
# The Applications of Fusion Neutrosophic Number Theory in Public Key Cryptography and the Improvement of RSA Algorithm

**Mehmet Merkepci[1], Mohammad Abobala[2], Ali Allouf[3]**

[1.] Department of Mathematics, Gaziantep University, Gaziantep, Turkey

[2.]-Tishreen University, Department of Mathematics, Latakia, Syria

[3.]-Tishreen University, Faculty Of computer engineering and automation, Latakia, Syria

Emails: mehmet.merkepci@gmail.com; Mohammadabobala777@gmail.com; Ali.allouf@gmail.com

**Abstract**

The objective of this paper is to build the neutrosophic version of the RSA crypto-algorithm, where we use the foundations of fusion neutrosophic number theory such as neutrosophic phi-Euler's function, neutrosophic congruencies, and neutrosophic inverses to build novel algorithms for cryptography depending of famous RSA algorithm.

**Keywords:** Neutrosophic Cryptography; Neutrosophic RSA Algorithm; Public key Cryptography; Fusion Neutrosophic Number Theory

## 1. Introduction.

Neutrosophic algebraic began with Kandasamy and Samarandache [4], by defining neutrosophic algebraic structures such as neutrosophic groups and rings [5,7]. The inserting of an algebraic symbol refers to indeterminacy with the logical property $\boldsymbol{I^2 = I}$ has led to many great advantages in the study of algebraic structures, see [1-3,6,8-12].

The neutrosophic number theory was born in 2020, where the concepts of fusion neutrosophic gcd, neutrosophic Diophantine equations, neutrosophic Euler's function, and neutrosophic congruencies were defined and handled by many authors, see [3,11].

Cryptography is drawing a line between fusion theory and computer science, where the RSA algorithm reflects the applications of classical number theory in coding texts. From this point of view, we are motivated to apply the foundations of neutrosophic number theory to the RSA algorithm to build a cryptosystem with more complexity depending on neutrosophic integers.

In [14], Merkepci et.al suggested for the first time the idea of using neutrosophic numbers in cryptography.

Firstly, we recall some basic concepts.

Doi: https://doi.org/10.54216/FPA.100206
Received: November 22, 2022 Accepted: March 04, 2023

**Definition. [3]**

Let $Z$ be the ring of integers, we say that $Z(I) = \{a + bI;\ a\ b \in Z\}$is the neutrosophic ring of integers.

**Definition. [3]**

a). let $a + bI, and\ c + dI$ are two neutrosophic integers, then:
$a + bI \leq c + dI$ if and only if $a \leq c\ , a + b \leq c + d$.
b). $a + bI$ is called positive neutrosophic integer if $a > 0$ and $a + b > 0$.
**Example.**
$3 + 2I$ is a positive neutrosophic integer, that is because $3 > 0$, $3 + 2 = 5 > 0$.
**Definition. [10] (RSA algorithm)**
Let $a + bI, c + dI$ be two neutrosophic positive integers, if $gcd(a + bI, c + dI) = 1$, then:
$(a + bI)^{\varphi(c+dI)} = 1(mod\ c + dI)$.
The previous theorem is called neutrosophic Euler's identity.
**Theorem.**
The encrypt the text $(m)$, follow these steps:

1. Pick two positive integers $p, and\ q$ and compute $n = pq$.
2. Compute $\varphi(n)$.
3. Pick a positive integer $1 < e < \varphi(n)$ such that $gcd\big(e, \varphi(n)\big) = 1$.
4. Use the formula $c \equiv m^e\ (modn)$ to get the encryption of $(m)$.
5. To decrypt the original text $(m)$, find $e^{-1}$ such that $e.e^{-1} \equiv 1(\ mod\ \varphi(n))$.
6. Then compute $m \equiv c^{e^{-1}}\ (mod\ n)$, to get the original text.

