Int. J. Pure Appl. Sci. Technol., 8(2) (2012), pp. 47-53

International Journal of Pure and Applied Sciences and Technology

ISSN 2229 - 6107

Available online at ***www.ijopaasat.in***

Research Paper

Generating Ciphertext Using Systems of Equations: An Asymmetric Key Approach

P.B. Zirra[1,*], G.M. Wajiga[2] and S. Boukari[3]

[1]Department of Mathematical Sciences, Adamawa State University, Mubi, Nigeria
[2]Department of Mathematics and Computer Science, Modibbo Adama University of Technology, Yola, Nigeria
[3]Mathematical Sciences Programme, Abubakar Tafawa Balewa University Bauchi, Nigeria

* Corresponding author, e-mail: (zirrapeter@yahoo.com)

(Received: 18-1-12; Accepted: 10-2-12)

Abstract: *The goal of cryptography is to provide confidentiality and privacy by scrambling information. If this information can be deciphered by unauthorized persons then this goal is defeated. In this paper we present a framework that allows cryptography to inherit some features from systems of nonlinear equations in such a way that the information is secured against brute force attack and differential crypto-analysis. The proposed method uses systems of nonlinear equations cryptography to establish a trusted link between two parties (the sender and the receiver) to disguise text and provide enhanced confidentiality and privacy in personal communication.*

Keywords: Asymmetric key, Brute force attack, Cryptography, Systems of nonlinear equations.

1. Introduction

Cryptography is the art and science of scrambling information. It has an extensive and mesmerizing history, and there is evidence that the Egyptians used cryptography about 4000 years ago in Forouzans' study [1]. Information scrambling has become an imperative in the Internet world and has the top priority use in e-commerce, e-banking, e-mail, medical databases and so many more.

Since the cryptosystem developed in this paper is based on the principle of the systems of nonlinear equations, it is presented briefly hereunder.

1.1 Systems of Linear and Nonlinear Equations

A nonlinear system of equation is defined by [2] and [3] as

$$\left.\begin{aligned} f_1(x_1, x_2, x_3, \cdots, x_n) &= 0 \\ f_2(x_1, x_2, x_3, \cdots, x_n) &= 0 \\ &\vdots \\ f_n(x_1, x_2, x_3, \cdots, x_n) &= 0 \end{aligned}\right\} \tag{1}$$

This system can be compressed as $F(X) = 0$, where $F = (f_1, f_2, f_3, \dots, f_n)^t$ and $X = (x_1, x_2, x_3, \dots, x_n)^t$. from the n-dimensional space $\Re^n$ into $\Re$. [4] assume that the system admits a unique solution.

There are several ways to solve systems of nonlinear equations (1), but the most widely used iterative method for solving such equations is the classical Newton's method as discussed in [5]. The nonlinear problems are often treated numerically by reducing them to sequence of linear problems [2].

2. The Problem

This paper addresses the problem of individual privacy and confidentiality in data communication. In order to describe some of the aspects involved, we refer to the following scenario: Consider a situation in which the encrypted information is intercepted by an authority, and subsequently the sender is coerced to reveal the keys that generated the cipher-text; the result of which is that the content of the message sent is revealed. This scenario high-lights a few key issues, namely: how to protect sender's privacy, how to provide more confidentiality and how to conceal communication. The immediate logical solution is to use systems of nonlinear equations. In Williams; Wiener; Menezes, Ooschot, & Vanstone; Boneh; Obi; Schneier; Young & Yang; Murphy; Stallings; Goh; Yusuf; Kaks' study (as cited in [5]), we understand that other existing cryptographic applications can be used, but we also realized that the keys can easily be detected or broken.

In this paper we present a solution which tries to solve some of these key issues. Our aim here is to offer that disguising component to cryptography to enhance personal privacy and confidentiality.

Since this paper only describes our solution to the conceptual framework, a comprehensive algorithm is not offered.

3. Asymmetric Key Distribution

Asymmetric key cryptography needs not to share secret key between two parties. Asymmetric keys can be much more secure than symmetric since it avoids the mechanism of key sharing. The message that is sent through the channel is called the ciphertext. To create the ciphertext from the plaintext, an encryption algorithm is used with the secrete key (public key). To create the plaintext from ciphertext, a decryption algorithm is used with another key called the private key. The resistance of the ciphertext to attack should be dependent only on the secrecy of the key and mathematical soundness of the algorithms.

