ISSN 1995-0802, Lobachevskii Journal of Mathematics, 2016, Vol. 37, No. 3, pp. 284–287. © Pleiades Publishing, Ltd., 2016.

RSA Cryptosystem for Dedekind Rings

K. A. Petukhova* **and S. N. Tronin****

(Submitted by E. K. Lipachev)

N.I. Lobachevskii Institute of Mathematics and Mechanics, Kazan (Volga Region) Federal University, Kremlevskaya ul. 18, Kazan, Tatarstan, 420008 Russia

Received July 6, 2015

Abstract—May soon be invented quantum computer and some known cryptosystems (such as RSA) will be threatened breaking. This paper is aimed at establishing necessary conditions for the maximum possible algebraic generalization of the classical RSA algorithm. We substitute ideals of a Dedekind ring for integers. Ideals in Dedekind rings allow the unique decomposition into a product of maximal ideals, but may not be the principal ideals. Also we define Euler's φ-function for ideal of a Dedekind ring and describe some properties of this function. We hope that our proposed method will help to develop algorithms for encryption, which is hard to crack using a quantum computer.

DOI: 10.1134/S1995080216030197

Keywords and phrases: *Algebraic cryptography, RSA, Dedekind ring, ideal, Euler's function, algebraic numbers, cryptographic protocol, security.*

1. INTRODUCTION

The aim of this paper is to establish necessary conditions for the maximum possible generalization of the well-known RSA algorithm. Integers are substituted by the ideals of a Dedekind ring. Herewith we use only the ideals, which possess the following the next property: quotient ring of any maximal ideal is the finite field. It is sufficient for defining an analog of Euler's function on the ideals of this ring. This generalized Euler's function possesses numerous properties typical for the normal Euler's function. It is possible to use this function to construct the cryptographic algorithm, which is coincident with the normal RSA algorithm if the original ring is the ring of integers.

Let us briefly describe the content of the paper. In section 1 we describe the main properties of the generalized Euler's function. In section 2 we construct an analog of the RSA algorithm and prove the correctness of this algorithm. In section 3 we present our ideas how to choose some Dedekind rings, which may be used instead of $\mathbb{Z}$. The author [6] proved that using the algebraic integers quadratic ring does not increase cryptographic security of the RSA algorithm. Note, that quadratic ring of algebraic integers are widely used in mathematical cryptography [1, 4].

We will further show the cryptographic security of the expected algorithm for some different Dedekind rings.

The results of this research were announced in [10].

*E-mail: ksenypet@mail.ru
**E-mail: Serge.Tronin@kpfu.ru

2. EULER'S φ-FUNCTION FOR IDEAL OF A DEDEKIND RINGS

Let us remember that the power of quotient ring $R/\mathfrak{A}$ is denoted $N(\mathfrak{A})$ and is called the norm of ideal $\mathfrak{A} \in R$.

Lemma 1. *Let R be a Dedekind ring, and $R/\mathfrak{P} < \infty$ for every maximal ideal $\mathfrak{P}$. Then $|R/\mathfrak{A}| = N(\mathfrak{A}) < \infty$ for every ideal $\mathfrak{A}$. With that if $\mathfrak{A} = \mathfrak{P}^n$, then $N(\mathfrak{P}^n) = N(\mathfrak{P})^n$.*

Proof. Since $\mathfrak{P}^n/\mathfrak{P}^{n+1} \cong R/\mathfrak{P}$ ([8, p. 13,(5)]), $|\mathfrak{P}^n/\mathfrak{P}^{n+1}| = |R/\mathfrak{P}| = N(\mathfrak{P})$.

Proof is made by the induction on n. Inductive hypothesis is $|R/\mathfrak{P}^n| = N(\mathfrak{P})^n$. Case $n = 1$ comes from the hypothesis of lemma. In case $n = 2$ we have $A \subset B \subset R$. Then there exists homomorphism $f : R/A \to R/B$, and $Ker(f) = B/A$. $f : x + A \to x + B$. Since $\mathfrak{P}^2 \subset \mathfrak{P}$, $f : R/\mathfrak{P}^2 \to R/\mathfrak{P}$ is surjective, $|Ker(f)| = |\mathfrak{P}/\mathfrak{P}^2| = N(\mathfrak{P})$. Above $|R/\mathfrak{P}^2| = |R/\mathfrak{P}| \cdot |\mathfrak{P}/\mathfrak{P}^2|$, hence $N(\mathfrak{P}^2) = N(\mathfrak{P})^2$. Suppose $|R/\mathfrak{P}^n| = N(\mathfrak{P})^n < \infty$. From $\mathfrak{P}^{n+1} \subset \mathfrak{P}^n$ we have surjective homomorphism $f : R/\mathfrak{P}^{n+1} \to R/\mathfrak{P}^n$, and $Ker(f) = \mathfrak{P}^n/\mathfrak{P}^{n+1}$. Hence $|R/\mathfrak{P}^{n+1}| \cong |R/\mathfrak{P}^n| \cdot |\mathfrak{P}^n/\mathfrak{P}^{n+1}| = N(\mathfrak{P})^n \cdot N(\mathfrak{P}) = N(\mathfrak{P})^{n+1}$.

