Neutrosophic Sets and Systems

Volume 54 Article 2

4-11-2023

On A Novel Security Scheme for The Encryption and Decryption Of 2×2 Fuzzy Matrices with Rational Entries Based on The Algebra of Neutrosophic Integers and El-Gamal Crypto-System

Mohammad Abobala

Ali Allouf

NSS
Neutrosophic Sets and Systems, Vol. 54, 2023
University of New Mexico

On A Novel Security Scheme for The Encryption and Decryption Of 2×2 Fuzzy Matrices with Rational Entries Based on The Algebra of Neutrosophic Integers and El-Gamal Crypto-System

[1]Mohammad Abobala, [2]Ali Allouf

[1] Tishreen University, Department Of Mathematics, Latakia, Syria

Mohammadabobala777@gmail.com

[2] **Tishreen University,** Faculty Of computer engineering and automation**, Latakia, Syria**

Ali1allouf@gmail.com

Abstract:

The main goal behind mathematical cryptography is to keep messages and multimedia messages secret at a time when modern means of communication have spread and become very diverse.

Fuzzy matrices as strong tools which was defined to deal with incomplete and uncertain data and many relationships in real life problems especially those which are related to images and graphs, may considered as important subjects for secret information and communication.

The aim of this research paper is to present a new model and method for encrypting 2×2 fuzzy matrices using the basic concepts in neutrosophic number theory and El Gamal algorithm in cryptography, where we generalize El Gamal algorithm to become applicable to the ring of neutrosophic integer numbers that represents the studied fuzzy matrices.

On the other hand, we study the applications of the novel algorithm to the encryption and decryption of some fuzzy relations represented in terms of fuzzy functions.

In addition, we illustrate many examples to clarify the validity of the new algorithm.

Key words:

Neutrosophic integer, fuzzy matrix, fuzzy relation, fuzzy graph, EL-Gamal crypto-system

Introduction and Preliminaries

The concept of fuzzy logic and fuzzy set was presented by Zadeh [10]. The main point of fuzzy approach is to deal with a degree for truth and a degree for falsity. Smarandache has generalized fuzzy ideas by introducing neutrosophic logic [16], which deals with a degree of truth (T), a degree of falsity (F), and a degree of indeterminacy (I).

If X is a non-empty set. A fuzzy set (subset) μ of the set X is defined as a function μ: X → [0, 1], and if μ is a fuzzy subset of a set X. For t ∈ [0, 1], the set X_t= {$x \in X ; \mu(x) \geq t$}, then μ is called a t-level subset of the fuzzy subset μ [3].

In the literature, we find many applications and approaches built over the ideas of fuzzy logic especially in probability, algebra, and graph theory [5, 7, 23].

The concept of fuzzy matrix was introduced in [6], and then it was studied widely in [8-9, 13], especially the algebraic properties and applications of these matrices.

A square 2×2 fuzzy matrix is defined as follows:

A=$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ with $a_{ij} \in [0,1]$.

Mathematical Asymmetric cryptography is a branch of applied mathematics and theoretical computer science that applies mathematical methods and models to encrypt messages and multimedia [4]. Many systems and algorithms were presented such as RSA algorithm and El-Gamal algorithm [4, 15]. In addition, many attacks and applications of some special numbers can be found in [20-21].

In [19], the first suggestion of using the generalizations of integers in cryptology was presented, where authors have suggested the usage of neutrosophic numbers, split-complex numbers, and dual numbers in cryptology.

Neutrosophic cryptography became known recently by using neutrosophic number theory in generalizing classical crypto-systems into more complex and powerful systems. We find a neutrosophic version of RSA and refined El-Gamal crypto-algorithm [18, 22].

In this paper, we continuo the previous efforts for applying neutrosophic number theory in cryptology, where a neutrosophic version of El-Gamal algorithm based on the foundations of neutrosophic number theory will be presented and handled. In addition, we apply this algorithm to encrypt and decrypt fuzzy 2×2 matrices with rational entries.

