Modified RSA in the Domains of Gaussian Integers and Polynomials Over Finite Fields.

Conference Paper · January 2005

Source: DBLP

4 authors, including:

Abdul-Nasser El-Kassar
Lebanese American University
72 PUBLICATIONS **799** CITATIONS

SEE PROFILE

Ramzi A. Haraty
Lebanese American University
158 PUBLICATIONS **716** CITATIONS

SEE PROFILE

Yahia Awad
12 PUBLICATIONS **44** CITATIONS

SEE PROFILE

MODIFIED RSA IN THE DOMAINS OF GAUSSIAN INTEGERS AND POLYNOMIALS OVER FINITE FIELDS

A. N. El-Kassar
Department of Mathematics
Beirut Arab University
P. O. Box 11-5020
Beirut, Lebanon
E-mail: ak1@bau.edu.lb

Ramzi Haraty
Division of Computer Science and Mathematics
Lebanese American University
P.O.Box 13-5053 Chouran
Beirut, Lebanon 1102 2801
E-mail : rharaty@lau.edu.lb

Y. A. Awad
Department of Mathematics
Lebanese International University
P. O. Box 5
Lebanon, West Bekaa
E-mail: yawad@liu.edu.lb

Abstract

The purpose of this paper is to extend the RSA public-key encryption scheme from its classical domain of natural integers **Z**, to two principal ideal domains, namely the domain of Gaussian integers, **Z**[*i*], and the domain of polynomials over finite fields, *F*[*x*]. The arithmetic needed for the modifications to these domains are described. The modified RSA algorithms are given. Proofs for the new method are provided. The computational procedures are described and illustrated in numerical examples. The advantages of new scheme over the classical are pointed out.

Keywords: RSA public-key cryptosystem, Gaussian integers, polynomials over finite fields

1 Introduction

The RSA public-key cryptosystem scheme [11], invented by Rivest, Shamir, and Adleman, is the most popular and widely used public-key cryptosystem. Its security is based on the intractability of both the integer factorization problem and the RSA problem. The RSA problem, see [9], is the problem of finding an integer m such that $m^e \equiv c \pmod{n}$, where n is a product of two distinct large odd primes p and q, e is a positive random integer such that $gcd(e,(p-1)(q-1)) = 1$, and c is any integer. That is, the RSA problem is that of finding e^{th} roots of an integer c modulo a composite integer n.

The classical RSA cryptosystem is described in the settings of the ring $\mathbf{Z}_n$, the ring of integers modulo a composite integer $n = pq$, where p and q are two distinct odd prime integers. Many aspects of arithmetic over the domain of integers can be carried out to the domain of Gaussian integers **Z**[*i*], the set of all complex numbers of the form $a + bi$, where a and b are integers, and to the domain of polynomials over finite fields *F*[*x*]. Recently, El-Kassar et al. [4] modified the ElGamal public-key encryption schemes from its classical settings of the domain of natural integers to the domain of Gaussian integers by extending the arithmetic needed for the modifications to the domains. A similar extension to the domain *F*[*x*] was given by El-Kassar and Haraty [5]. Haraty et al. [8] gave a comparative study of the extended ElGamal cryptographic algorithms.

In this paper, we present two extensions of the RSA cryptosystem in the domain of Gaussian and the domain of polynomials over finite fields by extending the computational procedures behind the RSA public-key cryptosystem using arithmetic modulo a Gaussian integer and arithmetic modulo a polynomial. First, we review the classical RSA public-key cryptosystem. Then, we modify the computational methods in the domain of Gaussian integers and the domain of polynomials over finite field. Finally, we show how the modified computational methods can be used to extend the RSA algorithm to these domains. Also, we show that the extended algorithms require a little additional computational effort than the classical one and accomplish much greater security.

2 Classical RSA Public-Key Cryptosystem

The RSA cryptosystem is described as follows: entity A generates the public-key by first generating two large random odd prime integers p and q, each roughly of the same size. Then, entity A computes the modulus $n = pq$ and $\phi(n) = (p - 1)(q - 1)$, where ϕ is Euler's phi-function. Next, entity A selects the encryption exponent e to be any random integer in the interval $(1, \phi(n))$, and which is relatively prime to $\phi(n)$. Using the extended Euclidean algorithm for integers, entity A finds the decryption exponent d, which is the unique inverse of e in $\mathbf{Z}_n$. The public-key is the pair (n, e) and A's private-key is the triplet (p, q, d).

