

Cryptography in Terms of Triangular Neutrosophic Numbers with Real Life Applications

Ali Hamza[1],Muhammad Naveed Jafar *[1], Ahtasham Habib[2], Sara Farooq[2],Ezgi TÜRKARSALAN[2]

[1] Department of Mathematics Lahore Garrison University, Sector-C, Av-4, DHA Phase VI 54000 Lahorer, Pakistan
[2] Department of Mathematics Lahore Garrison University, Sector-C, Av-4, DHA Phase VI 54000 Lahorer, Pakistan
[2] Department of Mathematics Lahore Garrison University, Sector-C, Av-4, DHA Phase VI 54000 Lahorer, Pakistan
[2] Department of Mathematics Lahore Garrison University, Sector-C, Av-4, DHA Phase VI 54000 Lahorer, Pakistan
[2]Department of Mathematics, TED University, Ön Cebeci, Ziya Gökalp Cd. 48/A, 06420 Çankaya/Ankara, Turkey

* Correspondence: naveedjafar@lgu.edu.pk

Abstract

In this article, our main focus is to put forward the concept of Cryptography in terms of triangular neutrosophic numbers. This kind of cryptography is really reliable, manual, secure, and based on few simple steps. All the encryption and decryption are easy to proceed (mention below). As we know, Public-key cryptography as an indefatigable defender for human privacy and use as information transfer from the ages. various concepts are available with regard to cryptography e.g. Elliptic curve cryptography. TNNC (Triangular neutrosophic numbers cryptography) is familiar with basic concepts of math as well as applicable in different situations e.g. code cryptography, detailed view cryptography, and Graph cryptography encryption facilitate.

Keywords: Cryptography, Triangular Neutrosphic numbers, Code Encryption, Detailed overview encryption.

Why is Cryptography in Terms of Triangular neutrosophic numbers required?

- Easy to use and no computer work required to proceed (Fully manual).
- With the help of math's law, it is impossible to decrypt without a key.
- No internet required for that kind of cryptography.
- Convenient for personal use as well as for personal records.
- Based on basic math calculation and possible to proceed with one formula.

1 Introduction and History

Analysts, investigators, and mathematicians from all over the world introduce a wide range of techniques to solve decision-making problems. After great approaches in the field of medicine, selection problem, human resources, and now with the help of Triangular neutrosophic numbers TNNs, new possibilities are available, with respect to cryptography. Researchers give their best, as fundamental of cryptography, principles, applications, and encryption slandered [1-2]. Cryptography has become really handy and image cryptography [3-6], color image cryptography has been introduced [7] and chocolate cryptography also has been developed [8]. Stegano-cryptosystems introduced as well as researchers have also create new approaches in cryptography including S-Boxes [9-19].

DOI: 10.5281/zenodo.4127138
Received: Jun 04, 2020 Accepted: September 14, 2020

Life is full of uncertainty and decision making, and math is a key to solve daily life problems, on the way to serve humankind. Fuzzy logic has its own importance (introduced by Molodtsov) [20] in 1999 to deal with uncertainty. After the fuzzy set theory [21-23] Intuitionistic fuzzy sets was introduced [24] then neutrosophic sets [25]. Fuzzy and Neutrosophic set theory plays an important role in the field of uncertainty and to handle situation regards to multi-criteria decision making and in the line of evolution, neutrosophic fuzzy numbers [26] and finally Triangular neutrosophic numbers were introduced [27].

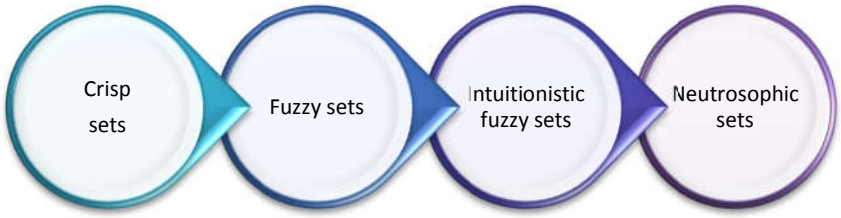


Figure 1

Researchers also exaggerate the concept of neutrosophic [28-40]. Neutrosophic sets, which we use, are base on truth, indeterminacy, and falsity. Wang [41] introduces Single-value neutrosophic sets and Ye [42] further furnished the concept of neutrosophic sets. Smarandache and many other researchers [43-50] introduce TOPSIS technique and their services in multi-criteria decision-making (MCDM), also appreciate able. As well as many other researchers from different origins of the world introduce many possibilities and put forward the concept of Multi-Criteria decision-making (MCDM) [51-57] and the properties of triangular and pentagonal neutrosophic number are proposed by A. Chakraborty [58-59].

UP until the 1970s, Encryption all over the world was based on symmetric ciphers, after that technology rises and overcomes Manual Cryptography methods. But remember that, online cryptography is risky and complex in some situations. Hence by TNNC Manual cryptography is simple to use secure, undemanding and Cipher Text is now more complex and impossible to break. With huge applications in code encryption, name encryption and complete information of the company is now secure manually.

1.1 Motivation and Benefits

As we all know that, neutrosophic is advance universe and really convenient to solve MCDM problems and now introduces new possibilities in Cryptography. With the help of Triangular Neutrosophic concept manual cryptography resurrect as well as, with more security, less demanding and easy steps to occur. This concept is totally new, Cipher text is now more complex, deal with truth, indeterminacy and falsity at the same time, Graph Encryption possible and with one key this cryptography is now personal cryptography. Hence, all the personal records (Account number, budget, earning, Persons for different situations, Graphs) are all Encrypted manually.

1.2 The Paper Presentation

In this current epoch, the concept of manual Cryptography as TNNC is extended.