**Remark.**
The pair $(e, n)$ is called the public key and it can be known to anybody, but $(e^{-1}, n)$ is called the secret key which is not published to the public.
**Remark.**
The complexity of the RSA algorithm comes from the problem of splitting a natural number $n$ into its prime factors, so that, if we chose a large number $n$, then breaking the code may be very hard.
**Example.**
Consider that $m = 3$ is the plain text, pick $p = 3, q = 5$, ten $n = pq = 15$, $\varphi(n) = 8$.
We pick $e = 3$, $e^{-1} = 3(mod 8)$.
$c \equiv m^e = 3^3 = 12(mod\ 15)$, which is the encrypted text.
To decrypt the previous message, then:
$m \equiv c^{e^{-1}} = 12^3 1728\ (mod\ 15) \equiv 3(mod\ 15)$, so that $m = 3$ which is the original text.

**Main discussion.**

**Why neutrosophic integers?**
The goal of cryptography is to keep the message secret, RSA depends on the problem of writing $n = pq$ which is complex for large numbers.
The neutrosophic integer ring $Z(I)$ helps with increasing the complexity, that is because splitting a neutrosophic positive integer is a harder problem.
For example, $n = 20 + 52I$ can be split into many different formulas such as:
$(4 + 2I)(5 + 7I), (4 - I)(5 + 9I), (2 + I)(18 + 14I)$ and so on:
This means that if we built a neutrosophic version of RSA, we get more complexity and we make it harder to break the code.
For this goal, we define a new version of the neutrosophic phi-Euler's function.
In [3], the neutrosophic phi-Euler's function is defined as follows:
$\varphi(x + yI) = \varphi(x).\varphi(x + y); x, x + y > 0$.
The function $\varphi$ measures the number of neutrosophic positive integers $a + bI$ such that $a + bI \leq x + yI$ and $gcd(a + bI, x + yI) = 1$.
In the following, we define the special neutrosophic phi-Euler's function.
**Definition.**
Let $x + yI$ be a positive neutrosophic integer, we define the special neutrosophic phi-Euler's function as follows:
$\varphi_s: Z(I) \to Z(I)\ ;\ \varphi_s(x + yI) = \varphi(x) + [\varphi(x + y) - \varphi(x)]I$ .
**Theorem.**
Let $A = a + bI, and\ M = m + nI$ be two positive neutrosophic integers with $gcd(A, M) = 1$, then $A^{\varphi_s(M)} = 1\ (mod\ M)$.

Doi: https://doi.org/10.54216/FPA.100206
Received: November 22, 2022 Accepted: March 04, 2023

