Indian Journal of Science and Technology, *Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/108970, December 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

New Cryptography Algorithm with Fuzzy Logic for Effective Data Communication

K. GaneshKumar[1*] and D. Arivazhagan[2]

[1]IT Department, AMET University, Kanathur, Chennai - 603112, Tamil Nadu, India; ganeshsvcet@gmail.com
[2]Department of E-Governance, AMET University, Kanathur, Chennai - 603112, Tamil Nadu, India; arivazhagand@hotmail.com

Abstract

In this communicative world, people forget to care about the security when the data communication gets the importance than the privacy most of the time. There the data theft takes place effortlessly. Many methodologies have been devised for making the effective communication either over the internet or intranet. However, the hackers enrich themselves than the new technologies whenever are launched. As need arises for cultivate the security key generation while secure data communication has to be ensured, we propose a new cryptography algorithm along with the fuzzy logic through this paper that materializes the secure communication possible. Firstly, we observed the flaw that causes for hacking effortlessly by the intruder during the data transmission over the network. Then the evaluation part could be done with the same context without losing data because of this proposed algorithm. This algorithm concentrates on image and text data encryption using fuzzy logic and on secured sharing theme which provides highly authenticated data transferring. The existing security algorithms had nod in many ways only for the secure data transmission rather than the complexity in which they have when need to be executed. Henceforth the aspirants who want to have the communication have to spend more time than the actual. Obviously the precious algorithms should have less processing time and high secure in nature. With keeps it as a main aspect the New Cryptography algorithm with fuzzy logic is proposed and has low process time and high security logics using various key for encryption and decryption. The results which produced by this proposed algorithm have been compared with exist algorithms and finally could arrive the conclusion that the proposed is highly effective in security aspects and needs minimum amount of time to be executed.

Keywords: Cryptography, Fuzzy Logic, Private Key, Public Key, RSA Algorithm, Security Key

1. Introduction

Everyone using computers all around the world irrespective of age and qualifications that not only for commercial but also for personal purposes[1,2]. Even the new born babies may seek their tablets as their very first activity in this world in near future. Technology doesn't have the limit even after gone to appreciable high within the last six to seven decades. As technology improves, the crime also increases in all sectors. In order to avoid this kind of crimes users had to meticulously keep active the traditional methods such as stopping additional services, updating the antivirus[3] in frequent intervals, providing the security by installing firewalls and concentrating on parental controls[4,5]. However, data confidentiality is not guaranteed and sometimes data could be stolen even in traditional computer security. There is an alternate way of solving this kind of cyber-crime issues[6] which is known as cryptography technology[7]. This is the powerful technology which can take control of both nodes and mediums and doesn't allow the hacker or theft to steal the information without the security key. This Cryptography technology plays a vital role both on sender and receiver sides while encrypt and decrypts the data as well. There are lot of cryptography algorithms exist for encrypting and decrypting the data during the data transmissions in last

*Author for correspondence

two decades. Even though the cryptography is evolved for providing tight security in data communication, there is lots of cyber-crime issues have been arisen with the development of advance technology and the same is focusing to use for malfunctions. Probably the technology which was derived for providing security in communication started to face somewhat failures. Without enriching the technology, it is not possible to avoid these kinds of issues and finally it led to the solution of providing the high security by evaluating new cryptography technology with fuzzy set[8], which is proposed here. A set of rules has been introduced for the process of encryption & decryption as a part of proposing new cryptography algorithm which is incorporated with fuzzy set. Fuzzy logic is the power full tool to Modeling and controlling the uncertain inputs[9]. The main objective of this paper is to enforce the security level in the data communication with a new encryption algorithm based on the public and private keys which are generated not by the algorithm but by fuzzy logic in server side. By generating the key with fuzzy set it is possible to achieve the objective to provide the high security in communication that is not been possible by the mere cryptography technology[9].

2. Methodology

As a part of the objective of this proposed paper the below algorithms are formulated to generate server public and private keys for both encryption and decryption[10].

