ENRICHMENT OF SECURITY THROUGH CRYPTOGRAPHIC PUBLIC KEY ALGORITHM BASED ON BLOCK CIPHER

PRAKASH KUPPUSWAMY,
Department of Computing Science & Technology,
Samara University, Ethiopia.
varshiniprakash@rediffmail.com, kpmvellore@yahoomail.com

Dr.C.CHANDRASEKAR,
Department of Computer Science,
Periyar Univeristy,Salem, India.
ccsekar@gmail.com

Abstract

In recent years Data Security using cryptography has emerged as a topic of significant interest in both academic and industry circles. This paper deals with a new algorithm, which is based on linear block cipher. Our goal is to build upon the new Asymmetric key algorithm based on linear block cipher or Hill cipher encryption codes of existing methods and design a set of simulation and emulation. It is the scheme based on the block cipher. All the encryption is based on the Alphabets and numbers. Here, we are creating synthetic data value, based on the 26 alphabets and 0-9 numerals. Encryption as cipher text use invertible square matrix, blocking the message according to the selected square matrix i.e if the square matrix is 3 x 3 make the message or plain text 3 blocks, and select 'e' as any natural number and multiply with selected matrix and message, use modulation 37, then the remainder is our cipher text or encrypted message. This factor is then transmitted. At decryption we use the inverse of the square matrix and inverse of e value which is now called as d and multiply with received message and use modulation 37, then remainder is our plain Text or message. The decryption algorithm will be there for the receiver as the private key known as k^i. The concept of this new algorithm is based on modular 37 (alphabets an numerals) whereas existing algorithms are based only on modular 26 (only alphabets). We are naming this linear based algorithm as New linear block cipher or Nlbc.

Keywords: Inverse, Modulation, Linear block, Nlbc (New linear block cipher), Private key or symmetric key, Public Key or Asymmetric key, Synthetic Value.

1. Introduction

Cryptography is the science of writing messages in secret code and an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription [5].

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 [5].

Within the context of any application-to-application communication, there are some specific security requirements, including [5]:-

- Authentication
- Privacy/confidentiality
- Integrity
- Non-repudiation

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[5].

2. 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 [1].

In general, the key space of the Hill cipher is precisely GL(r, Z_m) the group of r * r matrices that are invertible over Z_m 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 [1].

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 Z_m 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 [1].

For a fixed $n \epsilon$ IN, the key space K is the set of all invertible n x n matrices in ZZ^{nxn}_{26} $.P = C = ZZ^{n}_{26}$. Messages $m \epsilon ZZ^{*}$ that are longer than n are split into blocks of length n and are encrypted block-wise. All arithmetic operations are carried out modulo 26[1]. The *Hill cipher* is defined as follows:

For each $K \epsilon K$, define the encryption function
EK : ZZ^{n}_{26} -> ZZ^{n}_{26} by[1]

$EK(p) = K . p$ mod 26 ……………………………(1)
where "." denotes matrix multiplication modulo 26[1].

Letting K^{-1} denote the inverse matrix of K, the decryption function DK-1 : ZZ^{n}_{26} -> ZZ^{n}_{26} is defined by

$DK\text{-}1(c) = K^{-1} . c$ mod 26[1] ………………………...(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 [1].

3. The 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 Nlbc algorithm asymmetric or 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.

3.1. Encryption *technique*

Step1: To encrypt a text message at first the given text and numbers are stored in a string variable, say ***m.***
Step2: Select k *k square matrix called as k.
Step3: 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

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	Q
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	SPACE	
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	

3.2. 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: Receiving Cipher text and Private key k’ and $e^{'}$.
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.

3.3. Computational requirements

Our, New linear block algorithm needs following computational requirement to the formation of new public key algorithm.

3.3.1 Plaintext and Synthetic Data:

We know that, whatever message or plaintext consist of Alphabets between A to Z and numbers which is between 0-9.

Here, In New linear block cipher we introduce synthetic data, which is based on the sender’s message text. Normally the synthetic data value consists of equivalent value of alphabets and numbers. Alphabet value ‘A’ is 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.

