International Journal of Pure and Applied Mathematics
Volume 116 No. 3 2017, 711-715
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v116i3.17

FUZZY APPLICATION IN SECURED DATA TRANSMISSION

M. Muthumeenakshi[1], T. Archana[2], P. Muralikrishna[3] §

[1]Department of Commerce
VIT University
Vellore, 632014, Tamilnadu, INDIA

[2]School of Computer Science and Engineering
VIT University
Vellore, 632014, Tamilnadu, INDIA

[3]PG and Research Department of Mathematics
Muthurangam Government Arts College (Autonomous)
Vellore, 632002, Tamilnadu, INDIA

Abstract: The art or science encompasses the principles and methods of transforming an intelligible message into unintelligible, and then, retransforms that message back to its original form for more security. The objective is to develop simple, real time and secure system, which can be achieved through the software implementation. In this article, a fuzzy logic approach has been introduced to embed the encrypted message.

AMS Subject Classification: 68P25, 94A60
Key Words: encryption, decryption, fuzzy subset, fuzzy membership function

1. Introduction

Encryption can provide a fine solution for Cryptography. The encryption algorithm is the mathematical procedure for performing encryption on data. A key is used to cipher a message and to decipher it back to the original message. The implementation of these algorithms can be very intricate.

Received: June 12, 2017
Revised: September 28, 2017
Published: October 26, 2017

§Correspondence author

In 2009, Monisha[2] et.al discussed cryptographic application using quasi-group. Then, Vineet Sukhraliya[5] et. al studied Encryption and Decryption Algorithm using ASCII values. Recently, Wael Mahmoud[6] and Yamuna[4] et. al have used the graph theory technique for data transferring. Chandrasekaran[1] et. al dealt Cryptography using a pair of dice in 2015. After conducting a research on currently using such encryption algorithms, it is identified that all these algorithms concern only about security.

The proposed algorithm supports user with desired security level and processing level. The algorithm provides security levels and their corresponding processing levels by using various keys for the encryption/decryption process. This facility is achieved by using fuzzy logic proposed by Zadeh[7].

The aim of the present research is to come up with an encryption algorithm, which provides either low processing or high security according to user's requirement and it will be more advanced than the existing encryption algorithms.

2. Preliminaries and Notations

In this section, the notion of fuzzy subset and the information of a sample space of 2- dice are provided for encryption.

2.1 Fuzzy subset: A fuzzy subset in a non-empty set X is a function $\mu : X \to [0, 1]$.

2.2 Notations of dice: Let (a, b) denote the possible outcome of rolling the two dice, with a is the outcome from the first die, b is the outcome from the second die and which are the integers from 1 to 6. There are 36 possibilities for (a, b). The set of all possible outcomes is called the sample space.

3. Proposed Encryption Algorithm

In this section an algorithm has been proposed by using fuzzy membership values on sample space of 2-dice.

Algorithm:

STEP 1. A pair of dice was rolled and obtained a joint outcome. The outcome has been assigned with alphabets from A to Z and 0 to 9 accordingly.

(a,b)	***1***	***2***	***3***	***4***	***5***	***6***
1	A	B	C	D	E	F
2	G	H	I	J	K	L
3	M	N	O	P	Q	R
4	S	T	U	V	W	X
5	Y	Z	0	1	2	3
6	4	5	6	7	8	9

Table-1

STEP 2. The joint outcomes are converted into fuzzy membership value by using the fuzzy membership function $\mu : (a,b) \to [0,1]$ such that $\mu(a,b) = \frac{10a+b}{66}$. The converted outcomes are listed below in a fuzzy membership table.

(a,b)	***1***	***2***	***3***	***4***	***5***	***6***
1	0.167	0.182	0.197	0.212	0.227	0.242
2	0.318	0.333	0.348	0.364	0.379	0.394
3	0.470	0.485	0.500	0.515	0.530	0.545
4	0.621	0.636	0.652	0.667	0.682	0.697
5	0.773	0.788	0.803	0.818	0.833	0.848
6	0.924	0.939	0.955	0.970	0.985	1.000

Table-2

The fuzzy membership value is considered as 0.000 for an empty space .

STEP 3. To strengthen the secrecy, each data are multiply by 1000.

STEP 4. The decryption of the secret can be made by dividing the data by1000 and defuzzification the membership function is done by using the formula $\mu^{-1}(r) = \frac{66r}{10}$ where $r \in [0, 1]$ and the pair (a,b) can be identified using the quotient and the remainder of $\mu^{-1}(r)$.

4. Verification

In this section the proposed algorithn is verified by an exapmle for encryption and decryption.

4.1. Example for Encryption

Consider the chemical acid **HYDROBROMIC ACID**.
Using the present algorithm HYDROBROMIC ACID is encripted as
333 773 212 545 500 182 545 500 470 348 197 000 167 197 348 212.

4.2. Example for Decryption

Now, to decrypt a given code:
197 500 182 167 394 636 000 621 652 394 242 348 212 227

By dividing each code by 1000, the given code will be converted as a fuzzy membership value as given in Table-2

0.197 0.500 0.182 0.167 0.394 0.636 0.000 0.621 0.652 0.394 0.242 0.348 0.212 0.227

The above mentioned fuzzy membership value can be converted into integer values respective to the elements of the sample space of 2-dice as follows,

13 33 12 11 26 42 41 43 26 16 23 14 15

If the joint outcomes are converted into corresponding alphabets, it will become **COBALT SULFIDE**.

5. Conclusion

In this paper, the outcomes of a pair of dice have been converted into the respective characters and digits. These joint outcomes are modified into fuzzy membership values by using a suitable fuzzy membership function. The sender encrypts the data and the receiver will decrypt the message by converting the given codes into fuzzy membership values which are given in Table-2. This fuzzy membership values can be transformed into characters and numbers. In future, this concept can be explored by comparing the results of the proposed encryption algorithm with other existing encryption algorithms.

Acknowledgements

The authors would like to convey their warm gratitude to Dr.A.Manimaran, SAS, VIT University for his insightful and constructive support that led to an improved version of this paper.

References

[1] Chandrasekaran. V.M. , Manimaran, A and Akhil Ranjan, Cryptography using a pair of dice, *International Journal of PharmTech Research, (2015) 7(1), 85-89.*

[2] Monisha S and Kowar MK, Generation of quasigroup for cryptographic application. *Indian Journal of Science and Technology, (2009) 2(11), 356.*

[3] Narander Kumarand Priyanka Chaudhary, Performance Evaluation of Encryption/Decryption Mechanisms to Enhance Data Security, *Indian Journal of Science and Technology, (2016) 9(20), 1-10.*

[4] Yamuna.M and Karthika.K, Data Transfer using bipartite graph, *International Journal of Advance Research In Science And Engineering, (2015) 4(2), 128-131.*

[5] Vineet Sukhraliya , Sumit Chaudhary and Sangeeta Solanki, Encryption and Decryption Algorithm using ASCII values with substitution array Approach, *International Journal of Advanced Research in Computer and Communication Engineering, (2013) 2(8), 3094-3097.*

[6] Wael Mahmoud Al Etaiwi, Encryption Algorithm using Graph Theory, *Journal of Scientific Research & Reports, (2014) 3(19), 25192527.*

[7] Zadeh L.A, Fuzzy Sets, *Inform Control, (1965) 8, 338-353.*