Securing data using 4 variables linear block cipher Asymmetric key Algorithm

Prakash Kuppuswamy,
Lecturer,
Department of Computer Networks, Jazan University, KSA

Dr. Wajeeb Kharibi,
Associate Professor, Chairman
Department of Computer Networks, Jazan University, KSA

ABSTRACT

Many cryptographic algorithms used for ensuring security. But still has got several security breaches that need to be dealt with. An improvement over this has been implemented in this paper. Internet connection and networks applications are growing very fast, so the needs to protect such applications are increased. Encryption algorithms play a main role in information security systems. This paper deals with a new algorithm using modulus of 37 and 4 x 4 linear matrix. Internet and networks applications are growing very fast, so the needs to protect such applications are increased. Encryption algorithms play a main role in information security systems. This paper deals with a new algorithm using negative numbers based on linear matrix. It is time efficient and easily learns useful concept and skills. Our goal is to build upon the new Asymmetric key algorithm using linear block cipher or Hill cipher encryption codes of an existing method and design a set of simulation and emulation. Encryption works by running the data (represented as numbers) through a new encryption formula using only negative number using linear matrix and negative value of ‘e’ value. All the encryption based on the Alphabets and numbers, Here, we are assigning synthetic data value to the alphabets and 0-9 numerals. Encryption as cipher text using invertible square matrix, block the message into 4x4 matrix and select ‘e’ any natural number or any negative and multiply with selected matrix and message and use modulation 37, then remainder is our cipher text or encrypted message. Hence for which we got a factor which is then transmitted, and then at decryption using invert of the square matrix and inverse of e value i.e. called as d and multiply with received message and used modulation 37, remainder is our plain Text or message. The decryption algorithm will be there for the receiver as the private key is known as invertible of matrix i.e k⁻¹.

Keywords: Adjoint Matrix, Determination Matrix, Inverse, Modulation, Linear block, Private key or symmetric key, Public Key or Asymmetric key, Square Matrix, Synthetic Value, Transpose Matrix.

I. INTRODUCTION

In the present era of Information Technology, Transmission of information in a secured manner is the primary concern of all agencies. Security is highly essential as intruders are very keen to rob the information with all their might and intelligence. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Within the context of any application-to-application communication, there are some specific security requirements, including [6]:

- Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into ciphertext, which will in turn (usually) be decrypted into usable plaintext [6].

II. PREVIOUS WORK

Though Hill cipher’s or linear block cipher is susceptible to cryptanalysis and unusable in practice, still serves an important pedagogical role in both cryptology and linear algebra. It is this role in linear algebra that raises several interesting questions [2]. In general, the key space of the Hill cipher is precisely GL(r, Zₘ) the group of r x r matrices that are invertible over Zₘ for a predetermined modulus m. We first present a formula for the order of this group. We then consider involutory matrices, which eliminate the necessity of computing matrix inverses for Hill decryptions. Finally, we compare the total number of matrices with the number of invertible and involutory matrices, identifying the effects of change in dimension and modulus on the order of the key space [2].

It is fundamentally equivalent and is consistent with modern texts in cryptography. A plaintext string over an alphabet of order m is rewritten as a vector over Zₘ using a natural correspondence. In either column major or row-major order, the vector is rewritten as a matrix P with d rows, where d is an arbitrarily chosen positive integer [2]. For a fixed n ∈ IN, the key space K is the set of all invertible n x n matrices in Zₘ nxn. P = C = Zₘ nxn. Messages m ∈ Zₘ that are longer than...
are split into blocks of length \( n \) and are encrypted block-wise. All arithmetic operations are carried out modulo \( 26 \). The Hill cipher is defined as follows:

For each \( K \in K \), define the encryption function

\[
E_K : \mathbb{Z}_{26}^n \rightarrow \mathbb{Z}_{26}^n \text{ by } [2]
\]

\[
E_K(p) = K \cdot p \mod 26 \quad \text{………………… (1)}
\]

where \( \cdot \) denotes matrix multiplication modulo \( 26 \).