3.3.2 Square matrix

In matrix where m = n i.e., rows and columns are equal, are called square matrices. A square matrix **A** = [a*ij*] of order n × n. Its n components a*ii* form the main diagonal, which runs from top left to bottom right. The cross diagonal runs from the bottom left to upper right. In our New linear block algorithm, 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]*.

3.3.3 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| =ϵ a*ij* * c*ij*, I = 1 or 2 or ……….n *[2]*

3.3.4 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 *[2]*.

3.3.5 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 *[2]*.

3.3.6 Adjoint of a Matrix

The adjoint of a square matrix ‘A’ is denoted by adj(A) and is obtained by taking the transpose of the cofactor matrix A. Therefore adj A =$(cij)^T$ *[2]*.

3.3.7 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) x (b mod n)] mod n [7].

4. Implementation

The cryptography presented in this paper could be augmented with a payment mechanism: a commercial entity could accept payment from Alice (sender) and exchange for providing a common public scheme of using natural numbers. Here we consider a message including the numbers “*World cup 2011*” to be sent. In Section 4.1, encryption is discussed, in Section 4.2 the key generation and sharing is discussed and finally in section 4.3 decryption methods are shown.

4.1. Encryption

The Assumed Plain Text is “*World cup 2011*” (including alphabets and numbers). In this paper each alphabet and number is replaced by natural numbers 1to 36(26 alphabets +10 numerals (0-9)). So the encrypted characters are shown in the following table 2.

Step 1: Assigning Text to Synthetic Data

Table 2.Encryption of alphabets and numbers

Sl.No.	1	2	3	4	5	6	7	8	9	10	11	12
Message	W	O	R	L	D	C	U	P	2	0	1	1
Synthetic Data	23	15	18	12	4	3	21	16	29	27	28	28

Step 2: Making a message or Plain text as linear block

Table 3.Linear block text

Block. No.	**Message (or) Plain Text**	**Blocking the Plain text**			**Synthetic value for Plain Text Block**
1	WORLD CUP 2011	W	O	R	23,15,18
2		L	D	C	12,4,3
3		U	P	2	21,16,29
4		0	1	1	27,28,28

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

select ‘k’ = $\begin{pmatrix} 1 & 2 & 1 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$

1(5*9 – 6*8) – 2(4*9 – 7*6) +1 (4*8 – 5*7)
=1(45-48) – 2(36-42) + 1(32-35)
=1(-3) - 2(-6) +1(-3) =-3 +12 – 3 = 6

Therefore 6 is no common factor in Z_{37}.
Now det ‘k’ =

$C_{11}\ [-1]^{1+1}$ x $\begin{pmatrix} 5 & 6 \\ 8 & 9 \end{pmatrix}$ $= [-1]^{2}$ x (45-48) = -3

$C_{12}\ [-1]^{1+2}$ x $\begin{pmatrix} 4 & 6 \\ 7 & 9 \end{pmatrix}$ $= [-1]^{3}$ x (36-42) = 6

$C_{13}\ [-1]^{1+3}$ x $\begin{pmatrix} 4 & 5 \\ 7 & 8 \end{pmatrix}$ $= [-1]^{4}$ x (32-35) = -3

Then the value of
$C_{21} = -10$, $C_{22} = 2$, $C_{23} = 6$ and $C_{31} = 7$, $C_{32} = -2$, $C_{33} = -3$

Therefore Adj A = $\begin{pmatrix} -3 & -10 & 7 \\ 6 & 2 & -2 \\ -3 & 6 & -3 \end{pmatrix}$

Calculating $k^I = -6 * \begin{pmatrix} -3 & -10 & 7 \\ 6 & 2 & -2 \\ -3 & 6 & -3 \end{pmatrix} = \begin{pmatrix} (18\%37), (-36\%37), (18\%37 \\ (60\%37),(-12\%37),(-36\%37) \\ (-42\%37),(12\%37), (18\%37) \end{pmatrix} = \begin{pmatrix} 18 & 1 & 18 \\ 23 & 25 & 1 \\ 32 & 12 & 18 \end{pmatrix}$

Step 3: Message or Plain Text Encryption

Now, We already calculated the total number of block message is 4 and we know that Zn = 37, Then we already calculated ‘k’ and k^I.