From this point we will consider a Dedekind rings taking into account the following condition: $|R/\mathfrak{M}| < \infty$ for every maximal ideal. In particular, all the rings of algebraic integers satisfy this condition. Herewith assuming the above, we can define the Euler's function analog for the ideals of ring R:

$$\varphi(\mathfrak{A}) = |U(R/\mathfrak{A})|,$$

where $U(R/\mathfrak{A})$ is a group of units. This definition is correct by the lemma 1.

If $|R/\mathfrak{M}| < \infty$, where $\mathfrak{M}$ is a maximal ideal, then φ-function is defined for every ideal of a Dedekind ring R. If $\mathfrak{A} = \mathfrak{M}_1^{k_1} \cdot \mathfrak{M}_2^{k_2} \cdot \ldots \cdot \mathfrak{M}_m^{k_m}$, then $\varphi(\mathfrak{A}) = \prod_{i=1}^{m} \varphi(\mathfrak{M}_i^{k_i})$.

Lemma 2. *Let $\mathfrak{O}$ is a ring, $\mathfrak{N}$ is a maximal ideal and all elements from $\mathfrak{N}$ is nilpotent. Then $\mathfrak{O}$ is a local ring.*

Proof. Let $u \in \mathfrak{O}$, $u \notin \mathfrak{M}$, then $\mathfrak{O}u + \mathfrak{M} = \mathfrak{O}$. Hence $1 = wu + z$, where $w \in R$, $z \in \mathfrak{M}$. Then $wu = 1 - z$. But since z is nilpotent, then $1 - z$ is invertible. Hence u is invertible and u is not element of $\mathfrak{M}$. This means that $\mathfrak{O}$ is a local.

Theorem 1.*Let R be a Dedekind ring such that $|R/\mathfrak{M}| = N(\mathfrak{M}) < \infty$ for every maximal ideal, then $\varphi(\mathfrak{M}^n) = N(\mathfrak{M})^n - N(\mathfrak{M})^{n-1}$.*

Proof. The ring $R/\mathfrak{M}^n$ contains a maximal ideal $\mathfrak{M}/\mathfrak{M}^n$ and every element of $\mathfrak{M}/\mathfrak{M}^n$ is nilpotent. Hence $R/\mathfrak{M}^n$ is a local ring by the lemma 2. This means that $U(R/\mathfrak{N}^n) = R/\mathfrak{M}^n \setminus \mathfrak{M}/\mathfrak{M}^n$. Transferring to powers we have $\varphi(\mathfrak{M}^n) = |R/\mathfrak{M}^n| - |\mathfrak{M}/\mathfrak{M}^n|$. From above $|R/\mathfrak{M}^n| = N(\mathfrak{M})^n$. We still have $|\mathfrak{M}/\mathfrak{M}^n| = N(\mathfrak{M})^{n-1}$ to prove.

The proof is by induction on n.

Case $n = 2$. $\mathfrak{M}/\mathfrak{M}^2 \cong R/\mathfrak{M}$ by [8, page 13,(5)].

Case $n + 1$: $\mathfrak{M}^{n+1} \subset \mathfrak{M}^n \subset \mathfrak{M}$ and as in lemma 1 we have: there exists homomorphism $g : \mathfrak{M}/\mathfrak{M}^{n+1} \to \mathfrak{M}/\mathfrak{M}^n$ and it is surjection with kernel $\mathfrak{M}^n/\mathfrak{M}^{n+1} \cong R/\mathfrak{M}$. Then we have $|\mathfrak{M}/\mathfrak{M}^{n+1}| = |\mathfrak{M}/\mathfrak{M}^n| \cdot |\mathfrak{M}^n/\mathfrak{M}^{n+1}| = N(\mathfrak{M})^n \cdot N(\mathfrak{M})$.