**Proof.**
$A^{\varphi_s(M)} = (a+bI)^{\varphi(m)+[\varphi(m+n)-\varphi(m)]I} = (a)^{\varphi(m)} + I\left[(a+b)^{\varphi((m+n))} - (a)^{\varphi(m)}\right]$.
According to the assumption, we have $gcd(A,M) = 1$, so that $gcd(a,m) = gcd(a+b, m+n) = 1$, thus $(a)^{\varphi(m)} = 1\ (mod m)$, $(a+b)^{\varphi((m+n))} = 1\ (mod m+n)$, this implies that:
$A^{\varphi_s(M)} = 1\ (mod m) + I[1\ (mod m+n) - 1\ (mod m)] = 1\ (mod\ M)$.
**Remark.**
Let $x+yI, z+tI$ be two positive neutrosophic integers with $gcd(x+yI, z+tI) = 1$, then:
$\varphi_s[(x+yI)(z+tI)] = \varphi_s(x+yI).\varphi_s(z+tI)$.
**Proof.**
$(x+yI)(z+tI) = xz + I[(x+y)(z+t) - xz]$.
$\varphi_s[(x+yI)(z+tI)] = \varphi(xz) + I[\varphi[(x+y)(z+t)] - \varphi(xz)]$
$= \left[\varphi(x) + I[\varphi(x+y) - \varphi(x)]\right]\left[\varphi(z) + I[\varphi(z+t) - \varphi(z)]\right] = \varphi_s(x+yI).\varphi_s(z+tI)$.
**Example.**
Consider $A = 3+2I, B = 5+6I$, $3 < 5$ , $5 < 11$, and $gcd(3,5) = gcd(5,11) = 1$, thus $gcd(A,B) = 1$.
$\varphi_s(A) = \varphi(3) + [\varphi(5) - \varphi(3)]I = 2 + (4-2)I = 2 + 2I$.
$\varphi_s(B) = \varphi(5) + [\varphi(11) - \varphi(5)]I = 4 + (10-4)I = 4 + 6I$.
$A.B = 15 + 18I + 10I + 12I^2 = 15 + 40I$.
$\varphi_s(A.B) = \varphi(15) + [\varphi(55) - \varphi(15)]I = 8 + (40-8)I = 8 + 32I$.
$\varphi_s(A.B) = 8 + 32I = (2+2I)(4+6I) = \varphi_s(A).\varphi_s(B)$.
**The description of the neutrosophic RSA algorithm:**
Assume that we have two sides $X$ and $Y$, $X$ wants to send an encrypted text to $Y$.
Suppose that $M = m + nI$ is the text, to encrypt $M$, $X$ should follow these steps.
**Step1.**
$X$picks two neutrosophic positive integers, $P = a+bI, Q = c+dI$ and compute $N = PQ = ac + (ad + bc + bd)I$.
[ it is better to chose $a, a+b, c, c+d$ to be 4 large prime integers with $gcd(a,c) = gcd(a+b, c+d) = 1$].
**Step2.**
$X$ computes $\varphi_s(N) = \varphi_s(P).\varphi_s(Q)$, where:
$\varphi_s(P) = a - 1 + I[\varphi(a+b) - (a-1)] = a - 1 + I[a+b-1-a+1] = a - 1 + bI$.
$\varphi_s(Q) = a - 1 + I[\varphi(c+d) - (a-1)] = c - 1 + dI$.
**Step3.**
$X$ picks an arbitrary neutrosophic positive integer $E = e_1 + e_2 I$ with $gcd\left(E, \varphi_s(N)\right) = 1$ and $1 < E < \varphi_s(N)$, the public key is $(E, N)$.
**Step4.**
$X$ encrypts the text $M$ by the formula:
$C \equiv M^E (mod\ N) = (m+nI)^{(e_1+e_2 I)} (mod\ N) = \left((m)^{e_1} + I\left[(m+n)^{(e_1+e_2)} - (m)^{e_1}\right]\right)(mod\ N)$.
$X$ sends $C$ to the other side $Y$.
The secret key is $E^{-1} = ({e_1}^{-1} + I[(e_1+e_2)^{-1} - {e_1}^{-1}])\left(mod\ \varphi_s(N)\right) = s_1 + s_2 I\ \left(mod\ \varphi_s(N)\right)$.
$Y$ decrypts the message as follows:
$M \equiv C^{E^{-1}} (mod\ N)$
**Example.**
Suppose that the first side $X$ has a message $M = 3 + 3I$.
$X$ picks $P = 3+2I$ , $Q = 7+4I > 0$, $gcd(P,Q) = 1$, that is because $gcd(3,7) = gcd(5,11) = 1$.
$N = PQ = 21 + 12I + 14I + 8I = 21 + 34I$.
$\varphi_s(N) = \varphi(21) + [\varphi(55) - \varphi(21)]I = 12 + (40-12)I = 12 + 28I$
*the secert key is* $X$ takes $1 < E = 5 + 6I < \varphi_s(N)$, with $gcd\left(E, \varphi_s(N)\right) = 1$.
The public key is $(E, N) = (5+6I, 21+34I)$.
$X$ encrypts the text $M = 3 + 3I$ as follows:
$C \equiv M^E (mod\ N) = (3^5 + I[6^{11} - 3^5])(mod\ 21 + 34I) \equiv 3^5 (mod\ 21) + I[6^{11} (mod\ 55) - 3^5 (mod\ 21)]$
$\equiv 12 + I[6 - 12] = 12 - 6I$
The secret key is $E^{-1} = 5^{-1} (mod\ 21) + I[11^{-1} (mod\ 40) - 5^{-1} (mod\ 21)] = 5 + I[11-5] = 5 + 6I$.
$Y$ decrypts the message as follows:
$M \equiv C^{E^{-1}} (mod\ N) \equiv 12^5 (mod\ 21) + I[6^{11} (mod\ 55) - 12^5 (mod\ 21)] \equiv 3 + I[6-3] = 3 + 3I$.
**Example.**
Assume that $X$ wants to encrypt the text $M = 2 + 6I$.
$X$ picks $P = 7+4I$ , $Q = 13+6I$, $N = PQ = 91 + 116I$.
$\varphi_s(N) = \varphi(P).\varphi(Q) = (6+4I).(12+6I) = 72 + 36I + 48I + 24I = 72 + 108I$
$1 < E = 17 + 14I < 72 + 108I$, with $gcd(17,72) = gcd(31,180) = 1$.