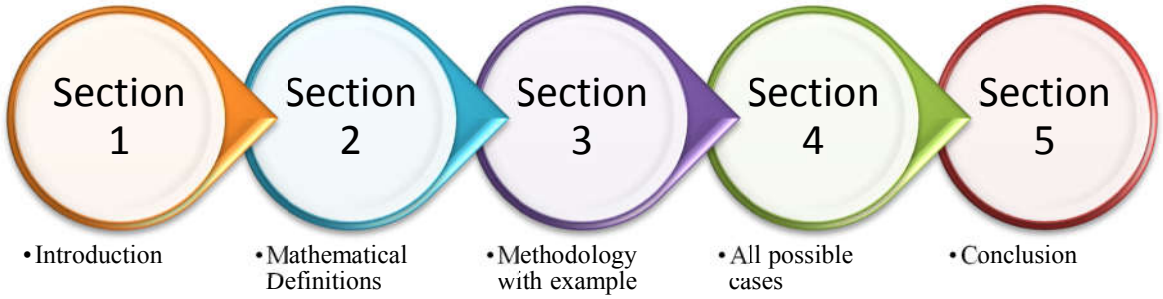
- Formation of Triangular Neutrosophic numbers Cryptography (TNNC) with detailed algorithm.
- Code Encryption as well as complete bank accounts encryption with budget amount.

DOI: 10.5281/zenodo.4127138

- ❖ Name of Persons for different situation also encrypted.
- ❖ Complete company data encrypted manually.

1.3 Structure of Paper

The article depends upon these following prospective.



2 Mathematical Definitions

Definition 2.1: Neutrosophic set: Set $\widetilde{n\dot{A}}$ is neutrosophic if $\widetilde{n\dot{A}} = \{\langle \tilde{x}; [\tilde{T}_{\widetilde{n\dot{A}}}(\tilde{x}), \tilde{I}_{\widetilde{n\dot{A}}}(\tilde{x}), \tilde{F}_{\widetilde{n\dot{A}}}(\tilde{x})]\rangle : \tilde{x} \in \tilde{X}\}$, where $\tilde{T}_{\widetilde{n\dot{A}}}(\tilde{x}) \longmapsto [0,1]$, $\tilde{I}_{\widetilde{n\dot{A}}}(\tilde{x})$ *and* $\tilde{F}_{\widetilde{n\dot{A}}}(\tilde{x})$ are membership functions of truth, indeterminacy and falsity with this following relation:

$$\mathbf{0}^- \leq \tilde{T}_{\widetilde{n\dot{A}}}(\tilde{x}), \tilde{I}_{\widetilde{n\dot{A}}}(\tilde{x}), \tilde{F}_{\widetilde{n\dot{A}}}(\tilde{x}) \leq \mathbf{3}^+$$

Definition 2.2: Triangular Neutrosophic Numbers: Single-value Triangular neutrosophic number is given as $\tilde{A}_{\widetilde{Neu}} = (\tilde{p}_1, \tilde{p}_2, \tilde{p}_3 : \tilde{r}_1, \tilde{r}_2, \tilde{r}_3)$ and their truth, indeterminacy and falsity membership is given as:

$$\tilde{T}_{\tilde{A}_{\widetilde{Neu}}}(\tilde{x}) = \begin{cases} \dfrac{\tilde{x} - \tilde{p}_1}{\tilde{p}_1 - \tilde{p}_2} & for\ \tilde{p}_1 \leq x < \tilde{p}_2 \\ 1 & when \quad \tilde{x} = \tilde{p}_2 \\ \dfrac{\tilde{p}_3 - \tilde{x}}{\tilde{p}_3 - \tilde{p}_2} & for\ \tilde{p}_2 < x \leq \tilde{p}_3 \\ 0 & otherwise \end{cases}$$

$$\tilde{I}_{\tilde{A}_{\widetilde{Neu}}}(\tilde{x}) = \begin{cases} \dfrac{\tilde{q}_2 - \tilde{x}}{\tilde{q}_2 - \tilde{q}_1} & for\ \tilde{q}_1 \leq x < \tilde{q}_2 \\ 0 & when \quad \tilde{x} = \tilde{q}_2 \\ \dfrac{\tilde{x} - \tilde{q}_2}{\tilde{q}_3 - \tilde{q}_2} & for\ \tilde{q}_2 < x \leq \tilde{q}_3 \\ 1 & otherwise \end{cases}$$

DOI: 10.5281/zenodo.4127138

$$\tilde{F}_{\tilde{A}_{\widetilde{Neu}}}(\tilde{x}) = \begin{cases} \dfrac{\tilde{x}-\tilde{p}_1}{\tilde{p}_1-\tilde{p}_2} & for\ \tilde{p}_1 \le x < \tilde{p}_2 \\ 1 & when \quad \tilde{x}=\tilde{p}_2 \\ \dfrac{\tilde{p}_3-\tilde{x}}{\tilde{p}_3-\tilde{p}_2} & for\ \tilde{p}_2 < x \le \tilde{p}_3 \\ 0 & otherwise \end{cases}$$

Where $0 \le \tilde{T}_{\tilde{A}_{\widetilde{Neu}}}(\tilde{x}) + \tilde{I}_{\tilde{A}_{\widetilde{Neu}}}(\tilde{x}) + \tilde{F}_{\tilde{A}_{\widetilde{Neu}}}(\tilde{x}) \le 3, \tilde{x} \in \tilde{A}_{\widetilde{Neu}}$

