A New Non Linear Model Based Encryption Mechanism with Time Stamp and Acknowledgement Support

Addepalli V. N. Krishna

Department of Computer Science, PJMS College of Engineer & Technology
Karmanghat, Hyderabad - 35, India
(Email: hari_avn @rediffmail.com)

(Received Dec. 9, 2009; revised and accepted Apr. 7, 2010)

Abstract

In this work a non linear model is going to be used which develops data distributed over an identified value which is used as nonce (IV). The key to be considered in the model is a combination of three values K, p & C_p which vary with the data developed. Thus by properly considering a combination of key values which are non linear in nature, data is derived from the developed model. This set of values is considered as a sub key for one round. A time stamp is considered which identifies the number of rounds of the given model. The process is repeated for different time stamp rounds in the encryption mechanism. Thus the model involves an identified value which is used as nonce (IV), a considered non linear set of values which are used as key and different timings as time stamp rounds which are very important parameters in symmetric data encryption schemes. This Model supports not only security but also timeliness of encryption mechanism and also acknowledgement support between the participating parties.

Keywords: Cubic spline interpolation, encryption decryption mechanism, key & sub key generation, non linear model, time stamp and nonce, tridiogonal matrix algorithm

1 Introduction

Historically, encryption schemes were the first central area of interest in cryptography [1, 2, 3, 4, 5, 6, 7, 8, 16]. They deal with providing means to enable private communication over an insecure channel. A sender wishes to transmit information to a receiver over an insecure channel that is a channel which may be tapped by an adversary. Thus, the information to be communicated, which we call the plaintext, must be transformed (encrypted)to a cipher text, a form not legible by anybody other than the intended receiver. The latter must be given some way to decrypt the cipher text, i.e. retrieve the original message, while this must not be possible for an adversary. This is where keys come into play; the receiver is considered to have a key at his disposal, enabling him to recover the actual message, a fact that distinguishes him from any adversary. An encryption scheme consists of three algorithms: The encryption algorithm transforms plaintexts into cipher texts while the decryption algorithm converts cipher texts back into plaintexts. A third algorithm, called the key generator, creates pairs of keys: an encryption key, input to the encryption algorithm, and a related decryption key needed to decrypt. This work mainly deals with the algorithm which generates sub keys which provides sufficient strength to the encryption mechanism.

Partial differential equations to model multiscale phenomena are ubiquitous in industrial applications and their numerical solution is an outstanding challenge within the field of scientific computing [10, 11, 12]. The approach is to process the mathematical model at the level of the equations, before discretization, either removing non-essential small scales when possible, or exploiting special features of the small scales such as self-similarity or scale separation to formulate more tractable computational problems. Types of data,

1) *Static:*
   Each data item is considered free from any temporal reference and the inferences that can be derived from this data are also free of any temporal aspects.

2) *Sequence:*
   In this category of data, though there may not be any explicit reference to time, there exists a sort of qualitative temporal relationship between data items.

3) *Time Stamped:*
   Here we can not only say that a transaction occurred before another but also the exact temporal distance between the data elements. Also with the events being uniformly spaced on the time scale.

4) *Fully Temporal:*
In this category, the validity of the data elements is time dependent. The inferences are necessarily temporal in such cases.

2 Numerical Data Analysis

The following are the steps to generate a numerical method for data analysis [13, 15].

2.1 Discritization Methods

The numerical solution of data flow and other related process can begin when the laws governing these processes have been express differential equations. The individual differential equations that we shall encounter express a certain conservation principle. Each equation employs a certain quantity as its dependent variable and implies that there must be a balance among various factors that influence the variable.

The numerical solution of a differential equation consists of a set of numbers from which the distribution of the dependent variable can be constructed. In this sense a numerical method is akin to a laboratory experiment in which a set of experimental readings enable us to establish the distribution of the measured quantity in the domain under investigation

Let us suppose that we decide to represent the variation of ϕ by a polynomial in x:

$$\phi = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

and employ a numerical method to find the finite number of coefficients a_1, a_2, ..., a_n. This will enable us to evaluate ϕ, at any location x by substituting the value of x and the values of a's in the above equation.

Thus a numerical method treats as its basic unknowns the values of the dependent variable at a finite number of location called the grid points in the calculation domain. This method includes the task of providing a set of algebraic equations for these unknowns and of prescribing an algorithm for solving the equations.