Letting \( K^{-1} \) denote the inverse matrix of \( K \), the decryption function \( D_K^{-1} : \mathbb{Z}_{26}^n \rightarrow \mathbb{Z}_{26}^n \) is defined by

\[
D_K^{-1}(c) = K^{-1} \cdot c \mod 26 \quad \text{………………… (2)}
\]

Since \( K^{-1} \) can easily be computed from \( K \), the Hill cipher is a symmetric cryptosystem. It is also the most general linear block cipher. Affine linear block ciphers are easy to break by known-plain-text attacks. That is, for an attacker who knows some sample plain texts with the corresponding encryptions, it is not too hard to find the key used to encrypt these plain texts [2].

In the previous algorithm we used 3 variable combination with mod 37, but we are trying to reduce the encryption and decryption timings and making complicated of the plain text in order to prevent from attack [1].

III. PROPOSED SCHEME

The algorithm of encryption and decryption of the technique is to use text and numbers during implementation of the message algorithm which is as follows. Here, we introduce our new algorithm is public key algorithm. The major advantage of asymmetric cryptography is to use two different keys, one Public (open) key and one Private (secret) key. The encrypted message by sender can be decrypted by the other at receiving end and vice versa.

A. Encryption technique

Step 1: To encrypt a text message at first the given text and numbers are stored in a string variable, say \( m \).

Step 2: Select \( k \times k \) square matrix called as \( K \).

Step 3: Select any integer value say as \( e \).

Step 4: Make plain text or message as blocks according to the \( K \) matrix. And transpose the selected block.

Step 5: Multiply Plain text or message with selected square matrix and \( e \) value.

Step 6: Use modulation 37 with derived message. The remainder is Cipher text or decrypted message. Announce Cipher text, \( e \), 37 as public key, and \( K \) as private key sent to the receiver in secured channel.

Table 1: Synthetic value for Alphabets and Numbers

<table>
<thead>
<tr>
<th>Alphabets &amp; Numerals</th>
<th>Synthetic value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A to Z</td>
<td>1 to 26</td>
</tr>
<tr>
<td>0 to 9</td>
<td>27 to 36, 37 used for blank space</td>
</tr>
</tbody>
</table>

B. Decryption Technique

Receiving the plaintext from cipher text using the key is called decryption or deciphering or decoding. Our New linear block cipher decryption sequences were as follows:-

Step 1: After received Cipher text and Private key \( K^{-1} \) and \( e^{-1} \).

Step 2: Arrange encrypted message as \( r \) blocks.

Step 3: Calculate with cipher text using Private key and \( d \).

Step 4: Make modulo 37 with calculated message. The remainder value is called Plain Text.

Step 5: Now we use modulation with calculated value the remainder text is called our Plain Text.

C. Computational Requirements

Formation of new proposal needs following computational requirement.

Plaintext and Synthetic Data:
The synthetic data value consist equivalent value of alphabets and numbers. Alphabet value ‘A’ assigned as integer number 1 and ‘B=2 ……so on. Next we consider integer value ‘0’ assigned as 27 and 1=28……9=36 also the space value considers as an integer number 37. The important of constructing synthetic data value is making confusion and diffusion of the attackers and to make more securable.

Square matrix

In matrix the case of \( m = n \) i.e., rows and columns are equal such matrices are called square matrices. A square matrix \( A = [a_{ij}] \) of order \( n \times n \). Its \( n \) components \( a_{ij} \) form the main diagonal, which runs from top left to bottom right. The cross diagonal runs from the bottom left to upper right. We are choosing square matrix for the purpose of perfect calculation of det of matrix and invertible matrix, which we can use at the time of Encrypting the plain text [2].

Determinant of matrix

Every square matrix can be assigned to a real number, which is called the determinant of the matrix. If \( A = (a_{ij}) \) is a square matrix of order, then the determinant of ‘\( A \)’ is denoted by \( |A| \) and is defined as

\[ |A| = \epsilon a_{ij} * c_{ij}, \ i = 1 \ or \ 2 \ or \ \ldots \ldots \ . n \] [3]

Minor of an element

The minor of an element \( a_{ij} \) is denoted by \( M_{ij} \) and is obtained by deleting the \( i \)th row and \( j \)th column in which the particular element \( a_{ij} \) occurred. The resultant matrix will be a square matrix [3].

Inverse of a matrix

An inverse of a function, usually written as \( f^{-1}(x) \), is a reflection of the original function, \( f(x) \), around the line \( y = x \). Basically, every \( x \) value is changed to a \( y \) value and every \( y \) value is change to an \( x \) value[3].