Parametric form is defined as: $(\tilde{A}_{\widetilde{Neu}})_{\tilde{\alpha},\tilde{\beta},\tilde{\gamma}}=\left[\tilde{T}_{\widetilde{Neu1}}(\tilde{\alpha}), \tilde{T}_{\widetilde{Neu2}}(\tilde{\alpha}): \tilde{I}_{\widetilde{Neu1}}(\tilde{\beta}), \tilde{I}_{\widetilde{Neu2}}(\tilde{\beta}): \tilde{F}_{\widetilde{Neu1}}(\tilde{\gamma}),\ \tilde{F}_{\widetilde{Neu2}}(\tilde{\gamma})\right]$, where,

$\tilde{T}_{\widetilde{Neu1}}(\tilde{\alpha})=\tilde{p}_1+\tilde{\alpha}(\tilde{p}_2-\tilde{p}_1), \tilde{T}_{\widetilde{Neu2}}(\tilde{\alpha})=\tilde{p}_3-\tilde{\alpha}(\tilde{p}_3-\tilde{p}_2)$, $\tilde{I}_{\widetilde{Neu1}}(\tilde{\beta})=\tilde{q}_2-\tilde{\beta}(\tilde{q}_2-\tilde{q}_1)$, $\tilde{I}_{\widetilde{Neu2}}(\tilde{\beta})=\tilde{q}_2+\tilde{\beta}(\tilde{q}_3-\tilde{q}_2)$, $\tilde{F}_{\widetilde{Neu1}}(\tilde{\gamma})=\tilde{r}_2-\tilde{\gamma}(\tilde{r}_2-\tilde{r}_1)$, $\tilde{F}_{\widetilde{Neu2}}(\tilde{\gamma})=\tilde{r}_2+\tilde{\gamma}(\tilde{r}_3-\tilde{r}_2)$, here $0<\tilde{\alpha} \le 1$, $0<\tilde{\beta} \le 1, 0<\tilde{\gamma} \le 1$ and $0 < \tilde{\alpha}+\tilde{\beta}+\tilde{\gamma} \le 3$.

Definition 2.3: Group is algebraic structure formed by:

¤ Set with element G.

¤ Closed operation on set G, as well as associative. Which is $(\tilde{a}.\tilde{b}).\tilde{c} = \tilde{a}.(\tilde{b}.\tilde{c})$, for $\tilde{a}, \tilde{b}, \tilde{c} \in G$.

¤ Identity element

¤ Availability of inverse under set operation

Group which have set operation commutative $(\tilde{a}.\tilde{b} = \tilde{b}.\tilde{a})$ defined as *abelian group.*

Here we have ''+'' as set operation and ''0'' as identity element. We gain a valid group by these prospective and by set of integers ''Z'', where pain of inverse and integers with opposite signs are used. With no inverse natural number ''N'' does not form a group.

Definition 2.4: With the operation (.) and $\tilde{a}$ be a element of group G with identity 1. Order of $\tilde{a}$ and it is of smallest integer $\tilde{n}$ such that:

$$\frac{\tilde{a}.\tilde{a}.\tilde{a}.\tilde{a}\ldots\tilde{a}}{\tilde{n}} = 1$$

Set $\{\tilde{a}, \tilde{a}^2, \tilde{a}^3, \tilde{a}^4, \ldots, \tilde{a}^{\tilde{n}}\}$ compose a cyclic subgroup of G with order $\tilde{n}$, here $\tilde{a}$ is g*enerator* for the subgroup.

3 Methodology with Example

Suppose the number in 0.97 as plain Text and the key for encryption is 0.21. The procedure depends upon following steps:

We have three values in Triangular fuzzy numbers.

Step 1

Add the key in second value of set:

{0.97,0.97,0.97} ⟼ add key (0.21) in second number ⟼ {0.97,1.18,0.97}

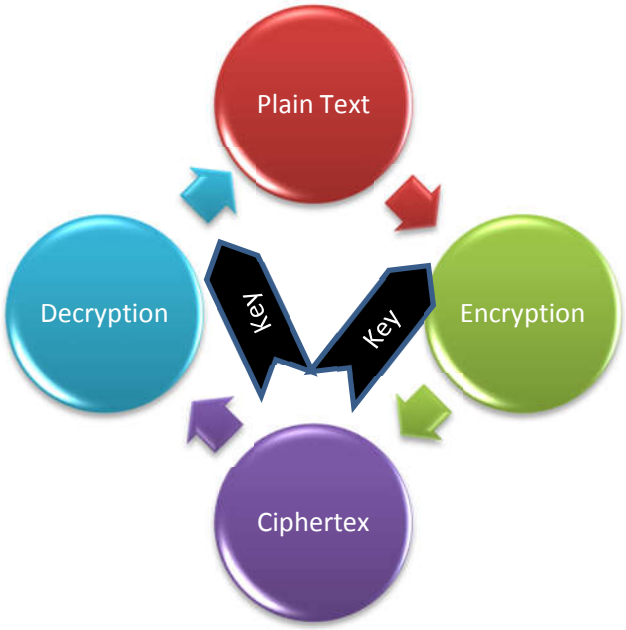
Step 2

DOI: 10.5281/zenodo.4127138

Apply formula $\frac{\tilde{a}_1+\tilde{b}_1+\tilde{c}_1}{3}$ for the process of encryption. The value after applying formula on above set is 1.04. In this case 1.04 is Cipher text.

Step 3 (Decryption)

For the process of Decryption, firstly multiply the Cipher text by 3 (Result 3.12), then subtract the key (Result 2.91) and finally divide the result by 3. Hence by this process we will get the plain text 0.97.



Security Analysis And Necessary Information

When we apply the key (methodology) then after applying the formula, it is impossible to move back to secure values without a key.

It's all up to you, which key you want to suppose. It's just like a simple pin code but all the encryption and decryption is only possible with pin code (key), which is unable to guess or break.