A discretization equation is an algebraic equation connecting the values of f for a group of grid points. Such an equation is derived from the differential equation governing f and thus expresses the same physical information as the differential information. That is only a few grid points participate in the given differential equation is a consequence of the piecewise nature of the profile chosen. The value of f at a grid point there by influence the distribution of f only in its immediate neighborhood. As the number of grid points becomes large, the solutions of discritization equations are expected to approach the exact solution of the corresponding differential equations.

2.2 Control Volume Formulation

The basic idea of the control volume formulation is easy to understand and lends itself to direct physical interpretation. The calculated domain is divided into a number of non overlapping control volumes such that there is one control volume surrounding each grid point. The differential equation is integrated over each control volume piecewise profiles expressing the variation a, f between grid points are used to evaluate the required integrals.

The most attractive feature of the control volume formulation is that the resulting solution would imply that the integral conservation of quantities such as mass, momentum and energy is exactly satisfied over any group of control volumes and of course over the whole calculation domain. This characteristic exists for any number of grid points, not just in a limiting sense when the number of grid points becomes large. Thus even the course grid solution exhibits exact integral balances.

2.3 Steady One Dimensional Data Flow

Steady state one-dimensional equation is given by $\partial./\partial x(k.\partial T/\partial x) + s = 0.0$, where k & s are constants. To derive the discretisation equation we shall employ the grid point cluster. We focus attention on grid point P, which has grid points E, W as neighbors. For one dimensional problem under consideration we shall assume a unit thickness in y and z directions. Thus the volume of control volume is $delx * 1 * 1$.

Thus if we integrate the above equation over the control volume, we get:

$$(K.\partial.T/.\partial X)_e - (K..\partial.T/.\partial X)_w + . \int S.\partial.X = 0.0.$$

If we evaluate the derivatives. $\partial T/\partial X$ in the above equation from piece wise linear profile, the resulting equation will be $Ke(Te - Tp)/(\partial X)_e - Kw(Tp - Tw)/(\partial X)_w + S * delx = 0.0$, where S is average value of s over control volume.

This leads to discretisation equation:

$$\begin{aligned} a_p T_p &= a_e T_e + a_w T_w + b, \text{where } a_e = K_e/\partial X_e \\ a_w &= K_w/dX_w \\ a_p &= a_e + a_w - s_p.delX \\ b &= s_e.delX. \end{aligned}$$

2.4 Grid Spacing

For the grid points it is not necessary that the distances $(dX)e$ and $(dX)w$ be equal. Indeed, the use of non uniform grid spacing is often desirable, for it enables us to deploy more efficiently. Infact we shall obtain an accurate solution only when the grid is sufficiently fine. But there is no need to employ a fine grid in regions where the dependent variable T changes slowly with X. On the other hand, a fine grid is required where the T_X variation is steep. The number of grid points needed for the given accuracy and the way they should be distributed in the calculation domain are the matters that depend on the nature of problem to be solved.

2.5 Solution of Linear Algebraic Equations

The solution of the discretization equations for the one-dimensional situation can be obtained by the standard Gaussian elimination method. Because of the particularly simple form of equations, the elimination process leads to a delightfully convenient algorithm.

For convenience in presenting the algorithm, it is necessary to use somewhat different nomenclature. Suppose the grid points are numbered $1, 2, 3, \ldots, n_i$ where 1 and n_i denoting boundary points.

The discretisation equation can be written as: $A_iT_i + V_iT_{i+1} + C_iT_{i-1} = D_i$, For $I = 1, 2, 3, \ldots, n_i$. Thus the data value T is related to neighboring data values T_{i+1} and T_{i-1}. For the given problem $C_1 = 0$ and $B_n = 0$;

These conditions imply that $T1$ is known in terms of $T2$. The equation for $I = 2$, is a relation between $T1$, $T2$ & $T3$. But since $T1$ can be expressed in terms of $T2$, this relation reduces to a relation between $T2$ and $T3$. This process of substitution can be continued until T_{n-1} can be formally expressed as Tn. But since Tn is known we can obtain T_{n-1}. This enables us to begin back substitution process in which $T_{n-2}, T_{n-3}, \ldots, T3, T2$ can be obtained.

For this tridiogonal system, it is easy to modify the Gaussian elimination procedures to take advantage of zeros in the matrix of coefficients.