2.1 Generating Server Public and Private Key

Step 1: Take any two prime numbers
X=3 and Y=11
Step 2: Calculate n (product of X and Y)
3*11=33
Step 3: Calculate A=(X-1)*(Y-1)
=(3-1)-(11-1)
=20
Step 4: Choose a Number D=7(D is a prime number; d should not divide by A)
Step 5: R=33 and D=7 this are the server Public key
Step 6: Server Private Key
D*I=1(mod A)
7*i=1(mod A)
7*i/20=? With remainder of 1
21/20 it has the remainder of 1
7*i/20= 21/20
7*i=21
I=3 Server Public key

2.2 Encrypting the Plain Text

Step 1: P^D=E(mod R)
P=the Plain text
R, D =Server public key
E= Encrypted message we want to Generate
Step 2: 14^7=E (mod 33)
Step 3: 105413504/33=3194348.606
3194345*33=105413458
E=105413504-10541348=20
Step 4: Encrypted message E=20

This value only sends by the client to the server and the server will decrypt the message as follows.

2.3 Decrypting the Plain Text

Step 1: E^i=P (mod n)
E=Encrypted Message
I=Server Secret Key
P=Plain text we want to recover
R=Server Public Key
Step 2: 20^3=P (mod 33)
8000/33=? With the remainder of P.
8000/33242.424242
242*33=7986
P=8000-7986=14
Step 3: The Plain text P=14

2.4 Issues in the RSA Algorithm

a) Generating a secure Public key is a tedious one
b) The keys such as R,N,A,I are computed from X and Y. So that the unauthorized users can easily hack the keys. Finally, it leads to data loss.

For instance, R = X * Y

c)There is a familiar arithmetic relation between the public and private keys. Yield, anyone could identify the key if he comes to know any one of the keys[11].

3. Fuzzy Logic

This is the method which reasoning that same as human reasoning, it involves and intermediates possibilities between digital values 0 and 1. It can be implemented both in hardware and software[12]. If we consider yes and

no are two Boolean values, the fuzzy logic takes certainly yes, possible yes, cannot say, possible no, certainly no. It helps to deal with the uncertainty in engineering.

Step 1: Define the Variables [Public and Private Key]

Step 2: Generate Fuzzy Set Using Membership function (fuzzification)

Step 3: Combine the results (Inference Engine).

Step 4: Convert the data in to non-fuzzy values (Defuzzification)

The steps are shown in Figure 1.

4. Fuzzy Logic System Architecture

Step 1: Define the fuzzy set.

It transfers the input into fuzzy set or fuzzy members such as,

LP=Large Positive
MP=Medium Positive
S=Small
MN=Medium Negative
LN=Large Negative

For instance, if we generate the public key 14, the fuzzy logic will generate a fuzzy set like

Key(R)= 13.8,13.9,14,14.1,14.2.

Step 2: Build Membership function for variables

In inference engine, we are using If-Then Rules to stimulate the human reasoning. Inside the Fuzzy inference the logical operators and three important functions are used that are AND, OR, NOT, MIN, MAX. The Tables 1–3 are shown how the operators are run[13].

Table 1. AND, Min Operator

A	B	A AND B	MIN(A,B)
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	1

Table 2. Or, Max operator

A	B	A OR B	MAX(A,B)
0	0	0	0
0	1	1	1
1	0	1	1
1	1	1	1

Table 3. Not, Compliment Operator

A	NOT A	1-A
0	1	1
1	0	0

The Truth table give the same results in logical operators and functions,

MIN(A,B) resolves Set A AND B
MAX(A,B) resolves Set A OR B
NOT A equalent for 1-A(Complement)

If we take fuzzy Variable for our Cryptography Purpose the below method is used in the Fuzzy Inference.

Not X=(1-Truth(x))
X and Y =MIN(TRUTH(x),TRUTH(Y))
X OR Y =MAX(TRUTH(x),TRUTH(Y))

The steps to create the rule base is

IF Number = (13.9 OR 13.8) AND Target=14 THEN

IF Number=(14.1 OR 14.2) AND Target=14 THEN

If Number =(14) AND(Target=14)

The Inference Engine Generate a Fuzzy Matrix for Inputs shown in Table 4.