To encrypt a message, entity B first represents the message as an integer m in $\mathbf{Z}_n$. Then, entity B obtains A's public-key (n, e) and use it to compute the cipher text $c \equiv m^e \pmod{n}$ and sends c it to entity A. Now, to decrypt c, entity A computes $m \equiv c^d \pmod{n}$ and recovers the original message m.

Example1. In order to generate the public-key, entity A selects the artificially small primes $p = 883$ and $q = 709$. Then A computes the modulus $n = 626047$ and $\phi(n) = 624456$. Next, A chooses encryption exponent $e = 333853$ and finds the decryption $d = 97213$ using the extended Euclidean algorithm for integers. Therefore, the public-key is (626047, 333853) and the private-key is (883, 709, 97213). Now, to encrypt the 10-bit message 1001110001, entity B represents the message in decimal notation as $m = 625$ in $\mathbf{Z}_n$, B computes

$$c \equiv 625^{333853} \pmod{626047} = 274608$$

and sends it to A. Finally, to decrypt c, A uses the decryption algorithm to get the original message

$$m \equiv 274608^{97213} \pmod{626047} = 625.$$

3 Arithmetic in Z[*i*]

The domain of Gaussian integers $\mathbf{Z}[i]$ is the subring of the field of complex numbers consisting of all elements of the form $a + bi$, where a and b are integers and $i = \sqrt{-1}$. For a Gaussian integer $\gamma = a + bi$, let $\delta(\gamma) = a^2 + b^2$ be the norm of γ. We say that a nonzero Gaussian integer β divides a Gaussian integer α if there $\gamma \in \mathbf{Z}[i]$ such that $\alpha = \gamma\beta$. If β divides α in $\mathbf{Z}[i]$ then $\delta(\beta)$ divides $\delta(\alpha)$ in $\mathbf{Z}$. A Gaussian integer β is said to be invertible, or a unit, if there is if there $\gamma \in \mathbf{Z}[i]$ such that $1 = \gamma\beta$; i.e., β divides 1. The units or invertible elements of $\mathbf{Z}[i]$ are 1, -1, i, and $-i$. Two elements α and β in $\mathbf{Z}[i]$ are called associates, denoted by $\alpha \sim \beta$, if one is a unit multiple of the other. For instance, the associates of $1+2i$ are $-1-2i$, $2-i$ and $-2+i$.

A nonzero nonunit Gaussian integer β is called prime provided that β divides γ or β divides α whenever β divides $\alpha\gamma$. It is well-known that β is a prime if and only if β has no proper divisors, that is, the only divisors of β are the units and the associates, see [6]. Also, if $\delta(\gamma)$ is prime in $\mathbf{Z}$ then γ must be a prime in $\mathbf{Z}[i]$. The Gaussian primes of $\mathbf{Z}[i]$, up to associates, see [8] or [10], are of the form:

i) $\alpha = 1 + i$;
ii) $\pi = a + bi$ and $\bar{\pi} = a - bi$, where $\pi\bar{\pi}$ is an odd prime integer q of the form $4k + 1$;
iii) p, where p is an odd prime integer of the form $4k + 3$.

Note that π and $\bar{\pi}$ in (ii) are not associates.

The domain of Gaussian integers is a factorization domain in which every nonzero nonunit element can be expressed as a product of primes. Moreover, this decomposition is unique up to the order and associates of the primes. For $\beta \in \mathbf{Z}[i]$, the ideal generated by β is $\langle\beta\rangle = \beta\mathbf{Z}[i] = \{\beta\gamma \mid \gamma \in \mathbf{Z}[i]\}$. The coset of a Gaussian integer α modulo $\langle\beta\rangle$, denoted by $\alpha+\langle\beta\rangle$ or $[\alpha]$, is the set $\alpha + \langle\beta\rangle = [\alpha] = \{\alpha + \gamma \mid \gamma \in \langle\beta\rangle\}$. Two cosets $\alpha+\langle\beta\rangle$ and $\gamma+\langle\beta\rangle$ are equal if and only if $\alpha-\gamma \in \langle\beta\rangle$; in this case both α and γ are representative of the same coset. The quotient ring of $\mathbf{Z}[i]$ modulo $\langle\beta\rangle$, denoted by $\mathbf{Z}[i]/\langle\beta\rangle$ or G_β, is the set of all cosets of $\langle\beta\rangle$. It is well-known that $\mathbf{Z}[i]/\langle\beta\rangle$ is a ring, see [7]. A complete residue system modulo β, denoted by $A(\beta)$, is any complete set of distinct representatives from $\mathbf{Z}[i]/\langle\beta\rangle$.

