# A New Model Based Encryption Mechanism With Time Stamp and Acknowledgement Support

A. V. N. Krishna[1] and A. Vinaya Babu[2]
*(Corresponding author: A. V. N. Krishna)*
Indur Institute of Engg. & Tech., siddipet, A. P., India[1]
Admissions, J.N.T.U.H, Hyderabad, A. P., India[2]
(Email: hari_avn@rediffmail.com
*(Received May 15, 2009; revised and accepted June 27, 2009)*

## Abstract

In this work a model is going to be used which develops data distributed over a identified value which is used as nonce (IV). By properly considering an empirical value, data is derived from the developed model. This empirical value is considered as a key. The process is repeated for different timings which are used as time stamps in the encryption mechanism. Thus this model generates a distributed sequence which is used as sub key. The model involves a identified value which is used as nonce (IV), a considered empirical value which is used as key and different timing as time stamps which are very important parameters in symmetric data encryption schemes which supports not only security but also timeliness of encryption mechanism and also acknowledgement between the participating parties.

*Keywords: Cubic spline interpolation, encryption decryption mechanism, key & sub key generation, time stamp and nonce, tri-diagonal matrix algorithm*

## 1 Introduction

Historically, encryption schemes were the first central area of interest in cryptography [1, 2, 5, 6, 7, 8, 9, 10, 15]. 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 multi-scale phenomena are ubiquitous in industrial applications and their numerical solution is an outstanding challenge within the field of scientific computing [3, 4, 11]. The approach is to process the mathematical model at the level of the equations, before discretion, 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 [12, 14].

### 2.1 Discretization 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 $\emptyset$ by a polynomial in $x$.

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

and employ a numerical method to find the finite number of coefficients $a_1, a_2 \ldots a_n$. This will enable us to evaluate $\emptyset$, 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 discretization 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 an $f$ 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 $\vartheta.\vartheta/x$ $(k.\vartheta T/\vartheta x)+s = 0$. 0 where k & s are constants. To derive the discretization 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

$$(K.\vartheta.T/.\vartheta X)e - (K..\vartheta T/.\vartheta X)_w + .\jmath S.\vartheta.X = 0.0.$$

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

This leads to discretization equation

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

### 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. In fact 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 ... $n_i$ where 1 and $n_i$ denoting boundary points.

The discretization equation can be written as

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

For $I = 1, 2, 3 \ldots n_i$. Thus the data value $T$ is related to neighboring data values $T_{i+1}$ and $T_{i-1}$. For the given problem

$$C_1 = 0 \text{ and } B_n = 0.$$

These conditions imply that $T_1$ is known in terms of $T_2$. The equation for $I = 2$, is a relation between $T_1$, $T_2$ & $T_3$. But since $T_1$ can be expressed in terms of $T_2$, this relation reduces to a relation between $T_2$ and $T_3$. This process of substitution can be continued until $T_{n-1}$ can be formally expressed as Tn. But since $T_n$ is known we can obtain $T_{n-1}$.This enables us to begin back substitution process in which $T_{n-2}$, $T_{n-3}$ ... $T_3$, $T_2$ can be obtained.

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

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

$$\begin{aligned} A_i &= A_i - (C_{i-1}/A_i) * B_i where i = 2, 3 \ldots n_i; \\ D_i &= D_i - (C_{i-1}/A_i) * D_i. \end{aligned}$$

Then computing the unknowns from back substitution

$$T_n = D_n/A_n;$$

Then

$$T_n = D_k - A_k * T_{k+1}/A_k, k = n_{i-1}, n_{i-2} \ldots 3, 2, 1.$$

# 3 Mathematical Modelling 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 Data Flow Problem

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

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,

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

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 $\alpha$ 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.

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

## 3.2 Procedure for Generating Data from Coefficients by Tri-diagonal Method

Using the coefficients of grid points, and by using the tri-diagonal matrix algorithm, the data distribution is calculated. The grid points are numbered $1, 2, 3, \cdots M$. 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 $I = 1, 2, 3 \cdots M$. Thus the data Ti is related to neighboring data values $T_{i+1}$ and $T_{i-1}$. For the given problem $C1 = 0$ and $BM = 0$ as $T_1$ & $TM$ 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 $TM - 2, TM - 3 \cdots T3$, $T2$ 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.