Referring to the tridiogonal matrix of coefficients above, the system is put into a upper triangular form by computing new A_i.

$$\begin{aligned} Ai &= Ai - (Ci - 1/Ai) * Bi, \text{where } i = 2, 3, \ldots, n_i \\ Di &= Di - (Ci - 1/Ai) * Di. \end{aligned}$$

2.6 Non Linear Model

In the work presented in "A new Model based encryption mechanism with time stamp and acknowledgement support", accepted and to be published in "International Journal of Network Security" in Nov 2010, the key used is constant which presents a linear case. In the present problem the key is considered a combination of three values which vary with the data generated.

A non linear problem can also be solved using Numerical method.

1) Initially the values of data at all grid points are guessed.
2) From theses guessed data values, coefficients of all grid points are calculated.
3) These linear set of algebraic equations are solved to get new values of data.
4) With these as better guesses, the procedure is returned to Step 2.

This process is continued until further iterations cease to produce any significant change in the values of Data. From the initial guessed values, the coefficients A[I], B[I], C[I], D[I] are calculated. Using these coefficients of grid points, the data is calculated. Let the new data generated is D[I]. Then D[I] is compared with initial guessed data. This procedure is repeated till the difference between present data and earlier data is less than say, 10^{-3}. The procedure is repeated for next delt. Finally the data distribution is obtained for all grid points for different times.

3 Mathematical Modeling of the Problem

The approach to time series analysis was the establishment of a mathematical model describing the observed system. Depending on the appropriation of the problem a linear or nonlinear model will be developed. This model can be useful to generate data at different times to map it with plain text to generate cipher text.

3.1 Linear & Non Linear Data Flow Problem

The initialization vector (IV) considered in the problem is:
When $t = 0$, $T(I) = Y(I) = 300$, where $I = 1, 2, ldots, M$.

Dividing the problem area into M number of points, and for simplicity by assuming data of the first and M^{th} grid points are considered to be known and constant.

For the grid points 2, $M - 1$, the coefficients can be represented by considering the conservation equation [10].

$$\begin{aligned} \alpha/\partial.x(T_{I+1}^{n+1} - T_I^{n+1}) + /\partial x(T_I^{n+1} - T_{I-1}^{n+1}) \\ = (\partial x)/\partial t(T_I^{n+1} - T_I^n), \end{aligned}$$

where T_I represents data value for the considered grid point for the preceding delt, $T_{I+1}^{n+1} \& T_I^{n+1}$ represents data values for the preceding and succeeding grid points for the current delt.

Considering α which is a key for the given model, the coefficients are obtained for each state (grid point) in terms of $A(I)$ refers to data value of the corresponding grid point, $C(I)$ and $B(I)$ refers to data values of preceding and succeeding grid points for the current delt, $D(I)$ refers to data value of the considered grid point in the preceding delt.

$$\begin{aligned} A(I) &= 1 + 2\alpha delt/(delx) * *2. \\ B(I) &= -\alpha delt/(delx) * *2. \\ C(I) &= -\alpha delt/(delx) * *2. \\ D(I) &= T_I^n. \end{aligned}$$

Where α is the key considered which is a constant value. By considering α as a function of 3 values b, C_p & K which are related as a ratio of K to bC_p, the model generated is a linear model.

By varying K as a function of data generated by the model, the model can be considered to be non linear in nature. For the grid points 2, $M-1$, the coefficients can be represented by considering the conservation equation [16],

$$K/\partial.x(T_{I+1}^{n+1} - T_I^{n+1}) - K/\partial x(T_I^{n+1} - T_{I-1}^{n+1}) = ((bC_p\partial x)/\partial t) * T_I^{n+1} - T_I^n),$$

where T_I^n represents data value for the considered grid point for the preceding delt, T_{I+1}^{n+1} & T_I^{n+1} represents data values for the preceding and succeeding grid points for the current delt.

$$T_{I+1}^{n+1}[bC_p\partial x)/\partial t + 2 * K/\partial x] + T_{I-1}^{n+1}[-L/\partial x] = T_I^n(bC_p\partial x)/\partial t).$$

Considering key as a ratio of three variables K, b, C_p for the given model, the coefficients are obtained for each state (grid point) in terms of $A(I)$ refers to data value of the corresponding grid point, $C(I)$ and $B(I)$ refers to data values of preceding and succeeding grid points for the current delt, $D(I)$ refers to data value of the considered grid point in the preceding delt.

$$\begin{aligned} A(I) &= bC_p\partial x/\partial t + 2 * K/\partial x \\ B(I) &= -K/\partial x \\ C(I) &= -K/\partial x \\ D(I) &= T_I^n((bC_p\partial x)/\partial t). \end{aligned}$$

3.2 Procedure for Generating Data from Coefficients by Tridiogonal Method

Using the coefficients of grid points, and by using the tridiogonal matrix algorithm, the data distribution is calculated. The grid points are numbered $1, 2, 3, \ldots, M$, with points 1 and M denoting extreme states.

