INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN MANAGEMENT AND COMPUTER APPLICATIONS
VOL. 2, ISSUE 3, MARCH 2013 ISSN NO: 2319-7471

Generating Ciphertext using Nonlinear System Equations Modified Approach: An Asymmetric Key Approach

Bhandari M. A.
ME (Computer Network), G.H. Raisoni College Of Engg.& Mangement, Pune, India
bhandari.mahesh@gmail.com

Abstract: Linear system based cryptography algorithms like Caesar Cipher, DES, IDEA etc. are attacked by different methods, and mostly by Brute Force technique or by Differential crypto-analysis [2]. The proposed Nonlinear System Equation based cryptographic algorithm is solution to a problem of Linear System Equation based cryptography. Proposed method in paper [1] gives details of Non-linear System Equation based crypto-system in which it uses Newton Method and Gaussian Elimination method. Newton Method uses Jacobian Matrix which contains partial derivative to get Linear System Equation and then iterative Gaussian Elimination method to get roots of Nonlinear System Equation and both methods reduces performance of system. Following proposed algorithm is uses derivative free and iteration reduced method for solving Nonlinear system of equation which improves performance of algorithm [7].

Keywords: Nonlinear System Equation, Newton Method, Gaussian Elimination Method, Derivative.

1. Introduction

Cryptography is system of hiding important data by using different mathematical methods and converting that important message in to such form that the important message becomes un- readable by any means. Different Linear System Equations are used for that but various attacks on such system are made and important information get lick so required a system which will overcome such attacks [2]. Nonlinear System of equation produces different solutions for different equations and its one of the important property of Nonlinear System Equation due to which it is used in cryptography. Following Table 1 will show some of equations and solution they provide [9].

Expression	No. of Solutions
exp(x)+2=0	has no solution
exp(-x)+3=0	has only one solution

And to solve such Nonlinear System equation one popular method called as Newton Method is used which by using Jacobian Matrix with partial derivative convert Nonlinear system Equation into Linear System of Equation and then uses iterative Gaussian Elimination method to solve and get roots of system which are used for positioning of characters at decryption. But due to this performance of system get reduced and to overcome a proposed algorithm is used.

Following paper describes a Linear Methods used for Encryption and Decryption, there drawback in first section, Nonlinear System Equation and methods of solving them and their drawbacks in second section. Third section gives details of Proposed Algorithm for Encryption and Decryption.

2. Related Work

1. **Linear Methods used for Encryption and Decryption**: The Caesar Cipher: One of the oldest method used for encryption and decryption of data. It converts message by replacing it with third letter i.e. if message is 'abc' then it converts it into 'def'. But it is simple to crack.
2. **Data Encryption Standard:** First standardize encryption algorithm. It uses 64 bit data and a same size key for encryption. Many methods and attacks are noted various weaknesses on this algorithm.

3. **Blowfish:** It is block cipher algorithm having block size of 64 bit and uses variable size keys e.g. 32 to 448 bits. It uses 14 or very less round and will get crack fast.

4. **Diffe-Hellman Algorithm:** A very first public key algorithm uses some Modular function for encryption and decryption of data. But variant of "Man in Middle" attack.

$$f(x) = \begin{cases} f1(X) \\ f2(x) \\ . \\ . \\ fn(x) \end{cases}$$

And lots of more methods are also there but all are having their own vulnerability and will be get attack [2].

Nonlinear System Equation and methods of solving them and their drawbacks: Nonlinear System of Equation is shown above and there are various methods to solve nonlinear system of equations from which most popular are Newton type methods.

1. **Newton Method:** It is most popular method to solve Nonlinear System of Equation and uses Jacobian Matrix for solving equation. But it requires good starting value, also analytic derivatives which are mostly not available and use of Jacobian Matrix is expensive.

2. **Quasi Newton method or Secant method**: It is another method but it used to find root of equation. It uses succession of roots of secant lines to find better approximate of roots of a function.

3. **Effati and Nazemi Method:** It is newly proposed method for solving nonlinear equation. But provides optimal solution to problem.

There are lots of other methods also used to solve Nonlinear System of equation like trust region method, Broyden method, Secant method etc [3].