4 Case study

Few cases are given below, which mention the requirement of TNNC and show how the process proceeds with a few simple steps, key and done as maximum security.

4.1 Case 1: Code Cryptography

In this current era, cryptography is really familiar for privacy. Suppose the deal $\tilde{A}$ of a company depend on three different values: Account number as Truth. Range of amount for the deal depend upon Indeterminacy and Falsity. Put these values after zero.

Truth Indeterminacy Falsity

DOI: 10.5281/zenodo.4127138

$\tilde{A}$ ={(0.9878677721, 0.9878677721, 0.9878677721) (0.9700, 0.9700, 0.9700) (0.10999, 0.10999, 0.10999)}

Let Key = 0.9786

Encryption: Add the key in the middle value of all above:

$\tilde{A}$ ={(0.9878677721, 1.966467772, 0.9878677721) (0.9700, 1.9486, 0.9700) (0.10999, 1.08859, 0.10999)}

Apply Formula $\frac{\tilde{a}_1+\tilde{b}_1+\tilde{c}_1}{3}$ and get the result as:

$\tilde{A}$ ={(1.31406777207) (1.2962) (0.43619)} This is the **Cipher Text.**

Decryption: Multiply the Cipher text by 3:

$\tilde{A}$ ={(3.94220331621) (3.8886) (1.30857)}, Now Subtract the key:

$\tilde{A}$ ={(2.96360331621) (2.91) (2.32997)}, Now divide it by 3:

Truth Indeterminacy Falsity

$\tilde{A}$ ={(0.9878677721, 0.9878677721, 0.9878677721) (0.9700, 0.9700, 0.9700) (0.10999, 0.10999, 0.10999)}

Table for Case 2:

This table is designed to convert the alphabets of names in fuzzy values and this process is required because security is the main motto of this research article. This table is unique and specially designed by the author and the table is based on simple values, which are supposed. Once we convert the unique alphabets of names in fuzzy values, then we will be good to go and able to apply it on a few simple steps of triangular neutrosophic numbers.

$\breve{A}$ 0.01	$\breve{B}$ 0.02	$\breve{C}$ 0.03	$\breve{D}$ 0.04	$\breve{E}$ 0.05	$\breve{F}$ 0.06	$\breve{G}$ 0.07
$\breve{H}$ 0.08	$\breve{I}$ 0.09	$\breve{J}$ 0.10	$\breve{K}$ 0.11	$\breve{L}$ 0.12	$\breve{M}$ 0.13	$\breve{N}$ 0.14
$\breve{O}$ 0.15	$\breve{P}$ 0.16	$\breve{Q}$ 0.17	$\breve{R}$ 0.18	$\breve{S}$ 0.19	$\breve{T}$ 2.0	$\breve{U}$ 2.1
$\breve{V}$ 2.2	$\breve{W}$ 2.3	$\breve{X}$ 2.4	$\breve{Y}$ 2.5	$\breve{Z}$ 2.6		

4.2 Case 2: Communication Cryptography

Suppose a company is suffering from quick base action and decided to mention volunteer to deal with that critical situation. Two senior persons of company are communicating and the topic under discussion is ideal person, backup person and really not recommended person to deal with that situation.

DOI: 10.5281/zenodo.4127138

The three persons are William as ideal person (Truth), Mason as backup (Indeterminacy) and john not recommended for this situation (Falsity). Now convert the names in the form of numbers.

This methodology, consist of one more step: Convert the name into number. For this procedure, Convert the name into less letter. William $\mapsto \breve{W}\breve{L}\breve{M}$, Mason $\mapsto \breve{M}\breve{S}\breve{N}$ and John $\mapsto \breve{J}\breve{H}\breve{N}$. Know by the help of above table entertain them with numerical values. $\breve{W}\breve{L}\breve{M} \mapsto$ 2.3+ 0.12+ 0.13=2.55. $\breve{M}\breve{S}\breve{N} \mapsto$ 0.13+ 0.19+ 0.14=0.46 and $\breve{J}\breve{H}\breve{N} \mapsto$ 0.10+ 0.08+ 0.14=0.32.

Truth Indeterminacy Falsity

$\tilde{A}$ ={(2.55, 2.55, 2.55) (0.46, 0.46, 0.46) (0.32, 0.32, 0.32)}

Let Key = 0.77

Encryption: Add the key in the middle value of all above:

$\tilde{A}$ ={(2.55, 3.32, 2.55) (0.46, 1.23, 0.46) (0.32, 1.09, 0.32)}

Apply Formula $\frac{\breve{a}_1+\breve{b}_1+\breve{c}_1}{3}$ and get the result as:

$\tilde{A}$ ={(2.806666667) (0.7166666667) (0.5766666667)} This is the **Cipher Text.**

Decryption: Multiply the Cipher text by 3:

$\tilde{A}$ ={(8.42) (2.15) (1.73)}, Now Subtract the key:

$\tilde{A}$ ={(7.65) (1.38) (0.96)}, Now divide it by 3:

Truth Indeterminacy Falsity

$\tilde{A}$ ={(2.55,2.55,2.55) (0.46,0.46,0.46) (0.32,0.32,0.32)}

Finally compare the number with name, by the help of table as $\breve{W}\breve{L}\breve{M} \mapsto$ 2.55, $\breve{M}\breve{S}\breve{N} \mapsto$ 0.46 and $\breve{J}\breve{H}\breve{N} \mapsto$ 0.32.

4.3 Case 3: Graph Cryptography

Suppose a person want to be aware of online scam and want to save his personal company information manually. Here, with the help of one single key he can store multiple data manually with few single steps.

a) Progress per 10 days

The progress is 89%, 29% and 69%, on the base of 1000$. Add zero in front of numbers.