Doi: https://doi.org/10.54216/FPA.100206
Received: November 22, 2022 Accepted: March 04, 2023

The public key is $(E, N) = (17 + 14I, 91 + 116I)$.
$E^{-1} = 17^{-1}(mod\ 72) + I[31^{-1}(mod\ 180) - 17^{-1}(mod\ 72)] = 17 + I[151 - 17] = 17 + 134I$.
The encrypted text is:
$C \equiv M^E(mod\ N) \equiv 2^{17}(mod\ 91) + I[8^{31}(mod\ 207) - 2^{17}(mod\ 91)] \equiv 32 + I[170 - 32] = 32 + 138I$.
$Y$ decrypts the message as follows:
$M \equiv C^{E^{-1}}(mod\ N) \equiv 32^{17}(mod\ 21) + I[170^{151}(mod\ 55) - 32^{17}(mod\ 21)] \equiv 2 + I[9 - 3] = 2 + 6I$.

**Complexity Analysis with respect to the classical version**

Now, we will compare RSA and neutrosophic RSA algorithms by the duration needed to be broken by using the Brute-force: (All are measured in seconds in the first table):
The first table shows the comparison for some special values of the entry n, and the second one shows the comparison depending on the size of the entry n.

Table (1)

| Classical RSA | Duration | Neutrosophic RSA | Duration |
|---|---|---|---|
| For $n = 187$ | 0.00344800949097 | For $n = 187 + 726I$ | 0.00703191757209 |
| For $n = 913$ | 0.00358390808105 | For $n = 913 + 13128I$ | 0.00805377960208 |
| For $n = 14041$ | 0.004469871521 | For $n = 14041 + 542968I$ | 0.00614380836489 |
| For $n = 557009$ | 0.00167393684387 | For $n = 557009 + 8635898I$ | 0.00369000434875 |
| For $n = 9192907$ | 0.00201606750488 | For $n = 9192907 - 8635898I$ | 0.00369000434875 |

We can see that the neutrosophic version of RSA needs more time to be broken, and its complexity is around twice of classical RSA.

**Another comparison will be illustrated by the size of the entry n and with the brute-force attack.**
The measures of the duration of classical RSA by the size of n can be found in [15].

Table (2)

| Classical RSA | Duration by millisec | Neutrosophic RSA | Duration by millisec |
|---|---|---|---|
| The size of n is 7 | 0.002 | Same size | 0,004 |
| The size of n is 8 | 0.002 | Same size | 0,005 |
| The size of n is 9 | 0.56 | Same size | 1,2 |
| The size of n is 10 | 4.2 | Same size | 8.6 |
| The size of n is 11 | 12.1 | Same size | 24.3 |

In the following graph, the x-axis refers to the time duration of classical RSA; the y-axis refers to the duration of the neutrosophic RSA.