Adjoint of a Matrix

The adjoint of a squarematrix ‘\( A \)’ is denoted by \( \text{adj}(A) \) and is obtained by taking the transpose of the cofactor matrix \( A \). Therefore \( \text{adj} \ A = (c_{ij})^T \) [3].

Transpose of Matrix

The transpose of a matrix \( A \) is another matrix denoted by \( A^T \) that has \( n \) rows and \( m \) columns. The transpose of a symmetric matrix \( A \) is equal to the original matrix, i.e., \( A = A^T \). Here, we are choosing the Transpose of Matrix for the purpose of making the message or plaintext confusion [3].

Modular function:

\( (a + b) \ mod \ n = [(a \ mod \ n) + (b \ mod \ n)] \ mod \ n. \)
\( (a-b) \ mod \ n = [(a \ mod \ n) - (b \ mod \ n)] \ mod \ n \)
\( (a \* b) \ mod \ n = [(a \ mod \ n) \* (b \ mod \ n)] \ mod \ n \) [8].

IV. IMPLEMENTATION

The cryptography presented in this paper could be augmented with a payment mechanism: a commercial entity could accept payment from Alice (sender) is exchange for providing a common public scheme of using natural numbers. An anonymous access method (using negative variables) could be used to minimize trust required placed upon the service. Alternately, the proposed scheme could be used in the absence of any commercial provider, simply by using the already-public Usenet and a public archiving mechanism. Here we consider a message including the numbers “Dravidian University 2009” to be sent. In Section A, encryption is discussed, in Section B the key generation and sharing discussed and finally in section C decryption methods is shown.

A. Encryption

The Assumed Plain Text is “Jazan University, KSA”. In this paper each alphabets and numbers replaced by natural numbers 1to 36(26 alphabets +10 numerals (0-9, 37 for blank space)). The encryption characters are shown in the following table 2.

Step 1: Assigning Text to Synthetic Data

Table 2: Encryption of alphabets and numbers

<table>
<thead>
<tr>
<th>J</th>
<th>A</th>
<th>Z</th>
<th>A</th>
<th>N</th>
<th>U</th>
<th>N</th>
<th>I</th>
<th>V</th>
<th>E</th>
<th>R</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1</td>
<td>26</td>
<td>1</td>
<td>14</td>
<td>21</td>
<td>14</td>
<td>9</td>
<td>22</td>
<td>5</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>1</td>
<td>T</td>
<td>Y</td>
<td>K</td>
<td>S</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>20</td>
<td>25</td>
<td>11</td>
<td>19</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 2: Making a message or Plain text as linear block

**Table 3: Plain text block**

<table>
<thead>
<tr>
<th>Block No.</th>
<th>Message or Plain Text</th>
<th>Plain Text Block</th>
<th>Synthetic Value for Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>JAZAN UNIVERSITY KSA</td>
<td>J A Z A</td>
<td>10,1,26,1</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>N U N I</td>
<td>14,21,14,9</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>V E R S</td>
<td>22,5,18,19</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>I T Y K</td>
<td>9,20,25,11</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>S A I</td>
<td>19,1,37,37</td>
</tr>
</tbody>
</table>

Step 3: Selecting r x r invertible matrix, Here we choose r = 4, Therefore, We

select ‘k’ = \[
\begin{pmatrix}
2 & 3 & 4 & 4 \\
3 & 2 & 3 & 2 \\
2 & 3 & 2 & 3 \\
1 & 2 & 3 & 4
\end{pmatrix}
\]

\[
|A| = 2 \begin{vmatrix} 2 & 3 & 2 & 2 \\ 3 & 2 & 3 & 2 \\ 2 & 3 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{vmatrix}
= 10
\]

\[
A = 10 \begin{pmatrix}
2 & 3 & 2 & 2 \\
3 & 2 & 3 & 2 \\
2 & 3 & 2 & 3 \\
1 & 2 & 3 & 4
\end{pmatrix}
\]

Now Adj of A=

\[
\begin{pmatrix}
-10 & 7 & 2 & 5 \\
10 & -6 & 4 & -10 \\
10 & -1 & -6 & -5 \\
10 & 2 & 2 & 10
\end{pmatrix}
\]

\[
|A| = 10
\]