$\tilde{A}$ ={(0.89, 0.89, 0.89) (0.29, 0.29, 0.29) (0.69, 0.69, 0.69)}

Let Key = 0.77

Encryption: Add the key in the middle value of all above:

$\tilde{A}$ ={(0.89, 1.66, 0.89) (0.29, 1.06, 0.29) (0.69, 1.46, 0.69)}

Apply Formula $\frac{\breve{a}_1+\breve{b}_1+\breve{c}_1}{3}$ and get the result as:

DOI: 10.5281/zenodo.4127138

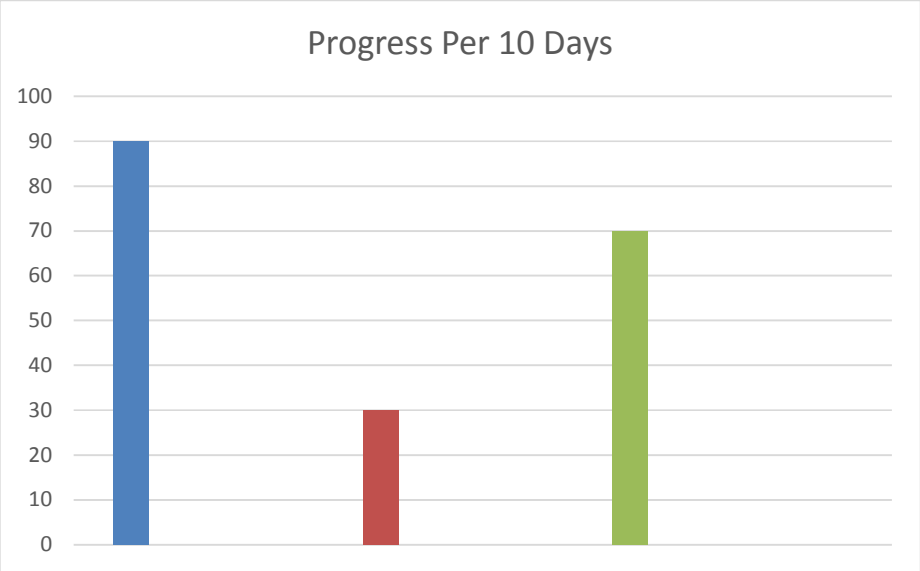
$\tilde{A}$ ={(1.146666667) (0.5466666667) (0.9466666667)} This is the **Cipher Text.**

Decryption: Multiply the Cipher text by 3:

$\tilde{A}$ ={(3.44) (1.64) (2.84)}, Now Subtract the key:

$\tilde{A}$ ={(2.67) (0.87) (2.07)}, Now divide it by 3:

$\tilde{A}$ ={(0.89, 1.66, 0.89) (0.29, 1.06, 0.29) (0.69, 1.46, 0.69)}



b) Budget

Now the most personal thing, need to hide is company budget, for this purpose we just have to follow these following steps. Firstly, convert it in percentage and then encrypt and decrypt it. The percentages are 39% as remaining, 42% and 19% are investment per 15 days.

$\tilde{A}$ ={(0.39, 0.39, 0.39) (0.42, 0.42, 0.42) (0.19, 0.19, 0.19)}

Let Key = 0.77

Encryption: Add the key in the middle value of all above:

$\tilde{A}$ ={(0.39, 1.16, 0.39) (0.42, 1.19, 0.42) (0.19, 0.96, 0.19)}

Apply Formula $\frac{\tilde{a}_1+\tilde{b}_1+\tilde{c}_1}{3}$ and get the result as:

$\tilde{A}$ ={(0.6466666667) (0.6766666667) (0.4466666667)} This is the **Cipher Text.**

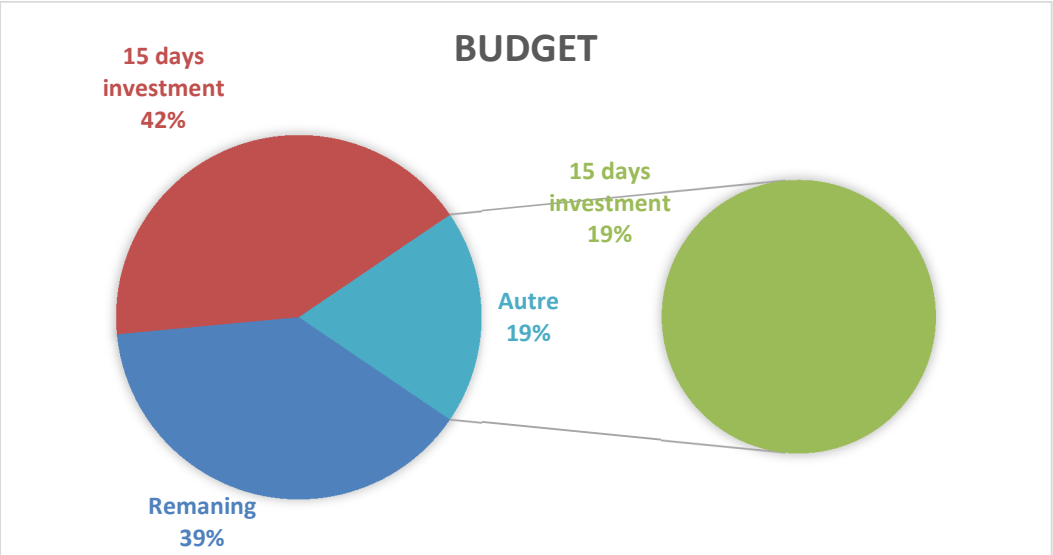
Decryption: Multiply the Cipher text by 3:

$\tilde{A}$ ={(1.94) (2.03) (1.34)}, Now Subtract the key:

$\tilde{A}$ ={(1.17) (1.26) (0.57)}, Now divide it by 3:

DOI: 10.5281/zenodo.4127138

$$\tilde{A} = \{(0.39, 0.39, 0.39) \quad (0.42, 0.42, 0.42) \quad (0.19, 0.19, 0.19)\}$$



c) Earning per 10 days

The progress is 899$, 299$ and 699$

$$\tilde{A} = \{(0.899, 0.899, 0.899) \quad (0.299, 0.299, 0.299) \quad (0.699, 0.699, 0.699)\}$$

Let Key = 0.77

Encryption: Add the key in the middle value of all above:

$$\tilde{A} = \{(0.899, 1.669, 0.899) \quad (0.299, 1.069, 0.299) \quad (0.699, 1.469, 0.699)\}$$

Apply Formula $\frac{\tilde{a}_1+\tilde{b}_1+\tilde{c}_1}{3}$ and get the result as:

$\tilde{A} = \{(1.155666667)\ (0.5556666667)\ (0.9556666667)\}$ This is the **Cipher Text.**

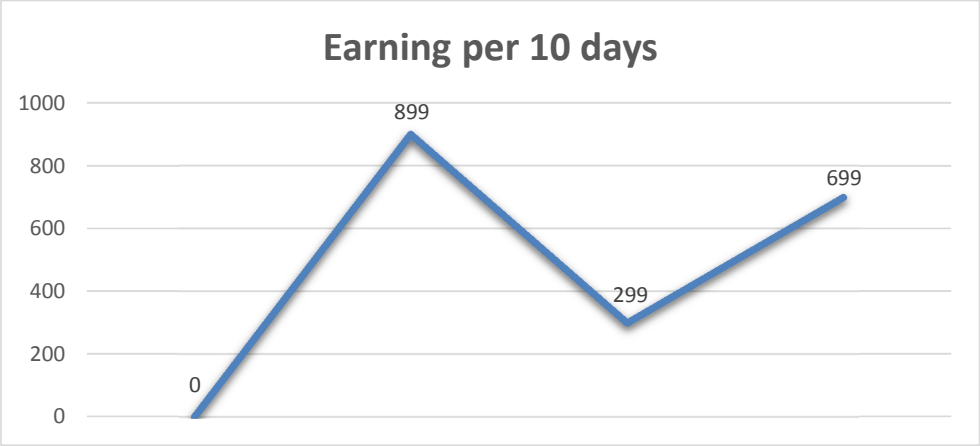
Decryption: Multiply the Cipher text by 3:

$\tilde{A} = \{(3.467)\ (1.667)\ (2.867)\}$, Now Subtract the key:

$\tilde{A} = \{(2.697)\ (0.897)\ (2.097)\}$, Now divide it by 3:

$$\tilde{A} = \{(0.899, 0.899, 0.899) \quad (0.299, 0.299, 0.299) \quad (0.699, 0.699, 0.699)\}$$

DOI: 10.5281/zenodo.4127138



Hence, by the help of TNNC, the complete data of company encrypted including progress, budget and earning as well as data depend upon three different parts.

Limitations

- All the calculations are basic and manual, hence image cryptography and sentence encryption are not possible yet.
- All the calculations are in regards to Triangular netrosophic numbers, so all the codes and values during the process lie between 0 and 3.
- Without the internet but with the help of reliable software like MATLAB, that kind of cryptography is possible and offline apps also developed for this procedure.

5 Conclusion

In this article, our main focus is to promote manual cryptography, which is more secure, less demanding and it is possible to create a personal record with a single key and by least step. All the necessary requirements and limitations of TNNC are also mentioned. Triangular neutrosophic numbers can be used in manual cryptography and now it is possible to create personal record secure manually with a single key. Cypher text is more secure, complex, and impossible to break without a key. The complete procedure of this new concept is available, and all possible personal records in regard to business or for any other condition now encrypted with few simple steps.

Acknowledgement: The authors are fully thankful to the respected Editor-in-chief as well as really great-full to their valuable comments and suggestions, which make this research better and reliable.

References

[1]. Delfs, H.and Knebl, H. Introduction to Cryptography Principles and Applications, *Springer*,2007.

[2] Daemen.J and V. Rijmen, The Design of RIJNDAEL: AES - The Advanced Encryption Standard, *Springer*, Berlin, Germany, 2002.

[3] H. Al-Assam, R. Rashid, and S. Jassim, "Combining steganography and biometric cryptosystems for secure mutual authentication and key exchange, "*in Proceedings of the 2013 8th International Conference for Internet Technology and Secured Transactions (ICITST '13)*, pp. 369–374, IEEE, London, UK, March 2013.

[4] A. Philip, "A generalized pseudo-Knight's tour algorithm for encryption of an image,"*IEEE Potentials,* vol.32,no.6,pp.10–16, 2013.

DOI: 10.5281/zenodo.4127138

[5] D. Bloisi and L. Iocchi, "Image based steganography and cryptography, "*in Proceedings of the 2nd International Conference on Computer Vision Theory and Applications''* (VISAPP'07), pp.127–134,Barcelona,Spain,March2007.

[6] H. Sharma, "Secure image hi dingal gorithm using cryptography and steganography, "*IOSR Journal of Computer Engineering*, vol. 13,no.5,pp.1–6,2013.

[7] J. Liu, H. Jin, L. Ma, Y. Li, and W. Jin, "Optical color image encryption based on computer generated hologram and chaotic theory, "Optics Communications,vol.307,pp.76–79,2013. [3] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol.28,no.4,pp.656–715,1949.

[8]. Bachman, D. J.; Brown, E. A.; Norton, A.H, Chocolate Key Cryptography*, Mathematics Teacher*, 104(2),2010, p100-104.