Encrypting Block 1:

The block 1 consist the Plaintext value (W, O, R), it’s equivalent Synthetic value is (23,15,18) as per the table, It is called as a ‘m’. Convert the given matrix as a transpose matrix and calculate with ‘e’. Our message consists 4 linear block.

m=(23,15,18)

$m^T = \begin{pmatrix} 23 \\ 15 \\ 18 \end{pmatrix}$ and $k = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$

Cipher Text = (k*m) mod 37

$$\begin{pmatrix} 1 & 2 & 1 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} * \begin{pmatrix} 23 \\ 15 \\ 18 \end{pmatrix} = \begin{pmatrix} (1*23)+(2*15)+(1*18) \\ (4*23)+(5*15)+(6*18) \\ (7*23)+(8*15)+(9*18) \end{pmatrix} \text{ mod } 37 = \begin{pmatrix} 34 \\ 16 \\ 36 \end{pmatrix}$$

Therefore (23, 15, 18) encrypted message is (34, 16, 36),

Similarly, Block-2 (12,4,3) encrypted message is (23,12,32), Block-3 (21,16,29) encrypted message is (8,5,18) and Block-4 (27,28,28) encrypted message is (0,9,36)

Now Encrypted value and cipher Text were as follows

Table 4. Encrypted Text

Sl. No.	Plain Text	Integer Value	Cipher Value	Encrypted Equivalent Text
1	W	23	34	7
2	O	15	16	P
3	R	18	36	9
4	L	12	23	W
5	D	4	12	L
6	C	3	32	5
7	U	21	8	H
8	P	16	5	E
9	2	29	18	R
10	0	27	0	0
11	1	28	9	I
12	1	28	36	9

Therefore the Plain Text or Message of “WORLD CUP 2011” is “*7P9WL5HER0I9*”

4.2 Key Generation

Now select any natural numbers, which is called as ‘e’ and multiply with Encrypted text.

Table 5. Adding key with Encrypted Text

Encrypted Text Value	Multiply with e (Assume e=5)	Mod 37	Receivers Message
34	170	22	V
16	80	6	F
36	180	32	5
23	115	4	D
12	60	23	W
32	160	12	L
8	40	3	C
5	25	25	Y
18	90	16	P
0	0	0	37
9	45	8	H
36	180	32	5

Announce public key 37, Encrypted messages and e
Now use as 'k' matrix as private key and e^I or *d* to decrypt the text

4.3 Decryption

Table 6.First Stage of Decryption

Encrypted Text	Using e' or d i.e 15	Revealed Cipher Text Key
22	330	34
6	90	16
32	480	36
4	60	23
23	345	12
12	180	32
3	45	8
25	375	5
16	240	18
0	0	0
8	120	9
32	480	36

Now use k^I

$$\begin{pmatrix} 18 & 1 & 18 \\ 23 & 25 & 1 \\ 32 & 12 & 18 \end{pmatrix}$$

Block 1

$$\begin{pmatrix} 18 & 1 & 18 \\ 23 & 25 & 1 \\ 32 & 12 & 18 \end{pmatrix} * \begin{pmatrix} 34 \\ 16 \\ 36 \end{pmatrix} = \begin{pmatrix} (18*34)+(1*16)+(18*36) \\ (23*34)+(25*16)+(1*36) \\ (32*34)+(12*16)+(18*36) \end{pmatrix} \text{mod } 37= \begin{pmatrix} 23 \\ 15 \\ 18 \end{pmatrix}$$

Block-1 (34, 16, 36) decrypted message is (23, 15, 18)