Two Gaussian integers α and β, are congruent modulo a nonzero Gaussian integer η, written as $\alpha \equiv \beta \pmod{\eta}$, if $\alpha-\beta$ divides η. The relation $\equiv$ modulo η is an equivalence relation. The congruence classes are the cosets of $\langle\beta\rangle$. We identify G_β with the complete residue system modulo β so that G_β is a ring under addition and multiplication modulo β. For example, when $\beta = 1 + 2i$, then

$$\mathbf{Z}[i]/\langle 1+2i\rangle = \{[0],[1],[2],[3],[4]\} = G_{1+2i}.$$

This ring is identified by $G_{1+2i} = \{0, 1, 2, 3, 4\}$.

We define the function $q(\beta)$ to be the order of the quotient ring $\mathbf{Z}[i]/\langle\beta\rangle$. Now, $q(\beta\gamma) = q(\beta)q(\gamma)$, see [2] or [3]. J.T. Cross [2] gave a full description for complete residue systems modulo prime powers of Gaussian integers. In particular, when p is a Gaussian prime of the form $4k+3$,

$$G_p = \{ a+bi \mid 0 \le a \le p-1,\ 0 \le b \le p-1\},$$

and when π is a factor the odd prime $q = \pi\bar{\pi}$ with q of the form $4k+1$,

$$G_\pi = \{ a \mid 0 \le a \le q-1\}.$$

For any two nonzero elements γ and β of $\mathbf{Z}[i]$, a complete set of residue system modulo $\gamma\beta$, see [3], is the set

$$A(\gamma\beta) = \{s + r\gamma : s \in A(\gamma), r \in A(\beta)\}.$$

A greatest common divisor of two Gaussian integers α and β is a divisor $\gamma = a + bi$ of both elements α and β and any other common divisor divides γ. Any two greatest common divisors α and β are associates so α and β have four greatest common divisors. The greatest common divisor α and β, denoted by $\gcd(\alpha, \beta)$, is the greatest common divisor $\gamma = a + bi$ with $a, b \ge 0$. The $\gcd(\alpha, \beta)$ can be written as

$$\gcd(\alpha, \beta) = \alpha\gamma + \beta\lambda,$$

where the unique coefficients γ and λ can be obtained by the extend Euclidean algorithm for Gaussian integers.

For a Gaussian integer β, let G_β^* be those elements of G_β that are relatively prime to β; i.e.,

$$G_\beta^* = \{\alpha \in G_\beta \mid \gcd(\alpha,\beta) = 1\}.$$

The set G_β^* is called a reduced residue system modulo β and is the group of units of G_β. When β is a Gaussian prime, G_β is a field and G_β^* is the set of nonzero elements in G_β. The number of elements in any reduced residue system G_β^*, denoted by $\phi(\beta)$, is Euler's phi function in $\mathbf{Z}[i]$, see [2] or [3]. The ϕ function is a multiplicative function; i.e., $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$. Also, for a prime power Gaussian integer, the value of the ϕ function is

$$\phi(\alpha^n) = 2^n - 2^{n-1},$$
$$\phi(\pi^n) = q^{n-1}(q-1),$$

or

$$\phi(p^n) = p^{2n-2}(p^2-1).$$

Thus, the value of ϕ for any Gaussian integer β can be obtained from the prime power decomposition of β.

4 Modified RSA In Z[*i*]

In the domain of Gaussian integers the RSA public-key scheme is described as follows. Entity A generates the public-key by first generating two large random Gaussian primes β and γ and computes $\eta = \beta\gamma$. If $\beta = \pi_1$ and $\gamma = \pi_2$, then the complete residue system modulo η has an order equal $q_1q_2 = (\pi_1\overline{\pi_1})(\pi_2\overline{\pi_2})$, see [3]. This choice yields a message space having an order same as that of the classical case; i.e,

$$|G_{\beta\gamma}| = |G_{\pi_1\pi_2}| = |\mathbf{Z}_{q_1q_2}| = q_1q_2.$$

Moreover, the order $G_{\beta\gamma}^*$ is

$$|G_{\beta\gamma}^*| = \phi(\eta) = \phi(\beta)\phi(\gamma)$$
$$= (q_1-1)(q_2-1) = |\mathbf{Z}_{q_1q_2}^*|.$$

Hence, the length of interval for the exponent e is $(\beta-1)(\gamma-1)$.