First, we recall some important concepts and definitions.

The description of El Gamal crypto-scheme:

Assume that we have two sides A and B, the first side A wants to send an encrypted message to B.

The recipient B picks a large prime number p and a generator $1 < g < p - 1$, then B picks x that $0 < x < p - 2$ and computes $X = g^x (mod\ p)$. The number x is kept as the secret key suppose that A wants to send (m) as a message to B.

A should pick $0 < r < p - 2$ and compute $R = g^r (mod\ p)$, the shared key K is computed as follows $K = X^r (mod\ p)$.

A encrypts the message as follows $S = m \times k$, and sends the encrypted message to B as a duplet (R, S).

The second side B decrypts the message by using her/his secret key x as follows $m = R^{-x} \times S$.

Definition: (Neutrosophic integers) [1]

Let R be any ring, I be an indeterminacy with the property $I^2 = I$. Then $R(I) = \{a + bI; a, b \in R\}$ is called a neutrosophic ring.

If $R = Z$ is the ring of integers, then $Z(I) = \{a + bI; a, b \in Z\}$ is called the neutrosophic ring of integers. Elements of Z(I) are called neutrosophic integers.

Theorem: (neutrosophic congruencies) [1]

Let $x = a + bI, y = c + dI, z = m + nI$ be three elements in Z(I). Then $x \equiv y(mod z)$ if and only if

$a \equiv c(mod\ m), a + b \equiv c + d(mod\ m + n)$.

Theorem: (neutrosophic powers) [2]

$(a + bI)^{c+dI} = a^c + I[(a + b)^{c+d} - a^c]$.

Definition [2]

Let $Z(I) = \{a + bI;\ a, b \in Z\}$ be the neutrosophic ring of integers, we say that $a + bI \leq c + dI$ if and only if $a \leq c\ and\ a + b \leq c + d$.

Z(I) is a partially ordered set with the previous relation.

Main Discussion

Neutrosophic Version of EL-Gamal algorithm:

To build a neutrosophic version of EL-Gamal Algorithm, we substitute each integer t by a positive neutrosophic integer $t_1 + t_2 I$; $t_1 > 0$, $t_1 + t_2 > 0$.

The recipient (B) picks a neutrosophic positive integer $p = p_1 + p_2 I$, where $p_1, p_1 + p_2$ are large primes.

(B) picks a generator $0 < g = g_1 + g_2 I < p = p_1 + p_2 I - 1$, i.e $g_1 < p_1 - 1$, $g_1 + g_2 < p_1 + p_2 - 1$.

(B) picks $0 < x = x_1 + x_2 I < p = p_1 + p_2 I - 2$, i.e $x_1 < p_1 - 2$, $x_1 + x_2 < p_1 + p_2 - 2$ and then computes $X = g^x(mod\ p) = {g_1}^x(mod\ p_1) + I[(g_1 + g_2)^x(mod\ p_1 + p_2) - {g_1}^x(mod\ p_1)]$.

The publish key is (g, X).

Assume that (A) will send $m = m_1 + m_2 I$ to (B).

(A) should pick $0 < r = r_1 + r_2 I < p = p_1 + p_2 I - 2$ and compute:

$R = g^r(mod\ p) = {g_1}^{r_1}(mod\ p_1) + I[(g_1 + g_2)^{r_1+r_2}(mod\ p_1 + p_2) - {g_1}^{r_1}(mod\ p_1)] = t_1 + t_2 I.$

The shared key

$K = X^r(mod\ p)$

$= {g_1}^{x_1 r_1}(mod\ p_1)$

$+ I\left[(g_1 + g_2)^{(x_1+x_2)(r_1+r_2)}(mod\ p_1 + p_2) - {g_1}^{x_1 r_1}(mod\ p_1)\right] = k_1 + k_2 I$

(A) encrypts its message as follows:

$S = m \times k = (m_1 + m_2 I)(k_1 + k_2 I) = m_1 k_1 + I(m_1 k_2 + m_2 k_1 + m_2 k_2)$

The other side (B)decrypts the message as follows:

$m = R^{-x}(mod\ p);\ R^{-1} = {t_1}^{-1}(mod\ p_1) + I[(t_1 + t_2)^{-1}(mod\ p_1 + p_2) - {t_1}^{-1}(mod\ p_1)]$

Example.