Step 3: Combine the Results

The fuzzy members' values (Fuzzy Set) perform evaluating the I-Then Rules. The operations used OR, AND, MAX, MIN Creating a final result from combine all the results, the result is called fuzzy value.

Step 4: Convert the data in to non-fuzzy values (Defuzzification).

Table 4. Fuzzy matrix

Key Target	13.8	13.9	14	14.1	14.2
13.8	No change	Add	Add	Add	Add
13.9	Subtract	No change	Add	Add	Add
14	Subtract	Subtract	No change	Add	Add
14.1	Subtract	Subtract	Subtract	No change	Add
14.2	Subtract	Subtract	Subtract	Subtract	No change

Defuzzification done by the output variables from membership function[14]

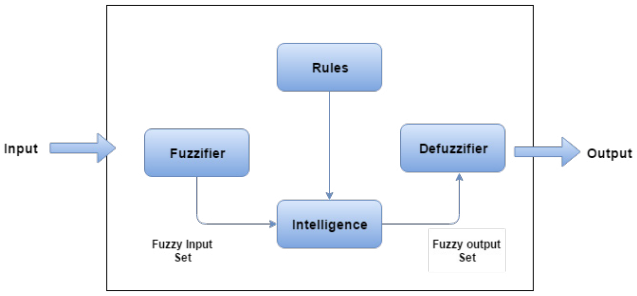

Figure 1. Block diagram of Fuzzy algorithm.

5. Proposed Encryption with Fuzzy Logic

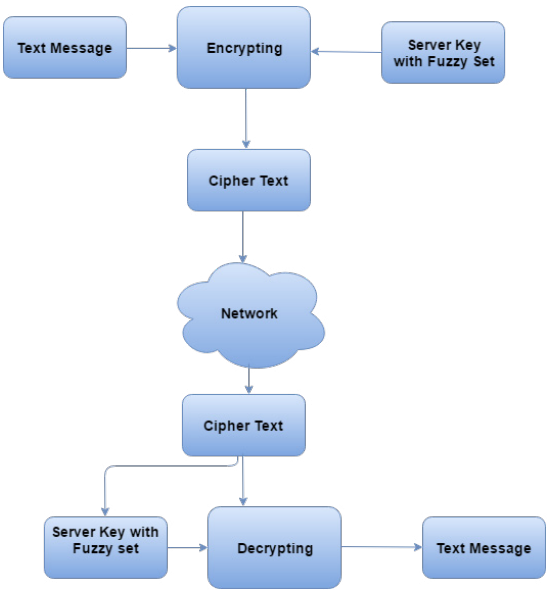

Figure 2. Block diagram of encryption with fuzzy logic.

6. Key Generation

Step 1: Generate two large prime numbers X and Y
Step 2: Let R= X Y
Step 3: Let m=φ(R) =(X-1)(Y-1)
Step 4: Choose a small prime number E, co-prime to m, with GCD(φ(n),E)=1
1<E<φ(n)
Step 5: Find D, such that D mod φ(R)=1 publish E and R as the public key keep D and M as the secret key.
Step 6: Apply fuzzy set to private key.
Step 7: Provide fuzzy encryption key to encrypt
Step 8: Encryption->Chipper=(message)^e mod R
Step 9: Decryption Message=(chipper)^d mod n

7. Result and Discussion

To distinguish the performance of this proposed new cryptography algorithm, in this section the results were compared with existing relevant cryptography algorithms in all aspects. The popular secret key algorithms such as DES, RSA and Blowfish were taken in account, and their performances were compared by encrypting the input files which are different both in content and sizes[15]. In spite of these three the RSA algorithm has more impact than other two algorithms in time consumption aspect while encrypting and decrypting the data. Henceforth, the RSA algorithm has been taken with this new proposed algorithm for assessing the optimization. Table 5 contains the speed benchmark comparison between New Cryptography algorithm and most commonly used RSA cryptography algorithm and the actual time variations also have been plotted. Meanwhile Figure 3 represents the graphical representation of comparative algorithms and from this result it is easy to observe that the fuzzy set incorporated algorithm has more advantages than the other algorithms in terms of Throughput, Data transmission speed, Data perseverance, Data confidentiality, and so on.