4. Suggested Framework

In order to make the cryptosystem a practical robust system, the proposed algorithm uses the following:

a) Encryption Rules:

i. Take the plaintext.
ii. Scan the plaintext and delete any repeated words.
iii. Count the number of words left over after the discard of repeated words to produce the public key using the algorithms in [5].
iv. Assign a variable index to each character position in a word. If characters are equal, assign the variable index of its previous occurrence.
v. Then transform each word into the form of equation (1) based on the number of public key and sums the like terms together.
vi. Send the ciphertext (systems of nonlinear equations) to the intended receiver in a carrier file using delta encoding principle.
vii. Get to the intended receiver the decryption key through a different Media.

b) **Decryption Rules:**

i. Obtain the ciphertext from the sender.
ii. Solve the ciphertext using the method in [5].
iii. Get the associated hexadecimal ASCII alphanumeric position table from the sender.
iv. Add the variable solution of each character to the (iii).
v. Get the variable position’s representation from the sender.
vi. Obtain the index values of the words previously discarded during the compression processes.
vii. Then decrypt the ciphertext using the secret keys.

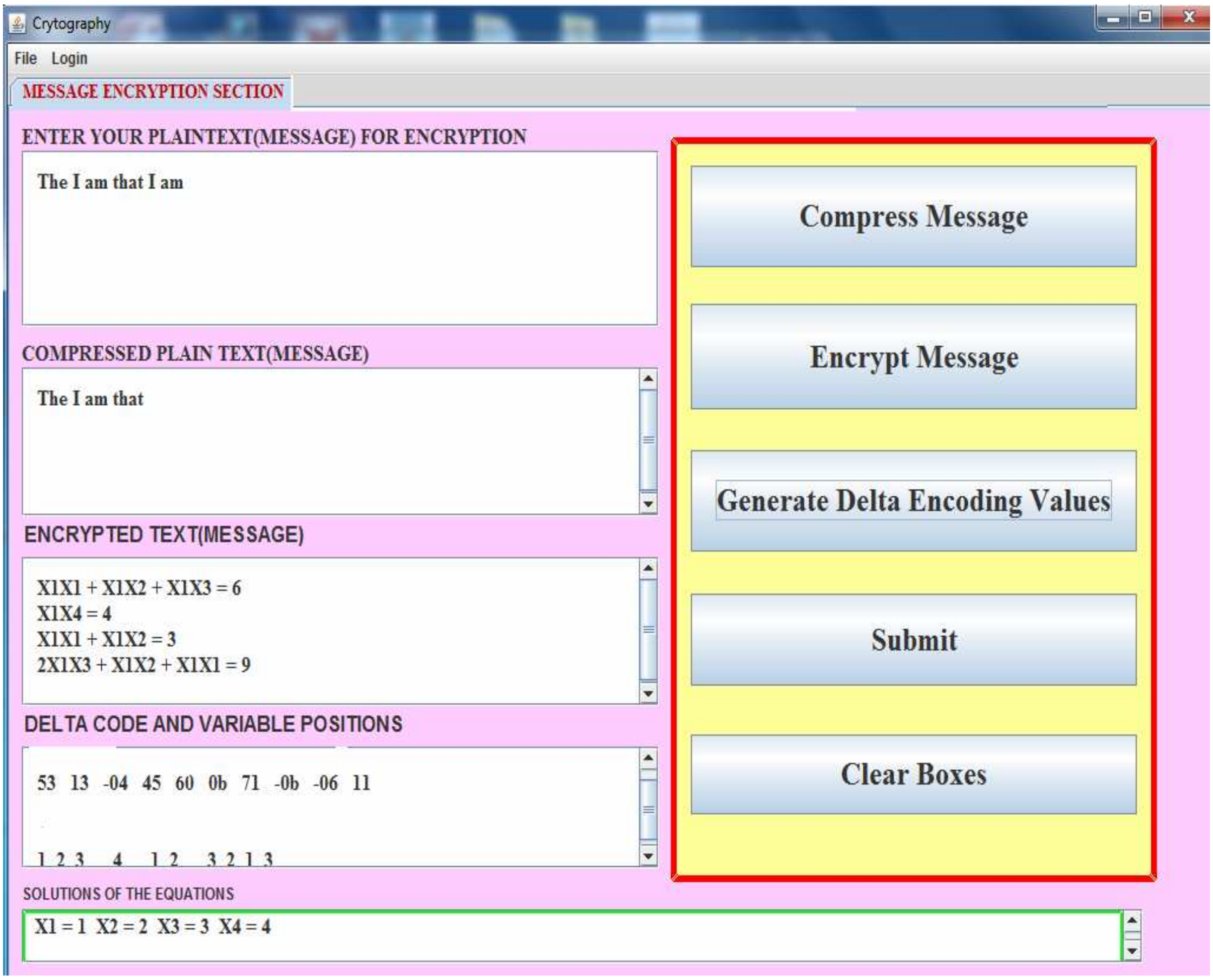
5. Results and Discussions

For experimentation and verification of above encryption and decryption rules, let the plaintext message be “*The I am that I am*.”