Consider that (B) has picked $p = p_1 + p_2 I = 5 + 6I$, the generator $g = 3 + 2I = g_1 + g_2 I$, the secret key $x = x_1 + x_2 I = 2 + 5I$.

$K = g^x(mod\ p) = 3^2(mod\ 5) + I[5^7(mod\ 11) - 3^2(mod\ 5)] = 4 + I[3 - 4] = 4 - I,$

the publick key is $(g, X) = (3 + 2I, 4 - I)$

Assume that (A)has decided to send $m = 4 + 4J$ to (B).

(A) picks $r = r_1 + r_2 I = 2 + I$ and computes:

$R = g^r(mod\ p) = 3^2(mod\ 5) + I[5^3(mod\ 11) - 3^2(mod\ 5)] = 4 + I[5 - 4] = 4.$

The shared key $K \equiv X^r(mod\ p) = 4^2(mod\ 5) + I[3^3(mod\ 11) - 4^2(mod\ 5)] = 1 + I[5 - 1] = 1 + 4I = k_1 + k_2 I.$

The encrypted message

$S = m \times k = (4 + 4I)(1 + 4I) = 4 + I(16 + 4 + 16) = 4 + 36I.$

(B) decrypts the message as follows:

$m = R^{-x}.s\ (mod\ p), where:$

$R^{-1} = 4^{-1}(mod\ 5) + I[4^{-1}(mod\ 11) - 4^{-1}(mod\ 5)] = 4 + I(3 - 4) = 4 - I$

$m \equiv R^{-x}.s\ (mod\ p) = (4 - I)^{2+5I}.(4 + 36I)(modp)$

$\equiv [4^2 + I(3^7 - 4^2)](4 + 36I)(modp)$

$= (16 + 271I)(4 + 36I)(modp) = (64 + 87416I)(modp) \equiv 64(mod\ 5) + I[(87416 + 64)(mod\ 11) - 64(mod\ 5)] = 4 + I(8 - 4) = 4 + 4I.$

Which is the plain text.

Example.

Consider the (B)has picked $p = p_1 + p_2 I = 13 + 6I$, the generator $g = g_1 + g_2 I = 5 + 3I$, the secret key is $x_1 + x_2 I = 6 + 3I$.

$$X \equiv g^x (mod\ p) = 5^6 (mod\ 13) + I[8^9 (mod\ 19) - 5^6 (mod\ 13)] = 12 + I[18 - 12]$$
$$= 12 + 6I$$

The public key is $(g, X) = (5 + 3I, 12 + 6I)$.

Assume that (A) has decided to send $m = 10 + I$ to (B).

(A) picks $r_1 + r_2 I = 3 + 2I$ and computes:

$$R \equiv g^r (mod\ p) = 5^3 (mod\ 13) + I[8^5 (mod\ 19) - 5^3 (mod\ 13)] = 8 + I[12 - 8]$$
$$= 8 + 4I$$

The shared key:

$$K \equiv X^r (mod\ p) = 12^3 (mod\ 13) + I[18^5 (mod\ 19) - 12^3 (mod\ 13)] = 12 +$$
$$I[18 - 12] = 12 + 6I = k_1 + k_2 I.$$