Doi: https://doi.org/10.54216/FPA.100206
Received: November 22, 2022 Accepted: March 04, 2023

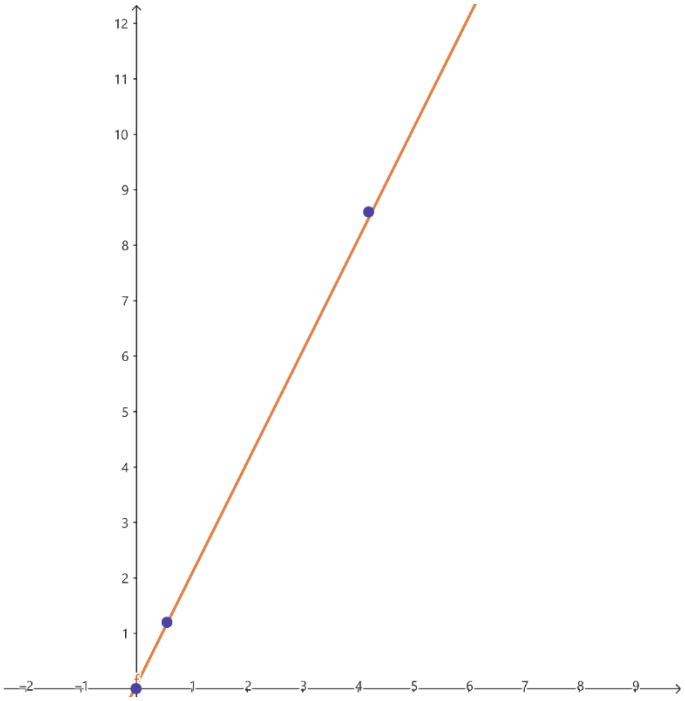

Figure 1: RSA and the neutrosophic RSA

Table 3: A comparison between the El-Gamal algorithm and the neutrosophic RSA algorithm:

| **El-Gamal** | **Duration by millisec** | **Neutrosophic RSA** | **Duration by millisec** |
|---|---|---|---|
| The size of n is 7 | 0.002 | Same size | 0,004 |
| The size of n is 8 | 0.002 | Same size | 0,005 |
| The size of n is 9 | 0.55 | Same size | 1,2 |
| The size of n is 10 | 4.2 | Same size | 8.6 |
| The size of n is 11 | 12.1 | Same size | 24.3 |

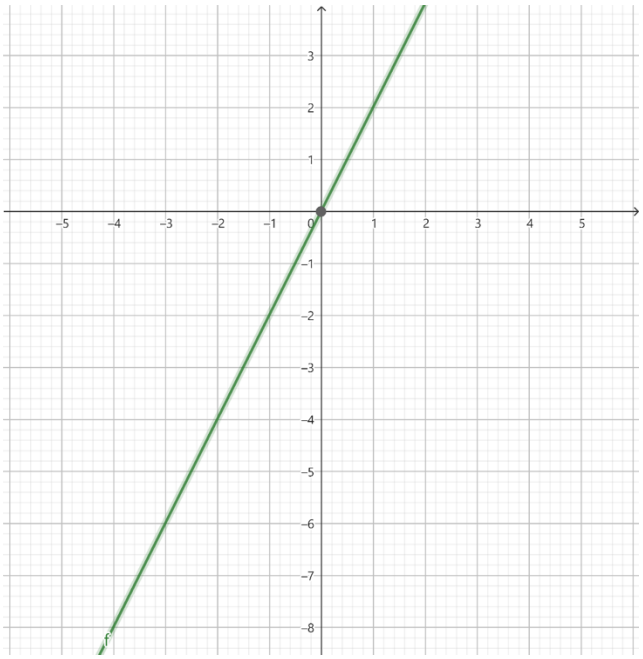

Figure 2: El-Gamal system and neutrosophic RSA

Doi: https://doi.org/10.54216/FPA.100206
Received: November 22, 2022 Accepted: March 04, 2023

In the previous graph, we can see easily that if the El-Gamal system needs t as the duration time to be broken by brute force, then the neutrosophic RSA algorithm needs around 2t.