The interface of the suggested application is simple enough to be used by any user. Fig. 2 shows a successful encryption interface with the encryption buttons while Fig. 3 shows a successful decryption interface with the decryption buttons.

From Fig. 1, the encryption is performed simply by typing the message to be enciphered in the text message box; this is followed by selecting the “compression message” button to discard repeated words. These provide the first level of security on the data. Furthermore, the user clicks on the “encrypt message” button to coverts the words to a system of nonlinear equations. These provide the second level of security of our sensitive information against the intruder. Finally, the user clicks on “generate delta encoding values” button to generate hexadecimal values corresponding to the position of each of the variables’ of the equations that represents the character position in a word. These enforced a third level security that further strengthens the protection of the data from the eyes of the cryptanalysts.

From the encryption result, it is clear that there is confidentiality and privacy of our data over an insecure channel, due to the multilevel enciphers used in the framework. This finding is in accordance with what was reported by [6] and [1].



ENTER YOUR PLAINTEXT(MESSAGE) FOR ENCRYPTION

The I am that I am

COMPRESSED PLAIN TEXT(MESSAGE)

The I am that

ENCRYPTED TEXT(MESSAGE)

X1X1 + X1X2 + X1X3 = 6
X1X4 = 4
X1X1 + X1X2 = 3
2X1X3 + X1X2 + X1X1 = 9

DELTA CODE AND VARIABLE POSITIONS

53 13 -04 45 60 0b 71 -0b -06 11

1 2 3 4 1 2 3 2 1 3

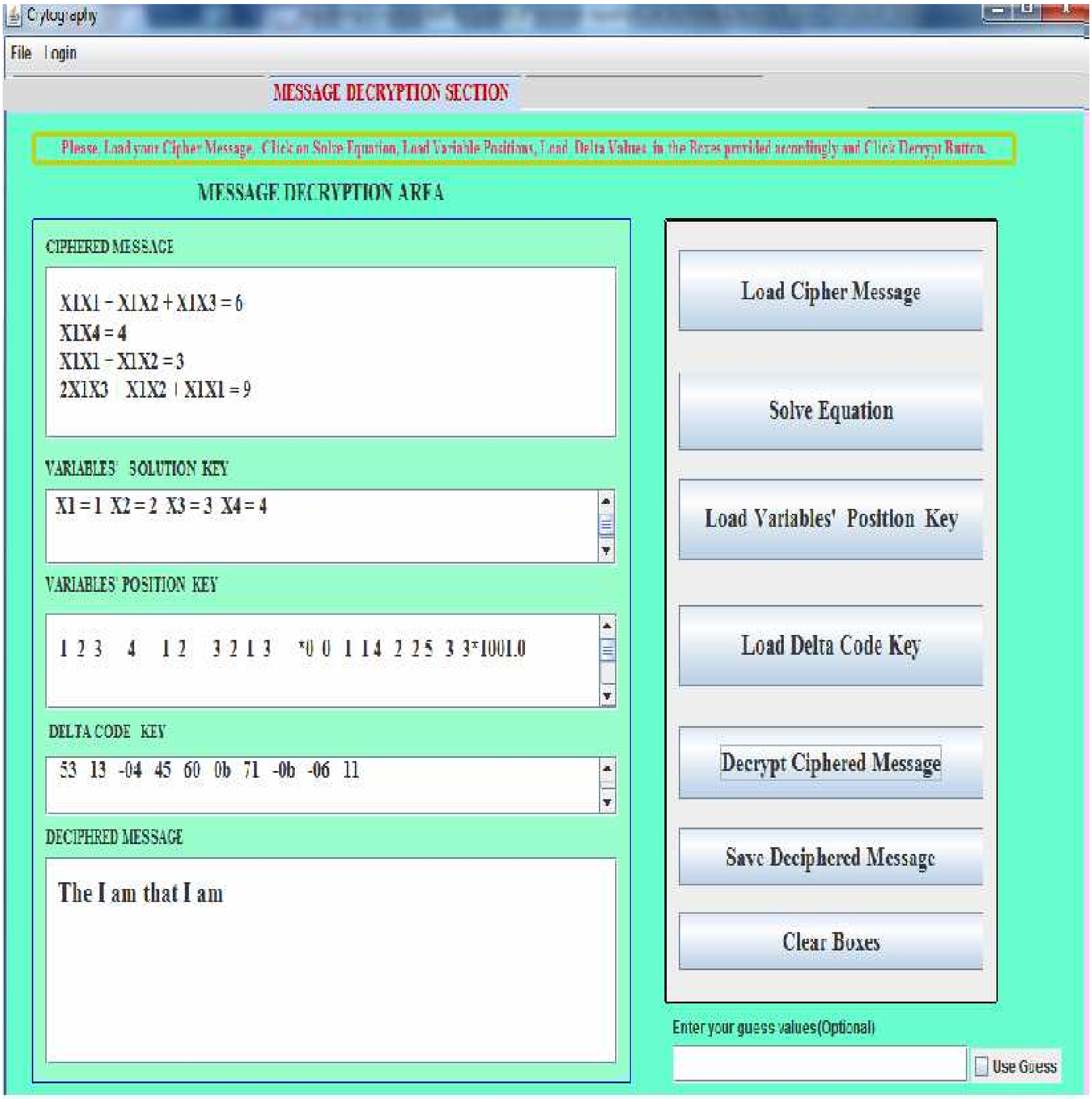
SOLUTIONS OF THE EQUATIONS

X1 = 1 X2 = 2 X3 = 3 X4 = 4

Fig. 1: Successful encryption interface with the encryption buttons