The encrypted message is:

$$S = m \times k = (10 + I)(12 + 6I) = 120 + I(60 + 12 + 6) = 120 + 78I.$$

(B) decrypts the message as follows:

$$R^{-1} = 8^{-1} (mod\ 13) + I[12^{-1} (mod\ 19) - 8^{-1} (mod\ 13)] = 5 + I(8 - 5) = 5 + 3I$$

$$m = (R^{-1})^x S\ (mod\ p), we\ have\ (5 + 3I)^{6+3I}.(modp) \equiv [5^6 + I(8^9 - 5^6)](modp)$$

$$= 5^6 (mod\ 13) + I[8^9 (mod\ 19) - 5^6 (mod\ 13)] = 12 + (18 - 12) = 12 + 6I$$

$$(120 + 78I)(modp) = 120 (mod\ 13) + I[198 (mod\ 19) - 120 (mod\ 13)]$$
$$= 3 + (8 - 3) = 3 + 5I$$

$$m = (12 + 6I)(3 + 5I) = (36 + 60I + 18I + 30I) = (36 + 108I)(mod\ p) \equiv$$
$$36 (mod\ 13) + I[144 (mod\ 19) - 36 (mod\ 13)] = 10 + I[11 - 10] = 10 + I.$$

Which is the plain text.

Fuzzy Matrices as Neutrosophic Points:

Definition:

Let A be a fuzzy 2×2 matrix

A=$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$

Then A can be written in term of a 2-dimensional neutrosophic point as follows: $A_N = (a_{11} + a_{12}I, a_{21} + a_{22}I)$.

Example:

Consider the following fuzzy matrix:

A=$\begin{pmatrix} 0.3 & 0.2 \\ 1 & 0.9 \end{pmatrix}$, then A can be written in the following form: $A_N = (0.3 + 0.2I, 1 + 0.9I)$.

The encryption/decryption of a fuzzy 2×2 matrix:

Let A be a fuzzy 2×2 matrix with rational entries

A=$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, assume that the sender (X) has decided to send the matrix A to the recipient (Y) as a cipher text.

As a first step, (X) should transform the fuzzy matrix A to a 2-dimensional neutrosophic point

$A_N = (a_{11} + a_{12}I, a_{21} + a_{22}I)$, then (X) picks a weight $w \in Z^+$ with the property $wa_{11}, wa_{22}, wa_{12}, wa_{21} \in Z^+$. This implies that $w(a_{11} + a_{12}I), w(a_{21} + a_{22}I) \in Z(I)$, and (X) should send w to (Y).

The recipient (Y) generates the public key as we explained above in neutrosophic El-Gamal algorithm, and shares his/her key with (X).

(X) decrypts the $w(a_{11} + a_{12}I), w(a_{21} + a_{22}I)$ by using the key, and sends the cipher neutrosophic point to (Y).

(Y) decrypts the message as we have shown previously, and divide it by the weight w. Then (Y) rearranges the values into matrix rows to get the plain text.

Example:

We explain the validity of the novel scheme by the following example.

Consider the following fuzzy matrix:

A=$\begin{pmatrix} 0.3 & 0.2 \\ 0.1 & 0.4 \end{pmatrix}$, then A can be written in the following form: $A_N = (0.3 + 0.2I, 0.1 + 0.4I)$. (X) picks w=10 and computes the new point $wA_N = (3 + 2I, 1 + 4I)$, thaen (X) shares w=10 with (Y).

Assume that the recipient (Y) has generated the public key as follows:

Consider the (Y)has picked $p = p_1 + p_2I = 13 + 6I$, the generator $g = g_1 + g_2I = 5 + 3I$, the secret key is $x_1 + x_2I = 6 + 3I$.

$$X \equiv g^x (mod\ p) = 5^6 (mod\ 13) + I[8^9 (mod\ 19) - 5^6 (mod\ 13)] = 12 + I[18 - 12]$$
$$= 12 + 6I$$

The public key is $(g, X) = (5 + 3I, 12 + 6I)$.

(X) will send $wA_N = (3+2I, 1+4I)$ to (Y).