Proposed Method

Encryption Rules:

1. Take the plaintext.

2. Scan the plaintext and delete repeated words.

3. Count the number of words left and discard repeated words to produce public key which is nothing but Nonlinear System of Equation.

4. Assign variable index to each character position in word. If two characters are equal then use previous index as position of character.

5. Send this ciphertext using delta encoding principle to intended receiver [10].

6. Provide secret key to intended receiver using different media of communication.

Decryption Rules:

1. Get Ciphertext from sender

2. Solve it by following step if Nonlinear System of equation does not hold trigonometric or exponential terms then,

a) Check the output value of equation first and then make that value half so values remains are root of equation e.g. if equation is of type: x1x1 + x1x2 + x1x3 = 6 then root of equation are always less than 6 take half of 6 i.e. 3 and root lies in between 1 to 3.

b) Else, if Nonlinear System of equation contains trigonometric, exponential terms, then use following proposed algorithm from paper [7] which is Derivative free method to solve Nonlinear System of equation.

3. Get associated alphanumerical position table from sender and add variable solution of each character.

4. Obtain the index values of the words previously discarded during the compression processes.

5. Then decrypt the ciphertext using the secret keys.

3. Programmer's design

This algorithm is basically designed for Encryption and Decryption of data which should not be attacked by Brute Force, Crypto-Analysis technique and any other attacks. Also in proposed algorithm Nonlinear System Equation should get solve by using iterative free and Derivative free methods. Due to which speed of solving Nonlinear System of equation will get increased and also of the proposed system. So proposed system will be more efficient than the previous system.

3.1. Mathematical Model

Following is the mathematical model for system which shows input ,output required for system and functionality of system it also provides details of different constraints used to develop a system.

Problem Statement:

1. To develop a cryptosystem which should use a Non- linear System of Equation but the method of solving equation at decryption side should be free from iteration and Derivative free Newton Method

a) **Problem Statement:** Let S is Cryptographical System based on Non- linear System of Equation based cryptosystem; such that S= {P, NSEG, DEV, R, C, DFIFN} where P is plaintext, NSEG is Nonlinear System Equation generator, Delta Encoded Value, Root of Nonlinear System Equation, C is Cipher- text, DFIFN is Derivative free and Iterative free Newton Method.

b) **Activity 1:** Let FpE be a rule of p into e such that for given Plain text; it returns Non Linear system of Equation. Fe(P)–¿ {NSE1, NSE2} that belongs to NSE.

c) **Activity 2:** Let FcDEV be a rule of NSE into DEV such that for given Nonlinear System Equation; it returns Delta Encoded Values FcDEV = {DEV1, DEV2 that belongs to DEV.

d) **Activity 3**: FpVIV be a rule of p into VIV such that for given plaintext; it returns Variable Index Value.

e) **Activity 4:** Let FcP be a rule of c into p such that for given Cipher Text; it returns a Plain- text i.e. Fc(P) = {P1, P2} belongs to Plaintext for Ciphertext. Also it uses a rule of FcDFIFN such that for given Ciphertext; it return Root of Equation of Nonlinear System of equation i.e. FcDFIFN = {R1, R2}= R.

3.2. Dynamic Programming and Serialization

In above proposed method there is no use of Dynamic Programming is used. But uses a Recursive method for solving Nonlinear System of equations).

3.3. Data independence and Data Flow architecture

Utilization of tables and serialization for forming input data independence and developing a process tree using data flow architecture).

3.4. Multiplexer Logic

Use of input data independence and serialization for exploring opportunities of morphism, and overloading; hence deriving the multi-threaded architecture SRS resulting in effective use of multicore CPU/concur- rent processing/memory requirements and segmentation. Here in above proposed method if function is provide with Plaintext then return different Roots for different equation e.g. FcP = {R1,R2,..,Rn} that belongs to Root of equation. This is morphism of Ciphertext which is Nonlinear System of equation to finding Root of equations. In Sequential System a loop for Ciphertext to Root of equation will get executed for 'n' number of times. And Morph always make it O(1) hence efficient.