Table 5. Comparison according to time

Key	Key Length	Cycles	RSA Algorithm Time Taken(ms)	New Cryptography Algorithm Time Taken(ms)
a	16	5	5.95	2.25
ab	32	10	6.95	3.15
abc	48	15	7.1	3.3
abcd	64	20	8.5	4.4
abcde	80	25	9.6	4.3
abcdef	96	30	10.1	5.2

7.1 Evaluating the Performance

This section describes the complete execution part of this work along with the existing methods in same circumstance to evaluate the performance in single hand. The

followings are the requirements behind for developing an application which carries new Cryptography technology[16].

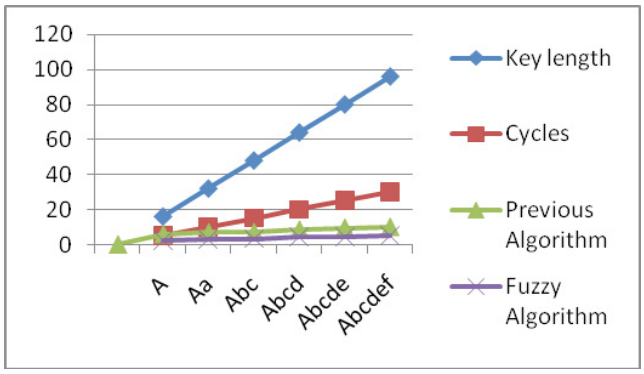

Figure 3. Graphical representation of effectiveness.

7.2 System Parameters

The application needs at least 32-bit dual core processor,1 GB RAM, 160GB Hard Drive and windows based environment to run. The program classes are compiled by the default java 7 interface supported by windows based NetBeans 8.

7.3 Execution Procedure

The algorithms were evaluated by letting the different sizes of data blocks (0.5MB to 20MB) into the application for checking out with all optional algorithms one by one and the performances were noted individually in terms of time requirements to encrypt and decrypt the data blocks. The appreciable consistent differences could be found by doing the data transmission process repeatedly. Based on the differences the reliability of this proposed New Cryptography Technology is drawn in chart along with the existing as proof and the algorithm's consistency also was proved by transmitting data in various type through this application in so many times.

7.4 Value Added Features

Though the comparison concentrates only upon time aspect as deliberated so far, this algorithm's advantages extend up to the feature of bulk data transmission as well as robust in secure key generation. So this new cryptography algorithm incorporates fuzzy set has strong evidence in terms of optimality and reliability in data transmission. Besides Figure 4 is a snap of the algorithm running in backdrop along with all other exists[17].

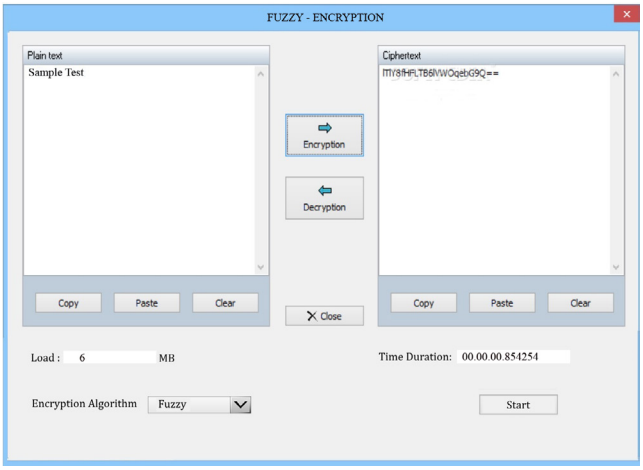

Figure 4.