(X) picks $r_1 + r_2 I = 3 + 2I$ and computes:

$R \equiv g^r (mod\ p) = 5^3 (mod\ 13) + I[8^5 (mod\ 19) - 5^3 (mod\ 13)] = 8 + I[12 - 8]$

$= 8 + 4I$

The shared key:

$K \equiv X^r (mod\ p) = 12^3 (mod\ 13) + I[18^5 (mod\ 19) - 12^3 (mod\ 13)] = 12 +$

$I[18 - 12] = 12 + 6I = k_1 + k_2 I.$

The encrypted message is:

$S = wA_N \times k = (3+2I, 1+4I)(12+6I) = (36+54I, 12+78I).$

(Y) decrypts the message as follows:

$R^{-1} = 8^{-1} (mod\ 13) + I[12^{-1} (mod\ 19) - 8^{-1} (mod\ 13)] = 5 + I(8-5) = 5 + 3I$

$m = (R^{-1})^x \times S\ (mod\ p), we\ have\ (5+3I)^{6+3I} (modp) \equiv [5^6 + I(8^9 - 5^6)](modp)$

$= 5^6 (mod\ 13) + I[8^9 (mod\ 19) - 5^6 (mod\ 13)] = 12 + (18 - 12) = 12 + 6I.$

On the other hand, $(36+54I, 12+78I)(mod\ p) = (36(mod\ 13) + I[90(mod\ 19) -$

$36(mod\ 13)], 12\ (mod\ 13) + I[90(mod\ 19) - 12(mod\ 13)])=$

$(10+4I, 12+2I).$

The plain text is $wA_N = (12+6I).(10+4I, 12+2I)(mod\ p) = (120+132I, 144+$

$108I)(mod\ p) \equiv (120(mod\ 13) + I[252(mod\ 19) - 120(mod\ 13)], 144(mod\ 13) +$

$I[252(mod\ 19) - 144(mod\ 13)]) = (3+2I, 1+4I).$

Now, (Y) should divide the plain text by w=10, and rearrange it as rows of a matrix to get:

A=$\begin{pmatrix} 0.3 & 0.2 \\ 0.1 & 0.4 \end{pmatrix}$.

A Comparison between El-Gamal algorithm and neutrosophic El-Gamal algorithm:

Since fuzzy matrices may have entries such as 0 or 1, then the encryption by using classical El-Gamal algorithm may be easy to be broken. Meanwhile, transforming them to neutrosophic points keeps the information secret. We explain it through the following example.

Example:

Consider the following fuzzy matrix:

A=$\begin{pmatrix} 0.3 & 0 \\ 0 & 0.4 \end{pmatrix}$, then A can be written in the following form: $A_N = (0.3, 0.4I)$. (X) picks w=10 and computes the new point $wA_N = (3, 4I)$, then (X) shares w=10 with (Y).

Assume that the recipient (Y) has generated the public key as follows:

Consider the (Y)has picked $p = p_1 + p_2 I = 13 + 6I$, the generator $g = g_1 + g_2 I = 5 + 3I$, the secret key is $x_1 + x_2 I = 6 + 3I$.

$$X \equiv g^x (mod\ p) = 5^6 (mod\ 13) + I[8^9 (mod\ 19) - 5^6 (mod\ 13)] = 12 + I[18 - 12]$$
$$= 12 + 6I$$

The public key is $(g, X) = (5 + 3I, 12 + 6I)$.

(X) will send $wA_N = (3 + 2I, 1 + 4I)$ to (Y).