Inverse of \( A \) is 26 in Zn37

\((10 * 26) \mod 37 = 1\) (verification)

Now finding the value of \( k' = \)
6 * \[
\begin{pmatrix}
-10 & 7 & 2 & 5 \\
10 & -6 & 4 & -10 \\
10 & -1 & -6 & -5 \\
10 & 2 & 2 & 10 \\
\end{pmatrix}
\] mod 37 = \[
\begin{pmatrix}
36 & 34 & 15 & 19 \\
1 & 29 & 30 & 3 \\
1 & 11 & 29 & 18 \\
36 & 15 & 15 & 1 \\
\end{pmatrix}
\]

Block 1 encryption

The block 1 consist the Plaintext value (J,A,Z,A), it’s equivalent Synthetic value is (10,1,26,1) as per the table, It called as a ‘m’. Convert the given matrix as a transpose matrix and calculate with ‘e’. Our message consists 5 linear blocks. Now \( m=(10,1,26,1) \)

\[
\text{Cipher Text} = (k*m) \mod 37
\]

\[
m^T = \begin{pmatrix}
10 \\
1 \\
26 \\
1 \\
\end{pmatrix}
\quad \text{and} \quad k = \begin{pmatrix}
2 & 3 & 4 & 4 \\
3 & 2 & 3 & 2 \\
2 & 3 & 2 & 3 \\
1 & 2 & 3 & 4 \\
\end{pmatrix}
\mod 37 = \begin{pmatrix}
20 \\
1 \\
4 \\
20 \\
\end{pmatrix}
\]

Therefore (10,1,26,1) encrypted message is (1,11,21,11)

Similarly block 2 to 5 synthetic value of text and Cipher Text value were as follows

**Table 4: Encrypted text**

<table>
<thead>
<tr>
<th>Block</th>
<th>Synthetic Value</th>
<th>Cipher Text Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block 1</td>
<td>10,1,26,1</td>
<td>20,1,4,20</td>
</tr>
<tr>
<td>Block 2</td>
<td>14,21,14,9</td>
<td>35,33,35,23</td>
</tr>
<tr>
<td>Block 3</td>
<td>22,5,18,19</td>
<td>22,20,4,14</td>
</tr>
<tr>
<td>Block 4</td>
<td>9,20,25,11</td>
<td>37,16,13,20</td>
</tr>
<tr>
<td>Block 5</td>
<td>19,1,37,37</td>
<td>4,22,4,21</td>
</tr>
</tbody>
</table>

Therefore the Plain Text or Message of “JAZAN UNIVERSITY KSA” is “TADT868WVTDN0PMTDVDU”

**B. Key Generation**

Here we are selecting another negative number which consider as a ‘e’ and multiply with Encrypted text.

**Table 5: Adding Key**

<table>
<thead>
<tr>
<th>Encrypted Text Value</th>
<th>Adding key (e=-4) mod 37</th>
<th>Receivers Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>31</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>33</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>21</td>
<td>U</td>
</tr>
<tr>
<td>20</td>
<td>31</td>
<td>4</td>
</tr>
<tr>
<td>35</td>
<td>8</td>
<td>H</td>
</tr>
<tr>
<td>33</td>
<td>16</td>
<td>P</td>
</tr>
<tr>
<td>35</td>
<td>8</td>
<td>H</td>
</tr>
<tr>
<td>23</td>
<td>19</td>
<td>S</td>
</tr>
<tr>
<td>22</td>
<td>23</td>
<td>W</td>
</tr>
<tr>
<td>20</td>
<td>31</td>
<td>4</td>
</tr>
</tbody>
</table>
Announce public key 37, Encrypted messages and e