Theorem 2. (Generalized Euler's Theorem) *Let R be a ring with above conditions, $m \in R$, $\mathfrak{A} \subset R$ be an ideal. If $Rm + \mathfrak{A} = R$ then $m^{\varphi(\mathfrak{A})} \equiv 1 \pmod{\mathfrak{A}}$.*

Proof. By the condition $m + \mathfrak{A}$ is in $U(R/\mathfrak{A})$.

Special cases of generalized Euler's function can be found in [2] and [7].

3. THE MAIN RESULT

Let R be a Dedekind ring with next conditions:

1. For every maximal ideal $\mathfrak{M}$ quotient-ring $R/\mathfrak{M}$ is finite.

2. It is possible to find the set $W \subset R$ for some maximal ideals $\mathfrak{M}_1, \mathfrak{M}_2 \in R$ and $\mathfrak{A} = \mathfrak{M}_1 \cdot \mathfrak{M}_2$ such that:

2.1. Every coset $R/\mathfrak{A}$ intersects with W and this intersection contain only one element (i.e. W consists of different elements from co-sets $R/\mathfrak{A}$ that's why we have one-by-one correspondence between W and $R/\mathfrak{A}$).

2.2. It is possible to find some convenient for calculations one-by-one correspondence between W and $[0, T] = \{0, 1, 2, \ldots, T-1, T\}$ with sufficiently large natural number T.

Suppose Alice wishes to enable anyone to send her secret messages, which only she can decrypt. She first picks two maximal ideals $\mathfrak{M}_1 \neq \mathfrak{M}_2 \subset R$. Then Alice computes $\mathfrak{A} = \mathfrak{M}_1 \cdot \mathfrak{M}_2$. Alice also chooses an encrypting exponent e, which satisfies $gsd(E, \varphi(\mathfrak{A})) = 1$. Now Alice's public key is the pair $(\mathfrak{A}, e)$, which she can publish in a public directory. Then Alice compute the decryption exponent d such as $ed = 1 + \varphi(\mathfrak{A})t$. Alice keeps secret her private key, which is triple $(d, \mathfrak{M}_1, \mathfrak{M}_2)$.

Now suppose Bob wishes to encrypt a message to Alice. He first look up Alice's public key and represent the message as an element $m \in W$. The ciphertext c is then produsd by raising the message to the power of the public encryption exponent modulo the public modulus, i.e.

$$c = m^e \pmod{\mathfrak{A}} \in W.$$

Alice on receiving c can decrypt the ciphertext to recover the message by exponentiating by the private decryption exponent, i.e.

$$m = c^d \pmod{\mathfrak{A}} \in W.$$

Theorem 3. *$m^{ed} \equiv m \pmod{A}$ for all $m \in W$.*

Proof. Case $Rm + \mathfrak{A} = R$. We can use Theorem 2: $m^{\varphi(\mathfrak{A})} \equiv 1 \pmod{\mathfrak{A}}$. From here $m^{\varphi(\mathfrak{A})t} \equiv 1 \pmod{\mathfrak{A}}$ and $m^{ed} = m \cdot m^{\varphi(\mathfrak{A})t} \equiv m \pmod{\mathfrak{A}}$.

Case $Rm + \mathfrak{A} \neq R$, $m \neq 0$. Then the ideal $Rm + \mathfrak{A}$ contains $\mathfrak{A} = \mathfrak{M}_1\mathfrak{M}_2$ and therefore $\mathfrak{M}_1\mathfrak{M}_2 = (Rm + \mathfrak{A})\mathfrak{M}'$ for a some ideal $\mathfrak{M}'$. So we have $Rm + \mathfrak{A} = \mathfrak{M}_1$ or $Rm + \mathfrak{A} = \mathfrak{M}_2$. Let $Rm + \mathfrak{A} = \mathfrak{M}_1$.

From $Rm + \mathfrak{A} = \mathfrak{M}_1$ we get $m \in \mathfrak{M}_1$, hence $m^{ed} \equiv m \pmod{\mathfrak{M}_1}$.

Since $m \in W$, $m \neq 0$, $m \in \mathfrak{M}_1$, then $m \notin \mathfrak{M}_2$. From this we have $Rm + \mathfrak{M}_2 = R$, and by Theorem 2 we get $m^{\varphi(\mathfrak{M}_2)} \equiv 1 \pmod{\mathfrak{M}_2}$. Next we calculate

$$m^{\varphi(\mathfrak{M}_1)\varphi(\mathfrak{M}_2)} = m^{\varphi(\mathfrak{A})} \equiv 1 \pmod{\mathfrak{M}_2},$$
$$m \cdot m^{\varphi(\mathfrak{A})t} \equiv m \cdot 1 = m \pmod{\mathfrak{M}_2},$$
$$m^{1+\varphi(\mathfrak{A})t} = m^{ed} \equiv m \pmod{\mathfrak{M}_2}.$$

From $m^{ed} \equiv m \pmod{\mathfrak{M}_1}$ and $m^{ed} \equiv m \pmod{\mathfrak{M}_2}$ we get $m^{ed} \equiv m \pmod{\mathfrak{M}_1\mathfrak{M}_2}$ by Chinese Remainder Theorem for rings.