(X) picks $r_1 + r_2 I = 3 + 2I$ and computes:

$$R \equiv g^r (mod\ p) = 5^3 (mod\ 13) + I[8^5 (mod\ 19) - 5^3 (mod\ 13)] = 8 + I[12 - 8]$$
$$= 8 + 4I$$

The shared key:

$K \equiv X^r (mod\ p) = 12^3 (mod\ 13) + I[18^5 (mod\ 19) - 12^3 (mod\ 13)] = 12 +$

$I[18 - 12] = 12 + 6I = k_1 + k_2 I.$

The encrypted message is:

$S = wA_N \times k = (3, 4I)(12 + 6I) = (36 + 18I, 72I).$

(Y) decrypts the message as follows:

$$R^{-1} = 8^{-1} (mod\ 13) + I[12^{-1} (mod\ 19) - 8^{-1} (mod\ 13)] = 5 + I(8 - 5) = 5 + 3I$$

$m = (R^{-1})^x \times S\ (mod\ p), we\ have\ (5 + 3I)^{6+3I} (modp) \equiv [5^6 + I(8^9 - 5^6)](modp)$

$= 5^6 (mod\ 13) + I[8^9 (mod\ 19) - 5^6 (mod\ 13)] = 12 + (18 - 12) = 12 + 6I.$

On the other hand, $(36 + 18I, 72I)(mod\ p) = (36(mod\ 13) + I[54(mod\ 19) -$

$36(mod\ 13)], 0\ (mod\ 13) + I[72(mod\ 19) - 0(mod\ 13)])=$

$(10 + 6I, 15I).$

The plain text is $wA_N = (12 + 6I).(10 + 6I, 15I)(mod\ p) = (120 + 168I, 270I)(mod\ p) \equiv (120(mod\ 13) + I[288(mod\ 19) - 120(mod\ 13)], 0(mod\ 13) + I[270(mod\ 19) - 0(mod\ 13)]) = (3, 4I)$.

Now, (Y) should divide the plain text by w=10, and rearrange it as rows of a matrix to get:

A=$\begin{pmatrix} 0.3 & 0 \\ 0 & 0.4 \end{pmatrix}$.

On the other hand, if (X) has ciphered his numbers with classical El-Gamal algorithm, then he gets 0 as a cipher text twice, that is because when he computes $S = (0) \times k = 0$ which is equal to the plain text. Meanwhile, when he uses neutrosophic formulas, he gets $(10 + 6I, 15I)$ which is different from the original message. From this point of view, we can say that the usage of neutrosophic numbers and neutrosophic El-Gamal algorithm is better that using classical algorithm only, especially in the case of ciphering 0 and 1 entries.

Applications to fuzzy relations

Let $X = \{x_1, x_2\}$,$Y = \{y_1, y_2\}$ be two sets with two elements, with a fuzzy relation R(X,Y) defined on X as follows:

$f_{ij}(x_i, y_j) = a_{ij} \in [0,1]$. Then this relation can be represented as a fuzzy 2×2 matrix

A=$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, so that by using neutrosophic El-Gamal algorithm we can encrypt it as a secret message.

We clarify that by the following example.

Example:

Assume that we have two men m_1, m_2, and two hospitals H_1, H_2. Suppose that the first man goes to the first hospital in 30% of cases of illness, and in 70% of cases, he goes to the second hospital.

As for the second man, he goes to the first hospital in 90% of cases, and he goes to the second hospital in 10% of cases.

Then, we can represent this information as a fuzzy relation, $f(m_1, H_1) = 0.3$,

$f(m_1, H_2) = 0.7, f(m_2, H_1) = 0.9, f(m_2, H_2) = 0.1$.

So, it can be described by the following fuzzy matrix with rational entries:

A=$\begin{pmatrix} 0.3 & 0.7 \\ 0.9 & 0.1 \end{pmatrix}$.

Then A can be written in the following form: $A_N = (0.3 + 0.7I, 0.9 + 0.1I)$. (X) picks w=10 and computes the new point $wA_N = (3 + 7I, 9 + I)$, then (X) shares w=10 with (Y).

