

# MODIFIED RSA IN THE DOMAIN OF GAUSSIAN INTEGERS

**A. N. El-Kassar**  
Department of  
Mathematics  
Beirut Arab  
University  
P. O. Box 11-5020  
Beirut, Lebanon  
E-mail: [ak1@bau.edu.lb](mailto: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](mailto: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](mailto: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 to the domain of Gaussian integers. Arithmetic needed for this modification is presented. 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

## 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  $e^{\text{th}}$  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 arithmetics over the domain of integers can be carried out to the domain of Gaussian integers  $\mathbf{Z}[i]$ , 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 an extension of the RSA cryptosystem in the domain of Gaussian by extending the computational procedures behind the RSA public-key cryptosystem using arithmetics modulo a Gaussian integer. First, we review the classical RSA public-key cryptosystem. Then, we modify the computational methods in the domain of Gaussian integers. Finally, we show how the modified computational methods can be used to extend the RSA algorithm to the domain  $\mathbf{Z}[i]$ . Also, we show that the extended algorithm requires a little additional computational effort than the classical one and accomplishes 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  $\phi$  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  $c$  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 the encryption exponent  $e = 333853$  and finds the decryption exponent  $d = 97213$  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 10011110001, entity  $B$  represents the message in decimal notation as  $m = 625$  in  $\mathbf{Z}_n$ , 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 $\mathbf{Z}[i]$

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  $\gamma$ . We say that a nonzero Gaussian integer  $\beta$  divides a Gaussian integer  $\alpha$  if there  $\gamma \in \mathbf{Z}[i]$  such that  $\alpha = \gamma\beta$ . If  $\beta$  divides  $\alpha$  in  $\mathbf{Z}[i]$  then  $\delta(\beta)$  divides  $\delta(\alpha)$  in  $\mathbf{Z}$ . A Gaussian integer  $\beta$  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.,  $\beta$  divides 1. The units or invertible elements of  $\mathbf{Z}[i]$  are 1,  $-1$ ,  $i$ , and  $-i$ . Two elements  $\alpha$  and  $\beta$  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  $\beta$  is called prime provided that  $\beta$  divides  $\gamma$  or  $\beta$  divides  $\alpha$  whenever  $\beta$  divides  $\alpha\gamma$ . It is well-known that  $\beta$  is a prime if and only if  $\beta$  has no proper divisors, that is, the only divisors of  $\beta$  are the units and the associates, see [6]. Also, if  $\delta(\gamma)$  is prime in  $\mathbf{Z}$  then  $\gamma$  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  $\pi$  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  $\pi$  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  $\beta$  is  $\langle \beta \rangle = \beta\mathbf{Z}[i] = \{\beta\gamma \mid \gamma \in \mathbf{Z}[i]\}$ . The coset of a Gaussian integer  $\alpha$  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  $\alpha$  and  $\gamma$  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  $G_\beta$ , 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  $\beta$ , denoted by  $A(\beta)$ , is any complete set of distinct representatives from  $\mathbf{Z}[i] / \langle \beta \rangle$ .

Two Gaussian integers  $\alpha$  and  $\beta$ , are congruent modulo a nonzero Gaussian integer  $\eta$ , written as  $\alpha \equiv \beta \pmod{\eta}$ , if  $\alpha - \beta$  divides  $\eta$ . The relation  $\equiv$  modulo  $\eta$  is an equivalence relation. The congruence classes are the cosets of  $\langle \beta \rangle$ . We identify  $G_\beta$  with the complete residue system modulo  $\beta$  so that  $G_\beta$  is a ring under addition and multiplication modulo  $\beta$ . 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  $4k+3$ ,

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

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

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

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

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

A greatest common divisor of two Gaussian integers  $\alpha$  and  $\beta$  is a divisor  $\gamma = a + bi$  of both elements  $\alpha$  and  $\beta$  and any other common divisor divides  $\gamma$ . Any two greatest common divisors  $\alpha$  and  $\beta$  are associates so  $\alpha$  and  $\beta$  have 4 greatest common divisors. The greatest common divisor  $\alpha$  and  $\beta$ , denoted by  $\gcd(\alpha, \beta)$ , is the greatest common divisor  $\gamma = a + bi$  with  $a, b \geq 0$ . The  $\gcd(\alpha, \beta)$  can be written as

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

where the unique coefficients  $\gamma$  and  $\lambda$  can be obtained by the extend Euclidean algorithm for Gaussian integers.