Similarly block-2 (23,12,32) decrypted message is (12,4,3),Block-3 (8,5,18) decrypted message is (21,16,29) and Block-4 (0,9,36) decrypted message is (27,28,28)

Table 7.Stages of Encryption/Decryption

Plain Text	Encryption			Decryption		Plain Text
	Synthetic Value	1st Stage	Add ‘e’ (5)	e’ or d (15)	Decryption	
W	23	34	22	34	23	W
O	15	16	6	16	15	O
R	18	36	32	36	18	R
L	12	23	4	23	12	L
D	4	12	23	12	4	D
C	3	32	12	32	3	C
U	21	8	3	8	21	U
P	16	5	25	5	16	P
2	29	18	16	18	29	2
0	27	0	0	0	27	0
1	28	9	8	9	28	1
1	28	36	32	36	28	1

5. 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 the final message. Here we analysed with existing public key algorithm to find out our New algorithm performance.

5.1 Encryption analysis

Nlbc encryption technique is very authoritative and straight forward. In this algorithm we can make any number of square matrices and blocks. The algorithm is based on the ‘r x r’ square matrix. Therefore we can select square matrix with any variables. When compare to other algorithm, The RSA algorithm calculates each and every text variable for encryption. The ElGammal algorithm produces two different cipher texts for single encryption. The Rabin method produces 4 cipher texts for single encryption. In our New linear block cipher algorithm we can make set of blocks in single encryption. The following table clearly indicates about encryption methods of various algorithms.

Table 8.Comparison of Encryption Cycle

Algorithm	No. of Text	Encryption cycle
RSA	3	3
ElGammal	3	6
Rabin	3	12
Nlbc	3	1

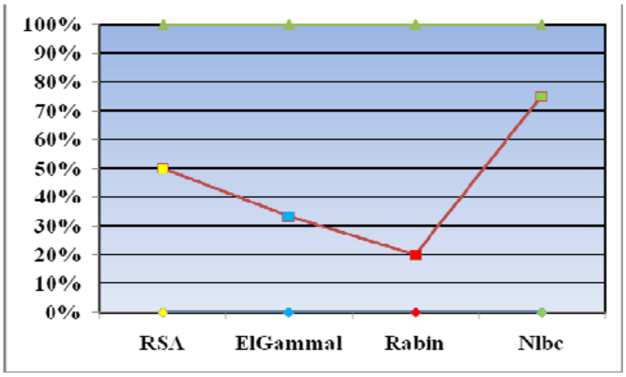


Fig 1. Comparison performance of Encryption

5.2 Decryption analysis

Nlbc decryption is complex without the private key. All the plain text are decrypted using inverse matrix as a key, Therefore it provides security from the unauthorized entities and susceptible. Moreover we are sending secret key through secured channel through key distribution centre or valid entity. Comparing to other algorithm, The RSA algorithm decrypt 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 decrypt using 4 steps to find a feasible solution. In our Nlbc algorithm we receive set of blocks and decrypt in single step. The following table clearly indicates about decryption methods of various algorithms.

Table 9.Comparison of Decryption Cycle

Algorithm	No. of Cipher Text	Decryption cycle
RSA	3	3
ElGammal	3	3
Rabin	3	12
Nlbc	3	1

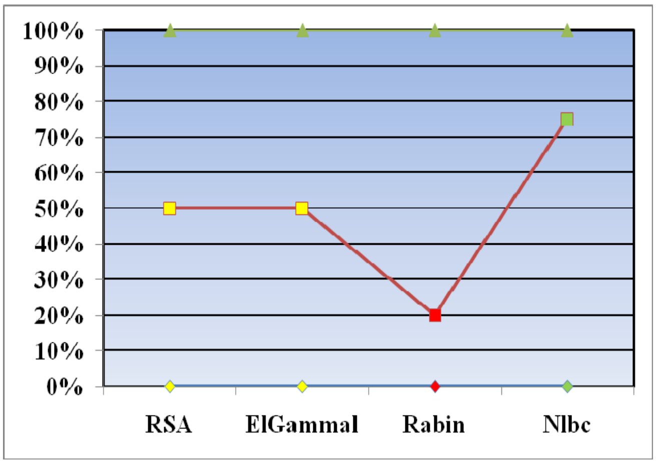


Fig 1. Comparison performance of Decryption

6. Conclusions and Future Work

Our New algorithm using Asymmetric key is based on the block cipher or hill cipher. The hill cipher or linear block cipher's openness to cryptanalysis has rendered it unusable in practice for the public key algorithm.