Assume that the recipient (Y) has generated the public key as follows:

Consider the (Y)has picked $p = p_1 + p_2I = 13 + 6I$, the generator $g = g_1 + g_2I = 5 + 3I$, the secret key is $x_1 + x_2I = 6 + 3I$.

$$X \equiv g^x(mod\ p) = 5^6(mod\ 13) + I[8^9(mod\ 19) - 5^6(mod\ 13)] = 12 + I[18 - 12]$$
$$= 12 + 6I$$

The public key is $(g, X) = (5 + 3I, 12 + 6I)$.

(X) will send $wA_N = (3 + 7I, 9 + I)$ to (Y).

(X) picks $r_1 + r_2I = 3 + 2I$ and computes:

$$R \equiv g^r(mod\ p) = 5^3(mod\ 13) + I[8^5(mod\ 19) - 5^3(mod\ 13)] = 8 + I[12 - 8]$$
$$= 8 + 4I$$

The shared key:

$K \equiv X^r(mod\ p) = 12^3(mod\ 13) + I[18^5(mod\ 19) - 12^3(mod\ 13)] = 12 +$

$I[18 - 12] = 12 + 6I = k_1 + k_2I$.

The encrypted message is:

$S = wA_N \times k = (3 + 7I, 9 + I)(12 + 6I) = (36 + 144I, 108 + 72I)$.

(Y) decrypts the message as follows:

$$R^{-1} = 8^{-1}(mod\ 13) + I[12^{-1}(mod\ 19) - 8^{-1}(mod\ 13)] = 5 + I(8 - 5) = 5 + 3I$$

$m = (R^{-1})^x \times S\ (mod\ p), we\ have\ (5 + 3I)^{6+3I}(modp) \equiv [5^6 + I(8^9 - 5^6)](modp)$

$= 5^6(mod\ 13) + I[8^9(mod\ 19) - 5^6(mod\ 13)] = 12 + (18 - 12) = 12 + 6I$.

On the other hand, $(36 + 144I, 108 + 72I)(mod\ p) = (36(mod\ 13) +$

$I[180(mod\ 19) - 36(mod\ 13)], 108\ (mod\ 13) + I[180(mod\ 19) - 108(mod\ 13)])=$

$(10 - I, 4 + 5I)$.

The plain text is $wA_N = (12 + 6I).(10 - I, 4 + 5I)(mod\ p) = (120 + 42I, 48 + 114I)(mod\ p) \equiv (120(mod\ 13) + I[162(mod\ 19) - 120(mod\ 13)], 48(mod\ 13) + I[162(mod\ 19) - 48(mod\ 13)]) = (3 + 7I, 9 + I)$.

Now, (Y) should divide the plain text by w=10, and rearrange it as rows of a matrix to get:

A=$\begin{pmatrix} 0.3 & 0.7 \\ 0.9 & 0.1 \end{pmatrix}$. This means that (Y) is able to reform the secret fuzzy relation in the original form

$f(m_1, H_1) = 0.3,$

$f(m_1, H_2) = 0.7, f(m_2, H_1) = 0.9, f(m_2, H_2) = 0.1.$

Conclusion

In this paper, we have used the basics of neutrosophic number theory and classical El-Gamal crypto-system to build a new version, which we call neutrosophic EL-Gamal algorithm.

In addition, we use the novel algorithm to encrypt and decrypt messages that contain 2×2 fuzzy matrices with rational entries.

On the other hand, some application of decrypting fuzzy relations and fuzzy functions, which can be represented as 2×2 fuzzy matrices with rational entries were presented and illustrated by examples.

In the future, we aim to find algorithm to encrypt and decrypt $n \times n$ fuzzy matrices with rational entries by using neutrosophic algebraic structures.

References

1. Abobala, M., (2021). Partial Foundation of Neutrosophic Number Theory. Neutrosophic Sets and Systems, Vol. 39..
2. Abobala, M., and Ziena, M.B., (2023) . A Study Of Neutrosophic Real Analysis By Using One Dimensional Geometric AH-Isometry. Galoitica Journal Of Mathematical Structures and Applications, Vol 3.
3. Akram, M.; Dudek, W.A. Regular bipolar fuzzy graphs. Neural Comput. Appl. **2012**, 21, 197–205.