If $\beta = \pi_1 = a+bi$ and γ is an odd prime of the form $4k+3$, then the factorization problem of the composite Gaussian integer $\eta = \beta\gamma = a\gamma+b\gamma i$ is easy to solve. This choice is excluded.

If β and γ are both of the form $4k + 3$, then the complete residue system modulo $\eta = \beta\gamma$ is of the form

$$G_\eta = \{r+s\beta \mid r \in G_\beta \text{ and } s \in G_\gamma\}.$$

It can be shown that this set is precisely

$$G_\eta = \{a+bi \mid 0 \le a \le \beta\gamma - 1,\ 0 \le b \le \beta\gamma - 1\}.$$

Note that the order of G_η is $\beta^2\gamma^2$ and that of G_η^* is $\phi(\eta) = \phi(\beta)\phi(\gamma) = (\beta^2-1)(\gamma^2-1)$. In this case, the message space is enlarged so that its order is the square of that of the classical case; that is, $|G_{\beta\gamma}| = |\mathbf{Z}_{\beta\gamma}|^2$. Moreover, the length of interval for the exponent e is enlarged from $(\beta-1)(\gamma-1)$ to $(\beta^2-1)(\gamma^2-1)$.

Now, entity A selects a random integer e and determines its unique inverse $d \in G_\eta$, where $gcd(e,\phi(\eta)) = 1$ and $1 < e$, $d < \phi(\eta)$. This is done by applying the extended Euclidean algorithm and writing $gcd(e, \phi(\eta)) = 1$ as $ex + \phi(\eta)y$ so that $d \equiv x \pmod{\phi(\eta)}$. The public-key is (η, e) and the private-key is (β, γ, d).

To encrypt the message m chosen from G_η, entity B first uses the public-key to compute the cipher text $c \equiv m^e \pmod{\eta}$ and sends it to A.

To decrypt the sent cipher text c, entity A uses the private-key d to recover the original message by $m \equiv c^d \pmod{\eta}$. In the following theorem, we prove that the decryption scheme actually works.

Theorem 1. Let η be a Gaussian integer and let $m, a \in G_\eta$. Suppose that e is an integer, $1 < e < \phi(\eta)$, $\gcd(e, \phi(\eta))=1$, and d is the inverse of e modulo $\phi(\eta)$. If $c \equiv m^e \pmod{\eta}$ and $a \equiv c^d \pmod{\eta}$, then $a = m$.

Proof: Let η be a Gaussian integer and let $m \in G_\eta$. Suppose that e is an integer with $\gcd(e, \phi(\eta)) = 1$ and $1 < e < \phi(\eta)$. Let d be the inverse of e modulo $\phi(\eta)$ so that

$$ed \equiv 1 \pmod{\phi(\eta)},$$

and $1 < d < \phi(\eta)$. Since $ed \equiv 1 \pmod{\phi(\eta)}$ in G_η, there exists an integer k so that $ed = 1 + k\phi(\eta)$. Suppose that

$$c \equiv m^e \pmod{\eta}$$

and

$$a \equiv c^d \pmod{\eta}.$$

Now, we have two cases to discuss.

Case 1: Suppose that $gcd(m, \eta) = 1$. Then $m \in G_\eta^*$ and by applying Lagrange theorem for finite groups or by using an extension to Euler's theorem to the domain of Gaussian integers, see [1], we have

$$m^{\phi(\eta)} \equiv 1 \pmod{\eta}.$$

Then,

$$a \equiv c^d \equiv (m^e)^d$$
$$\equiv m^{1+k\phi(\eta)}$$
$$\equiv m.(m^{\phi(\beta)})^k \equiv m \pmod{\eta}.$$

Hence, $a \equiv m \pmod{\eta}$. Since both a and m belong to the same complete residue system modulo η and $a \equiv m \pmod{\eta}$, we conclude that $a = m$.

Case 2: Suppose that $gcd(m, \eta) \neq 1$, then $gcd(m, \eta) = \beta$, $gcd(m, \eta) = \gamma$, or $gcd(m, \eta) = \eta$. If $gcd(m, \eta) = \eta$, then $m \equiv 0 \pmod{\eta}$ so that $c = a = m = 0$.