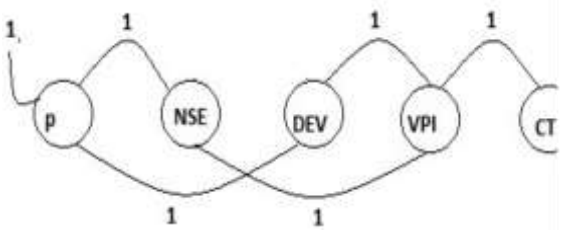

Fig. 1

3.5. Turing Machine

State Diagram of Encryption Method:

Above is the State Machine Diagram for Encryption method of an Algorithm which shows system states and the exact flow of system from state to state. Following are different states of Encryption Method:

1. Get Plaintext as Input for System
2. Then, it converts plaintext into Nonlinear System of Equation
3. Encryption Method also generates Delta Encoded Characters for non repeated palintext
4. And generate variable position index
5. And Ciphertext through Secure Line and other private keys using some other communication line

State Diagram of Decryption Method:

Following is the State Machine Diagram for Decryption method of an Algorithm which shows system states and the exact flow of system from state to state. Following are different states of Encryption Method:

1. Get Ciphertext as Input.
2. Solve Nonlinear System of Equation using Proposed Method.
3. The Root generated are used as to mark each character positions.
4. Use ASCII position table to get repeated characters positions.
5. Get the Plaintext.

4. Results and Discussion

Analytical Result shown in proposed method of solving Nonlinear System of Equation is given below which will get implement and then will compared with actual system. Also due to iterative free method a Cryptographical algorithm will work efficient than previously proposed method.

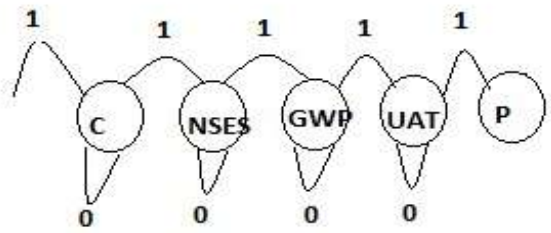

Fig. 2

5. Conclusion

The above method is Derivative free and iterative free method to solve Nonlinear System of Equation which improves efficiency of proposed method and also such efficient algorithm will be free from Brute force attack and not able to crack by Cryptographical analysis.

References

[1]. P. B. Zierra, G.M. Wajiga and S.Boukari, "Generating Ciphertext Using System of Equations: An Asymmetric Key Approach", Intenational Journal of Pure and Applied Science and Technology, vol 8(2), pp:- 47- 53, 2012.
[2]. Zierra Peter Buba, Gregory Maksha Wajiga, "Cryptography Algorithm for Secure Data Communication", Intenational Journal of Computer Science and Security, vol 5(2), pp:- 227- 243, 2011.
[3]. Crina Grosan and Ajith, "A New Approach for Solving Non-linear equation Systems", IEEE Transaction on Systems, Man and Cybernetics- Part A: Systems and Humans, vol 38(3), pp:- 698- 714, 2008.
[4]. Nusrat Yasmin, Moin-ud-din Junjua, "Some Derivative Free Iterative Methods For Solving Nonlinear Equations", Academic Research International, vol 2(1), pp:-75- 82, 2012.
[5]. Dr. Farooq Ahmad, Sifat Hussain, Muhammad Raza, "New Derivative Free Iterative Method For Solving Non-Linear Equations ", Academic Research International, vol 2(1), pp:- 117- 123, 2012.
[6]. P. A. Phiri and O. D. Makinde, "A new derivative-free method for solving nonlinear equations", International Journal of the Physical Sciences Vol. 5(7), pp.935-939, July 2010.
[7]. Gustavo Fernandez Torres, Francisco Ruben Castillo Soria, "Some New Derivative Free Methods For Solving Nonlinear Equations", Academic Research International, vol 2(1), pp:- 148- 153, 2012.
[8]. http://www.dspguide.com/ch26/4.htm.
[9]. Prof. Michael T. Heath, "Scientific Computing An Introductory Survey", Chapter 5, Nonlinear Equations", 2002.
[10]. Steven W. Smith, "Chapter No 27, "Data Compression".