From Fig. 2, the decrypted message is decrypted in the software using another key (different from the public key called private key). This key consists of values of the variables’ position that mostly constituted the solutions of the ciphertext and their corresponding delta encode values. It also holds the index values of the words that were discarded at the compression process. The secret keys could be used for recovering of the plaintext from the ciphertext at the recipient end only which the user obtain secretly through a different channel.

This result is in line with [7] on the strength of asymmetric key which revealed that using long and complex key is harder to break than the one done using smaller and short key. It is therefore, evident from the result of the proposed framework that the integrity of the data is assured.



Please, Load your Cipher Message. Click on Solve Equation, Load Variable Positions, Load Delta Values in the Boxes provided accordingly and Click Decrypt Button.

MESSAGE DECRYPTION AREA

CIPHERED MESSAGE

X1X1 - X1X2 + X1X3 = 6
X1X4 = 4
X1X1 - X1X2 = 3
2X1X3 X1X2 | X1X1 = 9

VARIABLES' SOLUTION KEY

X1 = 1 X2 = 2 X3 = 3 X4 = 4

VARIABLES' POSITION KEY

1 2 3 4 1 2 3 2 1 3 *0 0 1 14 2 25 3 3*1001.0

DELTA CODE KEY

53 13 -04 45 60 0b 71 -0b -06 11

DECIPHRED MESSAGE

The I am that I am

Fig. 2: Successful decryption interface with the decryption buttons.

It is clearly observed from the result that there is no correlation between frequency of occurrence of the plaintext and the ciphertext as experimentally shown in Fig. 3 and Fig. 4. Therefore, it becomes difficult to predict the key in differential crypto-analysis. This result concurred with that of [8] and [1] who also confirmed that any method of brute force attack by the cryptanalyst to find out the key is highly difficult in using single letter frequency statistics to break the ciphertext without the knowledge of the complex secret keys.