Suppose that $gcd(m, \eta) = \beta$. Then, $m \equiv 0 \pmod{\beta}$. Any power of m keeps the congruence true. Thus,

$$m^{1+k\phi(\beta)} \equiv 0 \equiv m \pmod{\beta}.$$

Now, $gcd(m, \eta) = \beta$ implies that $gcd(m, \gamma) = 1$ and

$$m^{\phi(\gamma)} \equiv 1 \pmod{\gamma}$$

so that

$$m^{1+k\phi(\eta)} \equiv m^{1+k\phi(\gamma)\phi(\beta)}$$
$$\equiv m.(m^{\phi(\beta)})^{k\phi(\gamma)}$$
$$\equiv m \pmod{\gamma}.$$

Since $ed = 1 + k\phi(\eta)$, we have that

$$m \equiv m^{ed} \equiv (m^e)^d \pmod{\beta},$$

and

$$m \equiv m^{ed} \equiv (m^e)^d \pmod{\gamma}.$$

Hence,

$$c^d \equiv m \pmod{\beta},$$

and

$$c^d \equiv m \pmod{\gamma}.$$

Since both β and γ are two distinct Gaussian primes with $(\beta, \gamma) = 1$, then we have that

$$c^d \equiv m \pmod{\eta}.$$

Finally, since both a and m belong to the same complete residue system modulo the Gaussian integer η, we conclude that $a = m$.

The case when $gcd(m, \eta) = \eta$ is similar to that of $gcd(m, \eta) = \beta$. ■

In the following we provide the algorithms for the RSA crytosystem in $\mathbf{Z}[i]$.

Algorithm 1: (RSA Gaussian public-key generation).

1. Generate two distinct large random Gaussian primes β and γ.
2. Compute η and $\phi(\eta)$.
3. Select an integer e in the interval $[2, \phi(\eta)-1]$.
4. Use the extended Euclidean algorithm to determine its inverse d modulo $\phi(\eta)$.
5. The public-key is (η, e) and the private-key is (β,γ,d).

Algorithm 2: (RSA Gaussian public-key encryption)}

1. Obtain the authentic public-key.
2. Represent the message as an integer m in $\boldsymbol{G}_\eta$.
3. Compute $c \equiv m^e \pmod{\eta}$ and send it to A.

Algorithm 3: (RSA Gaussian public-key decryption)}

1. Use the private-key d to recover $m \equiv c^d \pmod{\eta}$.

Example 2. Let $\beta = 27743$ and $\gamma = 23291$ be two Gaussian primes of the form $4k + 3$. Compute the product

$$\eta = \beta\gamma = 646162213$$

and

$$\phi(\eta) = 417525604196912640.$$

Note that, had we used the classical RSA, $n = 646162213$ and $\phi(n) = 646111180$. Now, Entity A chooses the integer

$$e = 16471875800465191,$$

and uses the extended Euclidean algorithm for integers to find

$$d = 200851669617899671$$

such that $ed = 1$ in G_η. Hence, A's public-key is the pair (646162213, 16471875800465191), and A's s private-key is the triplet (27743,23291, 200851669617899671).

Suppose that entity B wants to encrypt the message 1001110001. This representation can be regarded as a base $1+i$ representation the Gaussian integer. This message can be converted to $m = 9 + 4\ i$. Entity B computes the Gaussian integer m^e in G_η to get

$$m^e = (9 + 4\ i)^{16471875800465191} \equiv 636415678 + 168717186\ i \pmod{\eta}.$$

Hence, Entity B sends the ciphertext

$$c = 495038485 + 372009420\ i$$

in G_η entity A.

To decrypt the cipher text c, entity A computes

$$c^d = (495038485 + 372009420\ i)^d \equiv 4 + 9\ i \pmod{\eta}$$

and gets the original message m.

5 RSA Polynomials Cryptosystem

Given a prime number p and a polynomial $f(x)$ of degree n in the finite field $\mathbf{Z}_p[x]$ as a product of two distinct irreducible polynomials in $\mathbf{Z}_p[x]$, that is $f(x) = h(x)g(x)$, where $h(x)$ is of degree s and $g(x)$ is of degree r. The quotient ring of $\mathbf{Z}_p[x]$ modulo the ideal generated by $f(x)$, denoted by $\mathbf{Z}_p[x]/\langle f(x)\rangle$, consists of congruence classes of polynomials of degree less than that of $f(x)$. The ring $\mathbf{Z}_p[x]/\langle f(x)\rangle$ is finite of order p^n isomorphic to the direct sum of $\mathbf{Z}_p[x]/\langle h(x)\rangle$ and $\mathbf{Z}_p[x]/\langle g(x)\rangle$; that is,

$$\mathbf{Z}_p[x]/\langle f(x)\rangle \cong \mathbf{Z}_p[x]/\langle h(x)\rangle \oplus \mathbf{Z}_p[x]/\langle g(x)\rangle.$$