[9] J. Liu, B. Wei, X. Cheng, and X. Wang, "An AESS-box to increase complexity and cryptographic analysis," *in Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA '05),* pp. 724–728, Taipei, Taiwan, March2005.

[10] J. Rosenthal, "A polynomial description of the Rijndael advanced encryption standard*," Journal of Algebra and Its Applications*, vol.2,no.2,pp.223–236,2003.

[11]. Koç, Ç.K, Cryptographic Engineering, *Springer*, 2009, PP 125-128.

[12] K. Challita and H. Farhat, "Combining steganography and cryptography: new directions," *International Journal of New Computer Architectures and their Applications*, vol. 1, no. 1, pp. 199–208,2011.

[13] N. Ferguson, R. Schroeppel, and D. Whiting, "A simple algebraic representation of Rijndael," *in Selected Areas in Cryptography SAC'01, vol.2259 of Lecture Notesin Computer Science,* pp.103– 111, Springer, 2001.

[14] S. Murphy and M. J. Robshaw, "Essential algebraic structure within the AES," *in Advances in Cryptology—CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August18–22,2002 Proceedings, vol.2442 of Lecture Notesin Computer Science*, pp.1–16,Springer,Berlin, Germany,2002.

[15] L. Cui and Y. Cao, "A new S-box structure named affine-power affine, "*International Journal of Innovative Computing, Information and Control*, vol.3, no.3, pp.751–759,2007.

[16] L. Jingmei, W. Baodian, and W. Xinmei, "One AES S-box to increase complexity and its cryptanalysis*," Journal of Systems Engineering and Electronics*, vol.18, no.2, pp.427–433,2007.

[17] M. Khan and N.A. Azam, "Right translated AES gray S-boxes," *Security and Communication Networks*, vol. 8, no. 9, pp. 1627– 1635,2015.

[18] M. Khan and N.A. Azam, "S-boxes based on affine mapping and orbitofpowerfunction,"*3D Research*, vol.6, article12,2015.

[19] M.-T. Tran, D.-K. Bui, and A.-D. Duong, "Gray S-box for advanced encryption standard*," in Proceedings of the International Conference on Computational Intelligence and Security (CIS'08)*, pp.253–258, December2008.

DOI: 10.5281/zenodo.4127138

[20] Molodtsov, D.(1999). *Soft set theory - First results, Computers and mathematics with applications*. 37, 19-31.

[21] Zadeh, L.A. Fuzzy sets. *Inf. Control* **1965**, *8*, 338–353.

[22] Chang, S.S.L.; Zadeh, L.A. On fuzzy mappings and control. *IEEE Trans. Syst. Man Cybern.* **1972**, *2*, 30–34.

[23] Dubois, D.; Prade, H. Operations on fuzzy numbers. *Int. J. Syst. Sci.* **1978**, *9*, 613–626.

[24] Atanassov, K.T. *Intuitionistic Fuzzy Sets*; VII ITKR's Session: Sofia, Bulgarian, 1983.

[25] Smarandache, F. *A Unifying Field in Logics Neutrosophy: Neutrosophic Probability*; American Research Press: Rehoboth, DE, USA, 1998.

[26] F. Smarandache, Neutrosophic set, a generalization of the intuitionistic fuzzy sets, Inter. J. Pure Appl. Math. Vol.24 , pp. 287–297, 2005.

[27] Chakraborty, A.; Mondal, S. P.; Ahmadian, A.; Senu, N.; Alam, S.; and Salahshour, S.; Different Forms of Triangular Neutrosophic Numbers, De-Neutrosophication Techniques, and their Applications, Symmetry, vol 10, 327, 2018. ; doi:10.3390/sym10080327.

[28] Abdel-Basset, M., Atef, A., & Smarandache, F. A hybrid Neutrosophic multiple criteria group decision making approach for project selection. *Cognitive Systems Research*, vol 57, pp. 216-227, 2019.

[29] Abdel-Baset, M., Chang, V., & Gamal, A. Evaluation of the green supply chain management practices: *A novel neutrosophic approach. Computers in Industry*, vol 108, pp. 210-220, 2019.

[30] Abdel-Baset, M., Chang, V., Gamal, A., & Smarandache, F. An integrated neutrosophic ANP and VIKOR method for achieving sustainable supplier selection: *A case study in the importing field. Computers in Industry*, vol 106, pp. 94-110, 2019.

[31] Abdel-Basset, Mohamed, Mumtaz Ali, and Asma Atef. "Resource levelling problem in construction projects under neutrosophic environment." *The Journal of Supercomputing*, pp.1-25, 2019.

[32] Abdel-Basset, M., Manogaran, G., Gamal, A., & Smarandache, F. A group decision making framework based on neutrosophic TOPSIS approach for smart medical device selection. *Journal of medical systems*, vol 43(2), pp. 38, 2019.

[33] Abdel-Basset, M., Manogaran, G., Gamal, A., & Smarandache, F. A group decision-making framework based on the neutrosophic TOPSIS approach for smart medical device selection. *Journal of medical systems*, vol 43, issue 2, pp. 38-43, 2019.

[34] Abdel-Basset, M., Manogaran, G., Gamal, A., & Smarandache, F. A hybrid approach of neutrosophic sets and DEMATEL method for developing supplier selection criteria. *Design Automation for Embedded Systems*, pp.1-22, 2018.

[35] Abdel-Basset, M., Saleh, M., Gamal, A., & Smarandache, F. An approach of TOPSIS technique for developing supplier selection with group decision making under type-2 neutrosophic number. *Applied Soft Computing*, vol 77, pp. 438-452, 2019.