4. SOME KNOWN RESULTS AND FURTHER PERSPECTIVES

The RSA cryptosystem for $R \neq \mathbf{Z}$ was introduced earlier only for case $R = \mathbf{Z}[i]$. This was made in a series of papers: [3, 5] and so on. The authors of these papers have argued that cryptographic security for case $R = \mathbf{Z}[i]$ is greater than cryptographic security of usual RSA cryptosystem for $R = \mathbf{Z}$. At the same time the authors of paper [6] assert that this is not the case. We agree with the last authors. Moreover:

Theorem 4. *Let R be a quadratic ring of algebraic integers. Then cryptographic security of RSA for this R not exceed cryptographic security of usual RSA cryptosystem.*

Proof. As known from [9, § 4.5], for every ideal $I \subseteq R$, there exists $a, b, d \in \mathbf{Z}$ such that the following are true:

(a) $I = d(\mathbf{Z}a + \mathbf{Z}(-b + \delta))$, and

(b) $b^2 - tb + n \equiv 0 \pmod{a}$, or, equivalently, $a|N(-b+\delta)$.

Conversely, any $I \subseteq R$ satisfying (a) and (b) is an ideal.

Herewith the following proposition holds ([9, p. 84, proposition 4.9.10]): Let $I = \mathbf{Z}a + \mathbf{Z}(-b+\delta)$ be an ideal of R. Let $a = p_1^{e_1} \cdot \cdots \cdot p_r^{e_r}$ be the prime factorization of a in $\mathbf{Z}$. The factorization of I into prime ideals is given by

$$\mathfrak{A} = \prod_{i=1}^{r} (\mathbf{Z}p_i + \mathbf{Z}(-b+\delta))^{e_i}$$

Thus, the task to factorize the ideal is equivalent to the task of the natural numbers decomposition into the product of primes.

We may talk about the cryptographic security of the RSA for the Dedekind rings only when we define the form of ideals. In the previous theorem it was supposed that there exists a reasonably good way, which allows us to find a standard form for every ideal of R. So, if a question of finding a good algorithm, which will allow us to find a standard form of ideal in the quadratic ring can be successfully resolved, then the quadratic ring of algebraic integers (without $\mathbf{Z}$) will be unfit for being used as platform for the generalized RSA algorithm.

ACKNOWLEDGMENTS

This work was partially funded by the subsidy allocated to Kazan Federal University for the state assignment in the sphere of scientific activities (the registration number is 114 090 970 010).

REFERENCES

1. J. Buchmann, T. Takagi, and U. Vollmer, *High Primes and Misdemeanours: Lectures in Honour 60th Birthday of Hugh Cowie Williams*, A. J. Van Der Poorten, Andreas Stein, editors, Fields Institute Communications **41**, 111–122 (2004).
2. J. T. Cross, The American Mathematical Monthly **8** (90), 518-528 (1983).
3. A. N. El-Kassar, R. Haraty, and Y. A. Awad, *Proceedings of the ISCA 18th International Conference on Computer Applications in Industry and Engineering* (Honolulu, 2005), p. 298–303.
4. M. M. Gluhov, Mathematical Aspects of Cryptography **1** (1), 23–54 (2010).
5. R. A. Haraty, A. N. El-Kassar, and B. Shibaro, Journal of Mathematics and Statistics **1** (2), 354–359 (2006).
6. A. Koval and B.S. Verkhovsky, *5th International Conference on Information Technology: New Generations (ITNG-2008), Las Vegas, USA, 2008* (Las Vegas, 2008), pp. 101–105.
7. K. A. Rodosskii, *Euclidean Algorithm* (Nauka, Moscow, 1988) [in Russian].
8. H. P. F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory* (Cambridge Univ. Press, Cambridge, 2001).
9. M. Trifković, *Algebraic Theory of Quadratic Numbers* (Springer, New York, 2013).
10. S. N. Tronin and K. A. Petikhova, *International Conference "Algebra and Mathematical Logic: Theory and Applications", Kazan, Russia, 2014* (Kazan Univ., 2014), pp. 148–149.