Hence, the group unit $U(\mathbf{Z}_p[x]/\langle f(x)\rangle)$ is isomorphic to the direct product of $U(\mathbf{Z}_p[x]/\langle h(x)\rangle)$ and $U(\mathbf{Z}_p[x]/\langle g(x)\rangle)$; that is,

$$U(\mathbf{Z}_p[x]/\langle f(x)\rangle) \cong U(\mathbf{Z}_p[x]/\langle h(x)\rangle) \times U(\mathbf{Z}_p[x]/\langle g(x)\rangle).$$

Since $h(x)$ and $g(x)$ are irreducible, the quotient rings $\mathbf{Z}_p[x]/(\langle h(x)\rangle)$ and $\mathbf{Z}_p[x]/\langle g(x)\rangle$ are finite fields of order p^s and p^r , respectively. Also, the groups of units $U(\mathbf{Z}_p[x]/\langle h(x)\rangle)$ and $U(\mathbf{Z}_p[x]/\langle g(x)\rangle)$ are cyclic and of order $\phi(h(x)) = p^s - 1$ and $\phi(g(x)) = p^r - 1$, respectively.

Now, given a positive integer e such that $(e, \phi(f(x))) = 1$ and a polynomial $m(x)$, find a polynomial $c(x)$ such that $c(x) \equiv m(x)^e \pmod{f(x)}$ in $\mathbf{Z}_p[x]$. The polynomials $h(x)$ and $g(x)$ should be selected so that factoring $f(x) = h(x)g(x)$ is computationally infeasible.

In the following we present three algorithms for the RSA public-key encryption scheme over polynomials. To create an RSA public-key and a corresponding private-key, Entity A should do the following:

Algorithm 4: (RSA polynomials key generation).

1. Generate a random odd prime integer p.
2. Generate two irreducible polynomial $h(x)$ and $g(x)$ in $\mathbf{Z}_p[x]$.
3. Reduce the polynomial $f(x) = h(x)g(x)$ in $\mathbf{Z}_p[x]$.
4. Compute $\phi(f(x)) = (p^s - 1)(p^r - 1)$ the order of $U(\mathbf{Z}_p[x]/\langle f(x)\rangle)$.
5. Select an integer e in the interval $[2, \phi(f(x))-1]$ such that $(e, \phi(f(x))) = 1$.
6. Use the extended Euclidean algorithm to determine its inverse d modulo $\phi(f(x))$.
7. A's public-key is $(p, f(x), e)$, A's private-key is $(p, d, g(x), h(x))$.

The following algorithm shows how entity B encrypts a message $m(x)$ for A. Entity B should do the following:

Algorithm 5: (RSA polynomials encryption)

1. Receive A's authentic public-key $(p, f(x), e)$.
2. Represent the message as a polynomial $m(x)$ in the complete residue system modulo $f(x)$ in $\mathbf{Z}_p[x]$.
3. Compute the polynomial $c(x) \equiv m(x)^e \pmod{f(x)}$ in $\mathbf{Z}_p[x]$.
4. Send the ciphertext $c(x)$ to A.

The following algorithm shows how entity A decrypts the sent ciphertext $c(x)$ and recovers the real message $m(x)$. Entity A should do the following:

Algorithm 5: (RSA polynomials decryption)

1. Receive the ciphertext $c(x)$ from B.
2. Use the private-key d to recover $m(x)$ by reducing $c(x)^d \pmod{f(x)}$ in $\mathbf{Z}_p[x]$.

Let $a(x)$ be a polynomial in the complete residue system modulo $f(x)$ in $\mathbf{Z}_p[x]$. If $a(x) \equiv c(x)^d \pmod{f(x)}$, then $a(x) = m(x)$.

In the following theorem, we prove that the decryption scheme actually works.

Theorem 2. Let $a(x)$ be a polynomial in the complete residue system modulo $f(x)$ in $\mathbf{Z}_p[x]$. If $a(x) \equiv c(x)^d \pmod{f(x)}$, then $a(x) = m(x)$.

