, the greater $\frac{o}{n}$ is. Since in an RSA system *n* is surely a composed number, so the best choice is $s=2$, which is the best case with regard to the number of the fixed points, too. Now $N^{(n)}_{e^{2p_1^{(2)}},1}=3p_i$ for $i=1$ and $i=2$ and these values are relatively big numbers for both of the indices, if $p_1 \approx p_2$, that is, if both of the factors of *n* are approximately equal to $\sqrt{n}$.

□

There is a modification of the iterative decryption. If $\left(\left(c^{e^k}-c\right)\bmod n,n\right)>1$ and $\left(c^{e^k}-c\right)\bmod n \neq 0$ then either $\left(\left(c^{e^k}-c\right)\bmod n,n\right)=p_1$ or $\left(\left(c^{e^k}-c\right)\bmod n,n\right)=p_2$ and then *n* is factorized and the system is broken. But if both p_1 and p_2 are doubly Sophie Germain primes then this happens only if $k=2p_1^{(2)}$ or $k=2p_2^{(2)}$, that is, if $k \approx \frac{\sqrt{n}}{2}$.

3 Conclusion

In the previous parts of the article we could see that there is a natural relationship between the theoretically best choice of the parameters of an RSA system and the number of the modulo *n* roots of a special polynomial of integer coefficients namely of the polynomial $x^v - x^u$. Although there are other constrains on the choice of the parameters, the greatest part of the constrains follows from the properties of this polynomial. The analysis of the number of the modulo *n* roots of the polynomial $x^v - x^u$ shows that the mapping $m \mapsto m^e \bmod n$ of the set of the nonnegative integers less than *n* into itself is injective if and only if *n* is a squarefree integer and *e* is relatively prime to $\varphi(n)$. By the help of the analysis we pointed out that the cycling attack on the RSA is successful only in a very few cases if *n* is a product of only two factors of the same magnitude that are doubly Sophie Germain primes, and *e* is a primitive root with respect to $p-1$ and $q-1$ as moduli, where *p* and *q* are the two different factors of *n*.

References

[Menezes, Oorshot, Vanstone (96)] Menezes, A., Oorshot, P. V., Vanstone, S.: "Handbook of Applied Cryptography"; CRC Press, Inc. (1996)

[Niven, Zuckerman, Montgomery (91)] Niven, I., Zuckerman, H. S., Montgomery, H. L.: "An Introduction to the Theory of Numbers"; John Wiley & Sons, Inc., New York (1991)

[Rivest, Shamir, Adleman (78)] Rivest, R. L., Shamir, A., Adleman, L.: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"; Communications of the ACM 21, 2 (1978), 120-126

[Simmons, Norris (77)] Simmons, G. J., Norris, M. J.: "Preliminary comment on the M.I.T. *public-key cryptosystem*"; Cryptologia, 1 (1977), 406-414