[36] Saqlain, M., Jafar, M. N., Riaz, M. "A New Approach of Neutrosophic Soft Set with Generalized Fuzzy TOPSIS in Application of Smart Phone Selection," *Neutrosophic Sets and Systems*, vol. 32, pp. 307-316, 2020. DOI: 10.5281/zenodo.3723161.

[37] Saqlain M, Jafar N, Hamid R, Shahzad A. "Prediction of Cricket World Cup 2019 by TOPSIS Technique of MCDM-A Mathematical Analysis*," International Journal of Scientific & Engineering Research*, vol 10(2), pp. 789-792, 2019.

[38] Saqlain. M, Jafar. N. M, and Muniba. K, "Change in The Layers of Earth in Term of Fractional Derivative: *A Study," Gomal University Journal of Research*, vol 34(2), pp. 1-13, 2018.

[39] Saqlain. M., Jafar. N. and Riffat. A., "Smart phone selection by consumers' in Pakistan: FMCGDM fuzzy multiple criteria group decision making approach," *Gomal University Journal of Research*, vol 34(1), pp. 27-31, 2018.

[40] Saqlain M, Saeed M, Ahmad M. R, Smarandache F, Generalization of TOPSIS for Neutrosophic Hypersoft set using Accuracy Function and its Application, *Neutrosophic Sets and Systems (NSS),* vol 27, pp. 131137, 2019.

[41] Wang, H.B.; Smarandache, F.; Zhang, Y.Q.; Sunderraman, R. Single Valued Neutrosophic Sets. Tech. Sci. Appl. Math. 2010. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.309.9470&re p=rep1&type=pdf (accessed on 31 July 2018).

[42] Ye, J. A multicriteria decision-making method using aggregation operators for simplified neutrosophic sets. J. Int. Fuzzy Syst., vol 26,pp. 2459–2466, 2014.

[43] P. Biswas, S. Pramanik, and B. C. Giri. "A new methodology for neutrosophic multi-attribute decision making with unknown weight information," *Neutrosophic Sets and Systems*, vol 3, pp. 42-52, 2014.

[44] Parimala ,M,. Karthika, M, Florentin Smarandache , Said Broumi, "On αω-closed sets and its connectedness in terms of neutrosophic topological spaces," *International Journal of Neutrosophic Science*, Volume 2 , Issue 2, pp. 82-88 , 2020.

[45] Riaz. M., Saqlain. M. and Saeed. M., "Application of Generalized Fuzzy TOPSIS in Decision Making for Neutrosophic Soft set to Predict the Champion of FIFA 2018: *A Mathematical Analysis," Punjab University Journal of Mathematics*, vol 51(8), pp.111-126, 2019.

[46] Riaz. M., Saeed. M. Saqlain. M. and Jafar. N, "Impact of Water Hardness in Instinctive Laundry System based on Fuzzy Logic Controller," *Punjab University Journal of Mathematics*, vol 51(4), pp. 73-84, 2018.

[47] Smarandache, F." Neutrosophy. Neutrosophic probability, set, and logic, ProQuest Information & Learning, *Ann Arbor, Michigan*, USA, 1998.

[48] Smarandache, F., Pramanik, S., "New Neutrosophic Sets via Neutrosophic Topological Spaces," *In Neutrosophic Operational Research; Eds.; Pons Editions: Brussels, Belgium*, vol I, pp. 189–209, 2017.

[49] S. Pramanik, P. P. Dey and B. C. Giri, "TOPSIS for single valued neutrosophic soft expert set based multiattribute decision making problems," *Neutrosophic Sets and Systems,* vol 10, pp. 88-95, 2015.

[50] T. Bera and N. K. Mahapatra, Introduction to neutrosophic soft groups, *Neutrosophic Sets and Systems*, vol 13, pp. 118-127, 2016. doi.org/10.5281/zenodo.570845.

[51] Chakraborty, A. "A New Score Function of Pentagonal Neutrosophic Number and its Application in Networking Problem," *International Journal of Neutrosophic Science*, Volume 1, Issue 1, pp. 40-51, 2020.

[52] Deli I, Broumi S. Neutrosophic soft matrices and NSM decision making, *Journal of Intelligent and Fuzzy System* vol 28, pp.2233–2241, 2015.

[53] Edalatpanah, S. A., "A Direct Model for Triangular Neutrosophic Linear Programming," *International Journal of Neutrosophic Science*, Volume 1, Issue 1, pp. 19-28, 2020.

[54] F. Smarandache, Neutrosophic set, a generalization of the intuitionistic fuzzy sets, *Inter. J. Pure Appl. Math*. Vol.24, pp. 287–297, 2005.

[55] I. Deli and S. Broumi, "Neutrosophic Soft Matrices and NSM-decision Making," *Journal of Intelligent and Fuzzy Systems*, vol 28(5), pp. 2233-2241, 2015.

[56] K. Mondal, and S. Pramanik. Neutrosophic decision making model of school choice. *Neutrosophic Sets and Systems*, vol 7, pp. 62-68, 2015.

[57] Ma YX, Wang JQ, Wang J, Wu XH. An interval neutrosophic linguistic multi-criteria group decision–making the method and its application in selecting medical treatment options, *Neural Computer Application*. DOI:10.1007/s00521-016-2203-1. 2016.

[58] A. Chakraborty, S. Broumi, P.K Singh, "Some properties of Pentagonal Neutrosophic Numbers and its Applications in Transportation Problem Environment*," Neutrosophic Sets and Systems*, vol.28, pp.200215, 2019.

[59] A. Chakraborty, S. Mondal, S. Broumi, "De-Neutrosophication technique of pentagonal neutrosophic number and application in minimal spanning tree," *Neutrosophic Sets and Systems*, vol. 29, pp. 1-18, 2019. doi: 10.5281/zenodo.3514383.