Proof: Let $a(x)$ be a polynomial in the complete residue system modulo $f(x)$ in $\mathbf{Z}_p[x]$ such that $a(x) \equiv c(x)^d \pmod{f(x)}$. Since $e.d \equiv 1 \pmod{\phi(f(x))}$, then there exists an integer k such that $e.d = 1 + k\phi(f(x))$. Suppose that $\gcd(m(x), f(x)) = 1$. Then

$$\begin{aligned} a(x) &\equiv c(x)^d \pmod{f(x)} \\ &\equiv (m(x)^e)^d \pmod{f(x)} \\ &\equiv m(x)^{ed} \pmod{f(x)} \\ &\equiv m(x)^{1+k\phi(f(x))} \pmod{f(x)} \\ &\equiv m(x).m(x)^{k\phi(f(x))} \pmod{f(x)} \end{aligned}$$

Since $\gcd(m(x), f(x)) = 1$, Euler's theorem gives that

$$m(x)^{\phi(f(x))} \equiv 1 \pmod{f(x)}$$

and

$$a(x) \equiv m(x) \pmod{f(x)}.$$

Now suppose that $\gcd(m(x), f(x)) \neq 1$. Then, either $\gcd(m(x), f(x)) = f(x)$, $\gcd(m(x), f(x)) = g(x)$ or $\gcd(m(x), f(x)) = h(x)$. If $\gcd(m(x), f(x)) = f(x)$, then

$$\begin{aligned} m(x) \equiv 0 &\equiv m(x)^{ed} \pmod{f(x)} \\ &\equiv c(x)^d \equiv a(x) \pmod{f(x)}. \end{aligned}$$

If $\gcd(m(x), f(x)) = g(x)$, then $g(x)$ divides $m(x)$ and

$$\begin{aligned} m(x) \equiv 0 &\equiv m(x)^{ed} \pmod{g(x)} \\ &\equiv c(x)^d \equiv a(x) \pmod{g(x)}. \end{aligned}$$

Since $\gcd(m(x), f(x)) = g(x)$ and $\gcd(m(x), f(x)) \neq f(x)$, we have $\gcd(m(x), h(x)) = 1$. Now

$$\begin{aligned} e.d &= 1 + k\phi(f(x)) = 1 + k(p^s - 1)(p^r - 1) \\ &= 1 + k'(p^r - 1) = 1 + k'\phi(h(x)). \end{aligned}$$

Hence,

$$\begin{aligned} a(x) &\equiv c(x)^d \pmod{h(x)} \\ &\equiv m(x)^{ed} \pmod{h(x)} \\ &\equiv m(x)^{1+k'\phi(h(x))} \pmod{h(x)} \\ &\equiv m(x).m(x)^{k'\phi(h(x))} \pmod{h(x)} \end{aligned}$$

Since $\gcd(m(x), h(x)) = 1$, Euler's theorem gives that

$$m(x)^{\phi(h(x))} \equiv 1 \pmod{h(x)}$$

and

$$a(x) \equiv m(x) \pmod{h(x)}.$$

Since $h(x)$ and $g(x)$ are two distinct irreducible polynomials belonging to the ring $\mathbf{Z}_p[x]$, which is a principle ideal domain, it follows that $h(x)$ and $g(x)$ are prime polynomials. Therefore,

$a(x) \equiv m(x) \pmod{g(x)}$ and $a(x) \equiv m(x) \pmod{h(x)}$

implies that $a(x) \equiv m(x) \pmod{f(x)}$. A similar argument shows that $a(x) \equiv m(x) \pmod{f(x)}$ when $\gcd(m(x), f(x)) = g(x)$. Hence, the last congruence is always true. Finally, since $m(x)$ and $a(x)$ belong to the same complete residue system modulo $f(x)$ in $\mathbf{Z}_p[x]$, we have that $a(x) = m(x)$. ■

Next we present an example illustrating the RSA scheme over polynomials.

Example 3. (RSA polynomials encryption with small parameters)

Let $p = 101$. Entity A chooses the two irreducible polynomials $h(x) = 18x^2 + 71x + 88$ and $g(x) = 28x^3 + 83x^2 + 3x + 95$ in $\mathbf{Z}_{101}[x]$. Reducing the polynomial $f(x) = h(x)g(x)$ in $\mathbf{Z}_{101}[x]$, we get $f(x) = 100x^5 + 48x^4 + 28x^3 + 36x^2 + 40x + 78$. Compute $\phi(f(x)) = (101^3 - 1)(101^2 - 1) = 10509060000$. Then, entity A chooses the integer $e = 2580882461$ such that $(e, \phi(f(x))) = 1$ and $1 < e < \phi(f(x))$. Using the extended Euclidean algorithm for integers to find $d = 4894193141$ such that $ed \equiv 1 \pmod{\phi(f(x))}$ in $\mathbf{Z}_{101}[x]$. Hence, A's public-key is