The discretization equation can be written as:

$$A_iT_i + B_iT_{i+1} + C_iT_{i-1} = D_i.$$

For $I = 1, 2, 3, \ldots, M$. Thus the data T_i is related to neighboring data values T_{i+1} and T_{i-1}. For the given problem $C1 = 0$ and $BM = 0$ as $T1$ & TM represent boundary states.

These conditions imply that $T1$ is known in terms of $T2$. The equation for $I = 2$, is a relation between $T1$, $T2$ & $T3$. But since $T1$ can be expressed in terms of $T2$, this relation reduces to a relation between $T2$ and $T3$. This process of substitution can be continued until $TM-1$ can be formally expressed as TM. But since TM is known we can obtain $TM-1$.This enables us to begin back substitution process in which $TM-2$, $TM-3$, ..., $T3$, $T2$ can be obtained. This process is continued until further iterations cease to produce any significant change in the values of T's. Finally the data distribution is obtained for all grid points for different times by considering a suitable which is used as key.

Relationship between data values and a constant say K as Table 1

Table 1: Relationship between data values and a constant

SNO	Data Values	K
1.	300	140
2.	600	98
3.	900	82.3
4.	1200	69.3
5.	1500	59.5
6.	1800	58.3
7.	2100	58.3
8.	2400	58.3
9.	2700	58.3
10.	3000	58.3

4 Results

By Properly choosing random values for $b = 20$, $C_p = 1.4$, $delt = 2$, $delx = 2$, for a total time stamp of 6 units. Different data values obtained are

For $delt = 2$, $time = 2$;
31 6 7 4 31 9 11 13 30 22 29 20 24 0 12 10 17 11 0 1.

For $delt = 2$, $time = 4$;
8 21 4 3 5 11 10 13 5 31 22 4 15 14 28 25 29 22 15 1 3 33 2 6 22 12 10 11 29 1 26 21 3 32 0 4 12 8 1 30.

For $delt = 2$, $time = 6$;
31 6 7 4 31 9 11 13 30 22 29 20 24 0 12 10 17 11 0 1; 3 26 31 17 16 22 11 18 0 23 21 11 30 6 14 13 3 1 3 7; 3 11 20 23 5 31 9 18 0 21 31 17 12 18 6 11 0 9 30 1.

Thus by using a non linear key, for one time stamp value, a sequences can be generated which is used as sub key. This sub key can be mapped to plain text to generate cipher text for one time stamp round. The procedure is repeated for different time stamp rounds where the cipher text generated in the earlier round will be the input for current round. The output of the final round time stamp will be used as Cipher text.

4.1 Encryption

The encryption algorithm is shown in Table 2.

The process is repeated for different time stamps and the output of final round time stamp will be the cipher text generated.

4.2 Decryption

The reverse of the process used for encryption will generate plain text from the cipher text. The total time stamp used, Nonce value considered and parts of key like p &

Table 2: Encryption mechanism

Plain Text	**a**	**S**	**K**	**s**
Conversion to alpha numeric value	10	28	20	28
Sub key	30	6	7	4
Total	41	34	27	32
Mod 36	05	34	27	32
Cipher Text	05	Y	R	w

C_p needs to be properly shared between the participating parties for the success of this mechanism.

5 Security Analysis

1) As Space and time values are dynamic in nature, the number of rounds the algorithms considers and the length of sub key generated in Encryption Process are variable. This provides sufficient strength to the algorithm against Differential and Linear Crypto Analysis.

2) Because of dynamic nature of Space and Time variants, no specific representation between plain text and cipher text pairs is possible in this model. The model is free from Known Plain text and Cipher Text attacks.

3) The Model considers a key which is a combination of three values which are non linear in nature, a time stamp which is dynamic and a nonce value which is variable, any pattern representation between plain text and cipher text is not possible. Thus this algorithm is free from known statistical attacks and other modes of crypto analytical attacks.

Thus this algorithm provides sufficient strength against crypto Analysis.

6 Comparisons

Some advantages of our algorithm are listed as follows:

1) The algorithm is free from Differential and Linear Crypto Analysis.