**Conclusion**

In this paper, we have presented for the first time the neutrosophic version of the RSA algorithm depending on the foundations of fusion neutrosophic number theory. In addition, we have shown the efficiency of the neutrosophic version by illustrating many related tables and examples, where we have provided some numerical approaches, which showed that it has complexity two times more in a comparison with the classical version.

Neutrosophic number theory may have a great impact on cryptography, so we suggest researchers define a version of RSA depending on the refined neutrosophic number theoretical approach [12].

**References**

[1] Celik, M., and Olgun, N., " An Introduction To Neutrosophic Real Banach And Hillbert Spaces", Galoitica Journal Of Mathematical Structures And Applications, 2022.
[2] Celik, M., and Olgun, N., " On The Classification Of Neutrosophic Complex Inner Product Spaces", Galoitica Journal Of Mathematical Structures And Applications, 2022.
[3] Abobala, M., Partial Foundation of Neutrosophic Number Theory, Neutrosophic Sets and Systems, Vol. 39 , 2021.
[4] Smarandache, F., and Kandasamy, V.W.B., " Finite Neutrosophic Complex Numbers",·Source: arXiv. 2011.
[5] Agboola, A.A.A., Akinola, A.D., and Oyebola, O.Y., " Neutrosophic Rings I" , International J.Mathcombin, Vol 4,pp 1-14. 2011.
[6] Adeleke, E.O., Agboola, A.A.A.,and Smarandache, F., "Refined Neutrosophic Rings I", International Journal of Neutrosophic Science, Vol. 2(2), pp. 77-81. 2020.
[7] Abobala, M., "On Some Algebraic Properties of n-Refined Neutrosophic Elements and n-Refined Neutrosophic Linear Equations", Mathematical Problems in Engineering, Hindawi, 2021.
[8] Abobala, M., On Refined Neutrosophic Matrices and Their Applications In Refined Neutrosophic Algebraic Equations, Journal Of Mathematics, Hindawi, 2021.
[9] Cozzens, M. Miller, S.J. (2013). The Mathematics of Encryption: An Elementary Introduction, American Mathematical Society.
[10] Abdul Rahaman Wahab Sait , Irina Pustokhina , M. Ilayaraja, Modeling of Multiple Share Creation with Optimal Signcryption Technique for Digital Image Security, Journal of Intelligent Systems and Internet of Things, Vol. 0 , No. 1 , (2019) : 26-36.
[11] Sankari, H., and Abobala, M., "Neutrosophic Linear Diophantine Equations With two Variables", Neutrosophic Sets and Systems, Vol. 38, pp. 22-30, 2020.
[12] Ibrahim, M., and Abobala, M., "An Introduction To Refined Neutrosophic Number Theory", Neutrosophic sets and systems, Vol. 45, 2021.
[13] Smarandache, F. (1999). A Unifying Field in Logics. Neutrosophy: Neutrosophic Probability, Set and Logic. Rehoboth: American Research Press.
[14] Merkepci, M., and Sarkis, M., " An Application of Pythagorean Circles In Cryptography And Some Ideas For Future Non Classical Systems" , Galoitica Journal Of Mathematical Structures and Applications, 2022.
[15] Mezher, A,E., "Enhanced RSA Cryptosystem Based on Multiplicity Of Public and Private Keys ", International Journal Of Electrical and Computer Engineering, Vol.8, No.5, 2018.
[16] Sarkis, M., " On The Solutions Of Fermat's Diophantine Equation In 3-refined Neutrosophic Ring of Integers", Neoma Journal of Mathematics and Computer Science, 2023.

Doi: https://doi.org/10.54216/FPA.100206

Received: November 22, 2022 Accepted: March 04, 2023