# 4 Results

By considering a suitable key $\alpha = 4$, del $t = 2$, $delx = 2$ for a total time stamp of 6 units (see Tables 1 and 2), different data values obtained are

Table 1: Encryption

| Plain Text | a | s | k | s |
|---|---|---|---|---|
| Conversion to alpha numeric value | 10 | 28 | 20 | 28 |
| Sub key | 33 | 6 | 7 | 4 |
| Total | 43 | 34 | 27 | 32 |
| Mod 36 | 07 | 34 | 27 | 32 |
| Cipher Text | 07 | y | r | w |

Table 2: Decryption

| Plain Text | 07 | y | r | w |
|---|---|---|---|---|
| Conversion to alpha numeric value | 07 | 34 | 27 | 32 |
| Add 36 if less than 9 | 43 | 34 | 27 | 32 |
| Sub key | 33 | 6 | 7 | 4 |
| Subtract | 10 | 28 | 20 | 28 |
| Plain Text | a | s | k | s |

- *For delt = 2, time = 2;*
  33 6 7 4 33 8 11 13 32 22 29 20 26 0 18 10 17 11 1 1;
- *For delt = 2, time = 4;*
  8 22 4 3 5 11 11 13 5 30 22 4 17 14 28 27 29 29 15 1 3 30 2 6 27 12 10 15 29 1 26 26 3 32 0 4 18 8 1 32;
- *For delt = 2, time = 6;*
  33 6 7 4 33 8 11 13 32 22 29 20 26 0 18 10 17 11 1 1;
  3 26 34 17 16 29 11 19 0 23 22 11 33 6 14 13 3 1 4 7;
  3 10 21 23 5 33 9 18 0 20 31 17 15 18 6 14 0 9 31 1;

Thus by using the same key, by changing the time stamp values different sequences can be generated which are used as sub keys. These sub keys can be mapped to plain text to generate cipher text [13, 16].

## 5 Security Analysis

Analysis by Construction: In the given model, even though a single valued key is used, it also depends on time stamp. By changing the time stamp different values can be generated. By keeping the initialization vector constant, different values can be generated which provides good security against cryptanalysis. Since the model involves not only key, time stamps but also data of past time stamps, it is relatively free from cipher text attack, known plain text & cipher text attacks. Table 3 is a comparative study of developed model with DES & RC4 in terms of computational overhead, data overhead, complexity and security analysis.

## 6 Conclusion & Future Work

This encryption mechanism uses a Initialization Vector, Time Stamp & Key to generate distributed sequences which are used as sub-keys. Since the time stamp is variable in nature, the model provides sufficient security against cryptanalysis. The model is free from cipher text attack, known plain text & cipher text 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, *Efficiency Improvement to XTR and Two Padding Schemes for Probabilistic Trapdoor One-Way Function*, Master thesis, 2005.

[3] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, pp. 306-312, June-July 1929.

[4] L. S. Hill, "Concerning certain linear transformation apparatus of cryptography," *The American Mathematical Monthly*, vol. 38, pp. 135-154, 1931.

[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, "A new algorithm in network security," *Proceedings of CISTM-05*, pp. 24-26, Gurgoan, India, July 2005.

[7] A. V. N. Krishna, and A. Vinaya Babu, "Web and network communication security algorithms," *Journal on Software Engineering*, vol. 1, no. 1, pp. 12-14, July 2006.

[8] A. V. N. Krishna, S. N. N. Pandit, and A. Vinaya 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.

[9] 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.

[10] 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.

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

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

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

[14] *Raja Ramanna Numerical methods*, pp. 78-85, 1990.

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

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

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

| 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 a 40 bit key. | Equal | Exponential | chosen text only |
| New Model | 500 for a 8 bit key | Equal | Exponential | chosen text only |

* Block of data refers to 64 bits.

**A. V. N. Krishna** is working as Professor, Computer Science Dept. Indur Institute of Eng. & Tech., Siddipet, A.P, INDIA. He had done his M.E(Mechanical), M.Tech(Computer Science) and submitted his Ph.d thesis in Computer science. He has published work in Journals of National & International repute. His fields of Interest are Cryptography, Mathematical Modelling and Data Mining.

**A. Vinaya Babu** Professor, Computer Science Dept. Working as Director, Admissions, J.N.T.U.H, Hyderabad, A.P, INDIA. He had done his M.E(E.C.E), M.Tech(Computer Science) and Ph.d in Computer science. He has published work in Journals of National & International repute. His fields of Interest are Control Systems, Cryptography, Mathematical Modelling, Data Mining. He has guided number of students for Mtech & Ph.d programs.