$(p = 101, f(x) = 100x^5 + 48x^4 + 28x^3 + 36x^2 + 40x + 78,$
$e = 2580882461)$

and A's private-key is

$(p = 101, d = 4894193141, g(x) = 28x^3 + 83x^2 + 3x + 95,$
$h(x) = 18x^2 + 71x + 88).$

To encrypt the message $m(x) = 1 + x + 3x^2$, entity B reduces the polynomial

$$\begin{aligned} c(x) = m(x)^e &= (1 + x + 3x^2)^{2580882461} \\ &\equiv 8x^4 + 98x^3 + 39x^2 + 90x + 40 \pmod{f(x)} \end{aligned}$$

in $\mathbf{Z}_{101}[x]$ and sends it to entity A.

To decrypt the ciphertext $c(x) = 8x^4 + 98x^3 + 39x^2 + 90x + 40$, A reduces

$$a(x) = c(x)^d = (8x^4 + 98x^3 + 39x^2 + 90x + 40)^{4894193141} \equiv 1 + x + 3x^2 \pmod{f(x)}$$

in $\mathbf{Z}_{101}[x]$ to recover the original message $m(x)$.

5 Conclusion

Arithmetic needed for the RSA cryptosystem in the domains of Gaussian integers and polynomials over finite fields were modified and computational procedures were described. There are advantages for the new schemes over the classical one. First, generating the odd prime numbers in both the classical and the modified methods requires the same amount of efforts. Second, the modified method provides an extension to the range of chosen messages and the trials will be more complicated. This is due to the fact that the complete residue system $\mathbf{Z}_n$ has pq elements, while the complete residue system G_η has $\delta(\eta) = p^2q^2$ elements and the complete residue system $\mathbf{Z}_p[x]/\langle f(x)\rangle$ has $p^s p^r$ elements. Third, in $\mathbf{Z}_{n,}$, Euler phi function is $\phi(n) = (p - 1)(q - 1)$, in $\mathbf{Z}[i]$ is $\phi(\eta) = (p^2 - 1)(q^2 - 1)$, and in $\mathbf{Z}_p[x]/\langle f(x)\rangle$ is $\phi(f(x)) = (p^s - 1)(p^r - 1)$ so that an attempt to find the private key d from the public key (RSA problem) is more complicated. Finally, we note that the computations involved in the modified methods do not require computational procedures that are different from those used in the classical method.

5 REFERENCES

[1] Y. A. Awad, " MSc Thesis ", Beirut Arab University, 2002.

[2] J. T. Cross, "The Euler's ϕ-function in the Gaussian integers", Amer. Math. Monthly vol. 90, pp. 518-528, 1983.

[3] A. N. El-Kassar, "Doctorate Dissertation", University of Southwestern Louisiana, 1991.

[4] A. N. El-Kassar, Mohamed Rizk, N. M. Mirza, Y. A. Awad, “El-Gamal public key cryptosystem in the domain of Gaussian integers”, Int. J. Appl. Math., vol. 7 no. 4, pp. 405-412, 2001.

[5] A. N. El-Kassar, Ramzi A. Haraty, “ElGamal Public-Key Cryptosystem Using Reducible Polynomials Over a Finite Field”, IASSE 2004, pp. 189-194, 2004.

[6] A. R. Kenneth, "Elementary number theory and its applications", AT&T Bell Laboratories in Murray Hill, New Jersey, 1988.

[7] J. A. Gallian, "Contemporary abstract algebra", 4th edition, Houghton Mifflin Company, Boston, 1998.

[8] Ramzi A. Haraty, Hadi Otrok, A. N. El-Kassar, “A Comparative Study of ElGamal Based Cryptographic Algorithms”, ICEIS vol. 3 , pp. 79-84, 2004.

[9] A. J. Menezes, P. C. Van Orshot, S. A. Vanstone, "Handbook of Applied Cryptography", CRC press, 1997.

[10] I. Niven, H. S. Zukerman, and H. L. Montegomery, "An introduction to the theory of numbers", 5th ed., John Wiley, New York, 1991.

[11] R. Rivest, A. Shamir, L. Aldeman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM 21, 2, pp. 120-126, 1978.