The reason for selecting linear block cipher for our New algorithm; The linear algebra will not produce same kind of result for the repeated text variable. Also, we can construct 2 block, 3 block square matrix variable each and every time, which will secure our algorithm more. Another advantage for the linear block cipher, we can use negative variable for selecting the square matrix. This negative value make more complicated to the invader. Especially, in this algorithm we are concluding that Symmetric and practically unusable linear block cipher can be made 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 algorithms are working based on the 26 alphabets, especially hill cipher or linear block cipher. In Nlbc, we are extending the text value upto 37.

There are a few highlight points 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. With this Nlbc, we might wish to use the new private key in an identity and video based schemes. Our proposed methods capture the new idea of general usage in commercial sector also. Theoretical challenge is to study proofs of security for key refreshing in the standard model (i.e. with using random keys).

References

[1] John C. Bowman, *Math 422 Coding Theory & Cryptography*, University of Alberta, Edmonton, Canada.

[2] David A. Santos, *Linear Algebra Notes*, January 2, 2010 Revision, dsantos@ccp.edu.

[3] Pranam Paul, Saurabh Dutta, "*An Enhancement of Information Security Using Substitution of Bits Through Prime Detection in Blocks*", Proceedings of National Conference on Recent Trends in Information Systems (ReTIS-06), ,

Organized by IEEE Gold Affinity Group, IEEE Calcutta Section, Computer Science & Engineering Department, CMATER & SRUVM Project- Jadavpur University and Computer Jagat. July 14-15, 2006

[4] Koblitz, N. *A Course in Number Theory and Cryptography*, 2nd ed. New York: Springer-Verlag, 1994.

[5] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[6] Mark Adler and Jean-Loup Gailly,*An Introduction to Cryptography,* released June 8, 2004. www.pgp.com.

[7] Anoop MS, *Public Key Cryptography Applications Algorithms and Mathematical Explanations,* Tata Elxsi Ltd, India, anoopms@tataelxsi.co.in

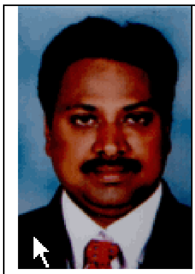
[8] F. Amin, A. H. Jahangir, and H. Rasifard, *Analysis of Public-Key Cryptography for Wireless Sensor Networks Security,World Academy of Science*, Engineering and Technology 2008

[9] Mao, W. *Modern Cryptography: Theory & Practice*. Upper Saddle River (NJ): Prentice Hall Professional Technical Reference, 2004.

[10] Schneier, B. *Applied Cryptography*, 2nd ed. New York: John Wiley & Sons, 1996.

[11] Katos, V. A *Randomness Test for Block Ciphers. Applied Mathematics*, (2005) Elsevier Publications.

[12] William C. Barker , Version 1.1*Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher* Revised NIST Special Publication 800-6719 May 2008.

	**PrakashKuppuswamy** Associated with Department of Computing Science & Technology, Samara University, Ethiopia. He is research Scholar proceeding in ‘Dravidan University’. He has been published few journals /Technical papers and participated many international conference in Rep. of Maldives, Libya and Ethiopia.		**Dr. C. Chandrasekar**, He is Scholar from Periyar University, Salem. He has been working as Reader at Dept. of Computer Science, Periyar University,Tamil Nadu, India. His research interest includes wireless networking, Mobile computing, Computer Communication and Networks. He was a Research guide at various universities in India. He has been published more than 50 technical papers at various National/ International Conference and Journals