8. Conclusion

The importance of such kind of encryption algorithm rapidly increases nowadays. So we developed an effective encryption algorithm with fuzzy sets key generation method. In spite of fuzzy incorporation, we could get the secure and optimal communication done in the transmission of data among the systems over inter and intranets. For keys generation on encrypt and decrypt the information both at client and server sides we used fuzzy logic that makes to have a robust security against the cyber-attacks and the intruders those who want to steal data[18]. Finally, the proposed algorithm was done by materializing with the code and got the result as we expected as optimal and the same was taken to compare with reputed existing related algorithms.

9. Reference

1. Ministry of science, technology and innovation, Malaysia. National Cyber Security Policy: The Way Forward, Federal Government Administrative Centre; 2006.
2. UK Office of Cyber Security. Cyber security strategy of the United Kingdom: Safety, security and resilience in cyber space, Office of Public Sector Information, Information Policy Team; 2009.
3. United State, executive office of the president. Cyber space policy review: assuring a trusted and resilient information and communication infrastructure. United State, Executive Office of the President; 2009.
4. Ganeshkumar K, Arivazhagan D, Sundaram S. Strategies of cybercrime: Viruses and security sphere. Journal of Academia and Industrial Research. 2013; 2(7):397–401.

5. Ganeshkumar K, Arivazhagan D, Sundaram S. Advance cryptography algorithm for symmetric image encryption and decryption scheme for improving data security. Journal of Academia and Industrial Research. 2014 Mar; 10(2):563–6.
6. Mikle O. Practical attacks on digital signatures using MD5 message digest. CryprologyePrint Archive; 2004. p. 356.
7. Sun Q, Chang SF. A secure and robust digital signature scheme for JPEG2000 image authentication. IEEE Transactions on Multimedia. 2005; 7(3):480–94.
8. Cramer R, Shoup V. Signature schemes based on the strong RSA assumption. ACM Transactions on Information and System Security (TISSEC). 2000; 3(3):161–85.
9. Noore A. A secure conditional access system using digital signature and encryption. IEEE International Conference on Consumer Electronics, ICCE; 2003.
10. Stern J, Pointcheval D. Flaws in applying proof methodologies to signature schemes. Advances in CRYPTO; 2002. p. 215–24.
11. Aydos M, Yantk T. A high-speed ECC-based wireless authentication on an ARM microprocessor. 16th Annual Conference on Computer Security Applications, ACSAC'00; 2000.
12. Shah M, Swaminathan AR. Privacy-preserving audit and extraction of digital contents. Cryptology ePrintArchive, Report 186; 2008.
13. Ding J, Yang BY. New differential-algebraic attacks and reparametrization of rainbow. Applied Cryptography and Network Security; 2008.
14. Tao R, Meng XY, Wang Y. Image encryption with multiorders of fractional fourier transforms. IEEE Transactions on Information Forensics Security. 2010; 5(4):734–8.
15. Wang XY, Yang L, Liu R, Kadir A. A chaotic image encryption algorithm based on perceptron model. Nonlinear Dynamics. 2010; 62(3):615–21.
16. Wang Y, Wong KW, Liao X, Chen G. A new chaos-based fast image encryption algorithm. Applied Soft Computing - Journal. 2011; 11(1):514–22.
17. Zaidan B, Zaidan A, Al-Frajat A, Jalab H. On the differences between hiding information and cryptography techniques: An overview. Journal of Applied Sciences. 2010; 10:1650–5.
18. Zhang G, Liu Q. A novel image encryption method based on total shuffling scheme. Optics Communications. 2011; 284(12):2775–80.
19. Zhao XY, Chen G. Ergodic matrix in image encryption. Second International Conference on Image and Graphics. 2002 Jul 26:394. DOI: 10.1117/12.477171.
20. Zhu ZL, Zhang W, Wong KW, Yu H. A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences. 2011; 181(6):1171–86.
21. Lakhtaria K. Protecting computer network with encryption technique: A Study. International Journal of Environmental Science and Technology. 2011; 4(4):44–51.