Now use $k^{-1}$ matrix as private key and $e'$ or ‘d’ to decrypt the text

<table>
<thead>
<tr>
<th>Encrypted Text</th>
<th>Using $e'$ or $d=9 \mod 37$</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>20</td>
</tr>
<tr>
<td>33</td>
<td>1</td>
</tr>
<tr>
<td>21</td>
<td>4</td>
</tr>
<tr>
<td>31</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>35</td>
</tr>
<tr>
<td>16</td>
<td>33</td>
</tr>
<tr>
<td>8</td>
<td>35</td>
</tr>
<tr>
<td>19</td>
<td>23</td>
</tr>
<tr>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>31</td>
<td>20</td>
</tr>
<tr>
<td>21</td>
<td>4</td>
</tr>
<tr>
<td>18</td>
<td>14</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>16</td>
</tr>
<tr>
<td>22</td>
<td>13</td>
</tr>
<tr>
<td>31</td>
<td>20</td>
</tr>
<tr>
<td>21</td>
<td>4</td>
</tr>
<tr>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>21</td>
<td>4</td>
</tr>
<tr>
<td>27</td>
<td>21</td>
</tr>
</tbody>
</table>

C. Decryption
Now use $k^{-1}$

\[
\begin{pmatrix}
36 & 34 & 15 & 19 \\
1 & 29 & 30 & 3 \\
1 & 11 & 29 & 18 \\
36 & 15 & 15 & 1 \\
\end{pmatrix}
\begin{pmatrix}
20 \\
1 \\
4 \\
20 \\
\end{pmatrix}
\mod 37 =
\begin{pmatrix}
10 \\
1 \\
26 \\
1 \\
\end{pmatrix}
\]

Block 1

The block 1 consist the cipher text value (20,1,4,20), we calculate using private key i.e $k^{-1}$

\[
\begin{pmatrix}
36 & 34 & 15 & 19 \\
1 & 29 & 30 & 3 \\
1 & 11 & 29 & 18 \\
36 & 15 & 15 & 1 \\
\end{pmatrix}
\begin{pmatrix}
20 \\
1 \\
4 \\
20 \\
\end{pmatrix}
\mod 37 =
\begin{pmatrix}
10 \\
1 \\
26 \\
1 \\
\end{pmatrix}
\]

Therefore block-1 (20,1,4,20) decrypted plaintext value is (10,1,26,1) and its equivalent plain text is (J A Z A). Similarly block 2 to 5 decrypted messages and Plain Text value were as follows

**Table 7: Decryption text**

<table>
<thead>
<tr>
<th>Block</th>
<th>Encryption</th>
<th>Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block 1</td>
<td>20,1,4,20</td>
<td>10,1,26,1</td>
</tr>
<tr>
<td>Block 2</td>
<td>35,33,35,23</td>
<td>14,21,14,9</td>
</tr>
<tr>
<td>Block 3</td>
<td>22,20,4,14</td>
<td>22,5,18,19</td>
</tr>
<tr>
<td>Block 4</td>
<td>37,16,13,20</td>
<td>9,20,25,11</td>
</tr>
<tr>
<td>Block 5</td>
<td>4,22,4,21</td>
<td>19,1,37,37</td>
</tr>
</tbody>
</table>

V. RESULT ANALYSIS

Here we have ciphered each alphabets and numbers into numbers using private and public key and hence decrypted the keys to obtain the final character and hence the final message. Here we have analysis with existing public key algorithm to find out our New algorithm performance.

**Table 8: Encryption/Decryption performance**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Encryption duration</th>
<th>Decryption Duration</th>
<th>Key generating duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>3.2</td>
<td>4.3</td>
<td>4.0</td>
</tr>
<tr>
<td>Rabin</td>
<td>4.4</td>
<td>5.2</td>
<td>6.4</td>
</tr>
<tr>
<td>ElGamal</td>
<td>7.2</td>
<td>5.3</td>
<td>5.0</td>
</tr>
<tr>
<td>3 block</td>
<td>4.4</td>
<td>4.6</td>
<td>4.0</td>
</tr>
<tr>
<td>4 x4 block</td>
<td>4.2</td>
<td>4.4</td>
<td>4.0</td>
</tr>
</tbody>
</table>

A. Encryption Analysis

Encryption technique is very authoritative and straight forward. In this algorithm we can make any number of square matrix and blocks. The algorithm based on the ‘r x r’ square matrix. Therefore we can select square matrix with any variables. If comparing to other algorithm, The RSA algorithm calculates each and every text variable for encryption. The ElGamal algorithm produces two different cipher texts for single encryption. The Rabin method produces 4 cipher texts for single encryption. In our New algorithm we can make set of blocks in single encryption. Table 8 clearly indicates about encryption methods of various algorithms.
B. Decryption Analysis