4. Cozzens, M. Miller, S.J. (2013). The Mathematics of Encryption: An Elementary Introduction, American Mathematical Society.
5. D.S.Malik, J.N.Mordeson, Fuzzy Commutative Algebra, World Scientific Publishing, Singapore, 1998.
6. G. Emam and M.Z. Ragab, The Determinant and Adjoint of a Square Fuzzy Matrix, Information Sciences, vol. 84 (New York, New York, 1995) pp. 209-220.
7. HAO, Jiang, General theory on fuzzy subgroupoids with respect to a t-norm T1, Fuzzy Sets and Systems, **117**, 455-461 (2001).
8. Ilanthenral, F. Smarandache, and W.B. Vasantha Kandasamy, Elementary Fuzzy Matrix215 Theory and Fuzzy Models for Social Scientists, (Los Angeles, California, 2007) p. 33.
9. K.S. Krishnamohan and K. Muthugurupackiam, Generalisation of Idempotent Fuzzy Matrices, International Journal of Applied Engineering Research, vol. 13, no. 13 (2018) pp. 11087-11090.
10. L.A.Zadeh, Fuzzy sets, Inform. Control 8(1965) 383-353.
11. M.G. Thomason, Convergence of powers of a fuzzy matrix, Journal of Mathematical Analysis and Applications, vol. 57(2) (February 1977) pp. 476-480.
12. Martin, N., Priya, R., & Smarandache, F. (2021). New Plithogenic sub cognitive maps approach with mediating effects of factors in COVID-19 diagnostic model. Journal of Fuzzy Extension and Applications, 2(1), 1-15. doi: 10.22105/jfea.2020.250164.1015
13. P.W. Eklund, X. Sun, and D.A. Thomas, Fuzzy Matrices: An Application in Agriculture, Proc. IPMU, (September 1995) pp. 765-769.
14. Polymenis, A. (2021). A neutrosophic Student's t –type of statistic for AR (1) random processes. Journal of Fuzzy Extension and Applications, 2(4), 388-393. doi: 10.22105/jfea.2021.287294.1149.
15. Rivest, R. Shamir, Adleman, A. (1975). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM (21): 120-126.
16. Smarandache, F. (1999). A Unifying Field in Logics. Neutrosophy: Neutrosophic Probability, Set and Logic. Rehoboth: American Research Press.

17. X.Yuan, E.S.Lee,Fuzzy group based on fuzzy binary operation, Comput. Math. App. 47 (2004) 631-641.
18. Merkepci, M., Abobala, M., and Allouf, A., " The Applications of Fusion Neutrosophic Number Theory in Public Key Cryptography and the Improvement of RSA Algorithm ", Fusion: Practice and Applications, 2023.
19. Merkepci, M,; 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**.
20. S.Barzut, M.Milosavljevic, S. Adamovic, M. Saračević, N. Macek, M.Gnjatovic (2021), A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks, Mathematics, 9(7), 730.
21. Aroukatos, N.; Manes, K.; Zimeras, S.; Georgiakodis, F. Techniques in Image Steganography using Famous Number Sequences.Int. J. Comput. Technol. 2013, 11, 2321–2329.
22. Merkepci, M., and Abobala, M., " Security Model for Encrypting Uncertain Rational Data Units Based on Refined Neutrosophic Integers Fusion and El Gamal Algorithm ", Fusion: Practice and Applications, 2023.
23. Hatip, A., " On Intuitionistic Fuzzy Subgroups of (M-N) Type and Their Algebraic Properties", Galoitica Journal Of Mathematical Structures and Applications, Vol.4, 2023.

Received: December 30, 2022. **Accepted:** April 01, 2023