2) The computing power needed to generate cipher text for one block of data is minimal when compared to standard algorithms like DES & Rc4.

3) The model provides sufficient strength to algorithm against crypto analysis in real time environment.

Table 3 showed a comparative study of developed model with DES & RC4 in terms of computational overhead, data overhead, complexity and security analysis

7 Conclusion & Future Work

This encryption mechanism uses a Initialization Vector (nonce value), Time Stamp & a non linear Key to generate distributed sequences which are used as sub-keys. Since the time stamp, nonce value and key are variable in nature, the model provides sufficient security against crypto analysis. The model is free from cipher text attack, known plain text & cipher text attacks. The model is also free from known statistical attacks, linear and differential crypto analytical attacks.

In the given model past & present time stamps have been used to generate data. By properly guessing future time stamps, the model can be made still stronger.

References

[1] H. Baker and F. Piper, *Cipher Systems*, North wood books, London, 1982.

[2] I. C. Chiang, *Efficient Improvement to XTR and Two Padding Schemes for Probabilistic Trapdoor One Way Function*, Master Thesis, Dec. 05, 2005.

[3] A. V. N. Krishna, "A new algorithm in network security," *International Conference Proceeding of CISTM-05*, pp. 24-26, Gurgoan, India, July 2005.

[4] A. V. N. Krishna and B. V. Vardhan, "Decision support systems in improving the performance of rocket missile systems," *Giorgio Ranchi, Anno LXIII*, no. 5, pp. 607-615, 2008.

[5] A. V. N. Krishna and S. N. N. Pandit, "A new algorithm in network security for data transmission," *Acharya Nagarjuna International Journal of Mathematics and Information Technology*, vol. 1, no. 2, pp. 97-108, 2004.

[6] A. V. N. Krishna, S. N. N.Pandit, and A. V. Babu, "A generalized scheme for data encryption technique using a randomized matrix key," *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 10, no. 1, pp. 73-81, Feb. 2007.

[7] A. V. N. Krishna and A. V. Babu, "Web and network communication security algorithms," *Journal on Software Engineering*, vol. 1, no. 1, pp. 12-14, July 06.

[8] A. V. N. Krishna and A. V. Babu, "Pipeline data compression & encryption techniques in e-learning environment," *Journal of Theoretical and Applied Information Technology*, vol. 3, no. 1, pp. 37-43, Jan. 2007.

[9] A. V. N. Krishna and A. V. Babu, "A new model based encryption mechanism with time stamp and acknowledgement support," *International Journal for Network Security*, vol. 11, no. 3, pp. 172-176, Nov. 2010.

[10] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly 36*, pp. 306V312, 1929.

Table 3: A comparative study of developed model with DES & RC4

Algorithm	**Computational overhead per block of data**	**Data Overhead per block of data**	**Complexity by its strength**	**Security Analysis**
DES	* 49392 for a56 bit key	Equal	Exponential	chosen text only
RC4	* 64,000 for a40 bit key	Equal	Exponential	chosen text only
New model	500 for a 8 bit key for one round of data	Equal	Exponential	chosen text only

* Block of data refers to 64 bits.

[11] L. S. Hill, "Concerning certain linear transformation apparatus of cryptography," *The American Mathematical Monthly*, vol. 38, pp. 135V154, 1931.

[12] S. N. N. Pandit, *Some Quantitative Combinatorial Search Problems*, Ph.D. Thesis, 1963.

[13] S. V. Patenkar, *Numerical Heat Transfer and Fluid Flow*, pp. 11-75, 1991.

[14] P. Rogaway, *Nonce Based Symmetric Encryption*. (www.cs.ucdavis.edu/rogeway)

[15] R. Ramanna, *Numerical Methods*, pp. 78-85, 1990.

[16] J. W. Stalling, *Cryptography and Network Security*, Pearson Education, ASIA, 1998.

[17] R. S. Thore and D. B. Talange, "Security of internet to pager E-mail messages," *Internet for India-1997 IEEE Hyderabad section*, pp. 89-94, 1997.

Addepalli V. N. Krishna working as Principal & Professor of Computer Science in PJMS College of Eng. & Tech., Hyderabad, A. P., India. He is an M. E(Mechanical), M. TECH(Computer Science), Ph.D(Computer Science & Engineering). He is actively involved in Teaching and Research for the last 19 yrs. His areas of interest are Cryptography, Data Mining and Mathematical Modelling.