For a Gaussian integer  $\beta$ , let  $G_\beta^*$  be those elements of  $G_\beta$  that are relatively prime to  $\beta$ ; i.e.,

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

The set  $G_\beta^*$  is called a reduced residue system modulo  $\beta$  and is the group of units of  $G_\beta$ . When  $\beta$  is a Gaussian prime,  $G_\beta$  is a field and  $G_\beta^*$  is the set of nonzero elements in  $G_\beta$ . The number of elements in any reduced residue system  $G_\beta^*$ , denoted by  $\phi(\beta)$ , is Euler's phi

function in  $\mathbf{Z}[i]$ , see [2] or [3]. The  $\phi$  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  $\phi$  function is

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

or

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

Thus, the value of  $\phi$  for any Gaussian integer  $\beta$  can be obtained from the prime power decomposition of  $\beta$ .

#### 4 Modified RSA In $\mathbf{Z}[i]$

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  $\beta$  and  $\gamma$  and computes  $\eta = \beta\gamma$ . If  $\beta = \pi_1$  and  $\gamma = \pi_2$ , then the complete residue system modulo  $\eta$  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 the order as the one 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

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

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

If  $\beta = \pi_1 = a+bi$  and  $\gamma$  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  $\beta$  and  $\gamma$  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

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

Note that the order of  $G_\eta$  is  $\beta^2\gamma^2$  and that of  $G_\eta^*$  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  $(\eta, e)$  and the private-key is  $(\beta, \gamma, d)$ .

To encrypt the message  $m$  chosen from  $G_\eta$ , 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.** Let  $\eta$  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  $\eta$  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  $G_\eta$ , 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,

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

Hence,  $a \equiv m \pmod{\eta}$ . Since both  $a$  and  $m$  belong to the same complete residue system modulo  $\eta$  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 equality 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

$$\begin{aligned}m^{1+k\phi(\eta)} &\equiv m^{1+k\phi(\gamma)\phi(\beta)} \\ &\equiv m \cdot (m^{\phi(\beta)})^{k\phi(\gamma)} \\ &\equiv m \pmod{\gamma}.\end{aligned}$$

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  $\beta$  and  $\gamma$  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  $\eta$ , 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 cryptosystem in  $\mathbf{Z}[i]$ .

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

1. Generate two distinct large random Gaussian primes  $\beta$  and  $\gamma$ .
2. Compute  $\eta$  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  $(\eta, e)$  and the private-key is  $(\beta, \gamma, d)$ .

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

1. Obtain the authentic public-key.
2. Represent the message as an integer  $m$  in  $G_\eta$ .
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

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

Had the classical RSA been used,  $n = 646162213$  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  $G_\eta$ . Hence,  $A$ 's public-key is the pair  $(646162213, 16471875800465191)$ , and  $A$ 's private-key is the triplet  $(27743, 23291, 200851669617899671)$ .

Suppose that entity  $B$  wants to encrypt the message 10011110001. This representation can be regarded as a representation base the Gaussian prime  $1+i$ . This message can be converted to  $m = 9 + 4i$ . Entity  $B$  computes the Gaussian integer  $m^e$  in  $G_\eta$  to get

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

Hence, Entity  $B$  sends the ciphertext

$$c = 495038485 + 372009420i$$

in  $G_\eta$  entity  $A$ .

To decrypt the cipher text  $c$ , entity  $A$  computes

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

and gets the original message  $m$ .

## 5 Conclusion

Arithmetic needed for the RSA cryptosystem in the domain of Gaussian integers were modified and computational procedures were described. We pointed out some of the advantages for the new scheme over the classical one. For instance, generating the odd prime numbers  $\beta$  and  $\gamma$ , Gaussian primes of the form  $p = 4k+3$ , in both the classical and the modified methods requires the same amount of efforts. Also, 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  $\beta\gamma$  elements, while the complete residue system  $G_\eta$  has  $\beta^2\gamma^2$ . In  $\mathbf{Z}_n$ , Euler phi function is  $\phi(n) = (\beta - 1)(\gamma - 1)$ , and in  $\mathbf{Z}[i]$  is  $\phi(\eta) = (\beta^2 - 1)(\gamma^2 - 1)$  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 method 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  $\phi$ -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", 4<sup>th</sup> 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 Oorshot, S. A. Vanstone, "Handbook of Applied Cryptography", CRC press, 1997.
- [10] I. Niven, H. S. Zukerman, and H. L. Montgomery, "An introduction to the theory of numbers", 5<sup>th</sup> 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.