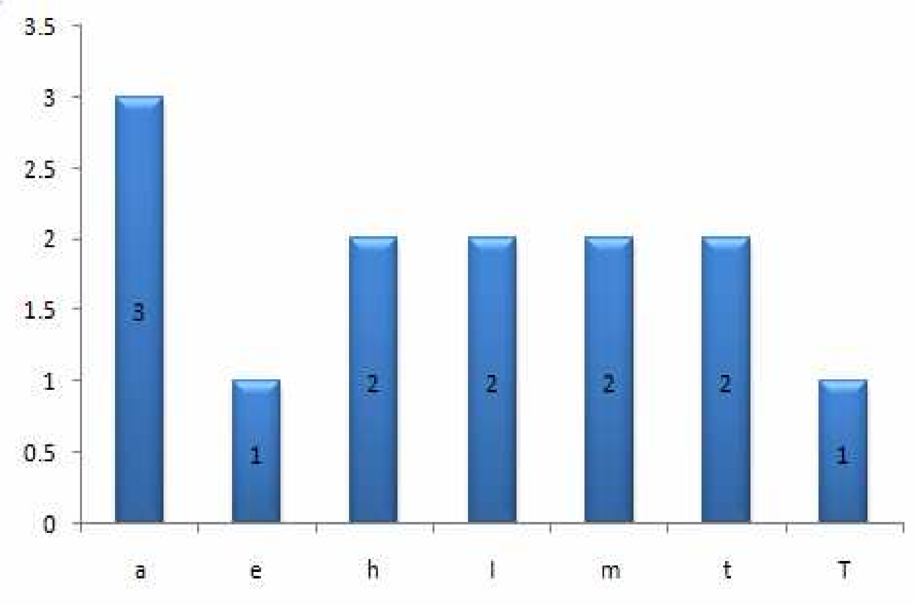


Fig. 3. Frequency of plaintext

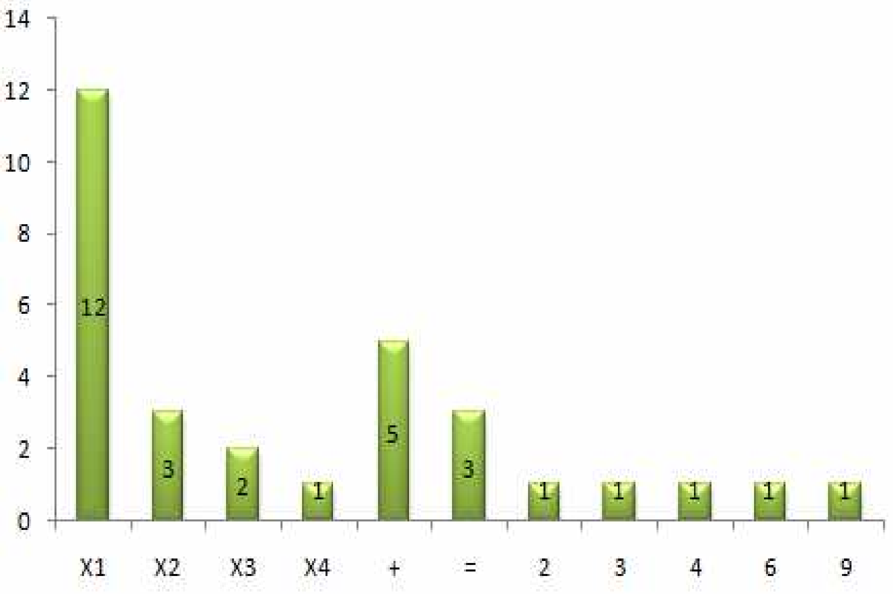


Fig. 4. Frequency of ciphertext

6. Summary/Conclusion

We have developed a complex encryption key using systems of nonlinear equations to establish a trusted link between a sender and recipient. The results proved how the key could offer personal privacy and confidentiality in insecure channel. The larger the text, the more complex the decryption key becomes thereby becoming almost impossible for intruders to obtain the private key.

References

[1] M. Abutaha, M. Farajallah, R. Tahboub and M. Odeh, Survey paper: cryptography is the science of information security, *International Journal of Computer Science and Security (IJCSS)*, 5(2011), 298-309.

[2] R.J. Burden and J.D. Faires, Numerical Analysis (7th Edition), Brooks/Cole, USA, 2001.

[3] G. Crina and A. Ajith, A new approach for solving nonlinear equations system, *IEEE Transaction on Systems, Man and Cybernetic*, 38(2008), 698-714.

[4] J. Biazar and B. Ghanbary, A modification on Newton's method for solving systems of nonlinear equations, *World Academy of Science, Engineering and Technology,* 58(2009*)*, 897- 901.

[5] P.B. Zirra and G.M. Wajiga, Cryptographic algorithms for secure data communication, *International Journal of Computer Science and Security*, 5(2011), 227-243.

[6] D. Salomon, Data Privacy and Security (1st ed.), Springer-Verlag Inc., USA,2003.

[7] S.A.M. Diaa, M.A.K. Hatem and M.H. Mohiy, Evaluating the performance of symmetric encryption algorithms, *International Journal of Network Security*, 10(2010), 213-219.

[8] R.R. Sahoo and G.S. Rath, Designing a cryptosystem by implementing reversible sequential switching M/C- a symmetric approach, *International Journal of Computer and Communication Technology (IJCCT),* 2(2010), 173-175.