The New algorithm decryption is complex without the private key. All the plain text is decryption using inverse matrix as a key. Therefore it is providing secure from the unauthorized entities and susceptible. Moreover we are sending secret key through secured channel through key distribution centre or valid entity. If comparing to other algorithm, The RSA algorithm decrypting the cipher text one by one. The ElGammal algorithm receives the two cipher text and calculating decryption once. The Rabin method receives the 4 cipher texts and decryption using 4 steps to find a feasible solution. In this new proposed algorithm we receive set of blocks variable and decryption also using single steps. The following table clearly indicates about decryption methods of various algorithms.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>No. of Cipher Text</th>
<th>Decryption cycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>ElGammal</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Rabin</td>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>3 variable block</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4 x 4 Nlbc</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

The performance of implementation of the Negative number algorithm examined, primarily on an Intel Pentium Dual CPU T3400 Dual Core 2.16 Ghz, 2.00 GB RAM, 32 Bit Operating System offer a reasonable number of processors which allows for good scalability testing.

VI. CONCLUSION AND FUTURE WORK

Our New 4x4 linear matrix algorithm using Asymmetric key based on the block cipher or hill cipher. The hill cipher or linear block cipher openness to cryptanalysis has rendered it unusable in practice for the public key algorithm. It still serves an important academic role in both cryptology and linear mathematics. In our New linear block cipher public algorithm, that raises several interesting questions such as key generation method, key distribution method, security concern. The reason for selecting linear block cipher for our new algorithm, the linear algebra will not produce same kind result for the repeated text variable. The advantage for the linear block cipher, we can use any variable for selecting the square matrix. This negative value make more complicated to the invader. Especially, in this chapter we are concluding, Symmetric and practically unusable linear block cipher to make usable format, strong security and announcing as a public key algorithm.
Another innovative idea for our New algorithm, We are extending characters upto 37 letters. Most of the algorithm working based on the 26 alphabets, especially hill cipher or linear block cipher working based on the 26 alphabets only. In this chapter we are extending the text value upto 37. This 4x4 linear matrix implementation of the previous 3 variable algorithm in security, time consumption etc.,

There are few highlight point about our experimental setup, First one is we are converting the alphabets to synthetic data value, second is we are selecting random number ‘e’ for announcing public keys. The bottleneck of our New algorithm, we are keeping linear variable as a private key.

To date, we have only modelled the security of our key refreshing mechanism when it is used in tandem with an alphabets and number scheme. Yet we might wish to use the new private key in an identity, video based scheme. Our proposed methods capture the new idea of general usage in commercial sector. Theoretical challenge is to study proofs of security for key refreshing in the standard model (i.e. with using random keys).

Acknowledgments

We would like thank to Dean Dr. Omar Saeed Mushayt and Vice Dean Dr. Saeed, Jazan University, KSA for their extreme support in the entire manner.

REFERENCES

[1] Prakash kuppuswamy, Dr.Chadrasekar, Enrichment of security through cryptographic public key algorithm based on block cipher, ijcse-11-02-03-085
[2] John C. Bowman, Math 422 Coding Theory & Cryptography, University of Alberta, Edmonton, Canada
[3] David A. Santos, Linear Algebra Notes, January 2, 2010 Revision, dsantos@ccp.edu.
[9] Anoop MS, Public Key Cryptography Applications Algorithms and Mathematical Explanations, Tata Elxsi Ltd, India, anoopms@tataelxsi.co.in
<table>
<thead>
<tr>
<th><strong>Prakash Kuppuswamy</strong> Lecturer, C-Net Department in Jazan University, KSA He is research Scholar proceeding in ‘Dravidian University’. He has been published few journals/Technical papers and participated many international conference in Rep. of Maldives, Libya and Ethiopia.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dr. Wajeb Gharibi</strong> is an Associate Professor, Chairman, Department of Computer Networks, College of Computer Science &amp; Information Systems, Jazan University, Jazan, Kingdom of Saudi Arabia. He obtained his Ph. D degree in Informatics from Institute of Mathematics and Computer Science, Byelorussian Academy of Sciences, USSR in 1990. His research interests include Information Security, Microelectronics; embedded systems, Design &amp; analysis of network algorithms, Combinatorial optimization, computational geometry, discrete convexity, operations research and data analysis</td>
</tr>
</tbody>
</table>