African Journal of Mathematics and Computer Science Research Vol. 3(12), pp. 290-296, December 2010
Available online at http://www.academicjournals.org/AJMCSR
ISSN 2006-9731 ©2010 Academic Journals

Review

Key exchange scheme with higher security and its analysis

H. K. Pathak[1] and Manju Sanghi[2]*

[1]S.o.S (Support on Site) in Computer science and (information technology) IT, Pt. Ravishanker Shukla University, Raipur - 492010 (C.G.) Bhilai- 490024 (C.G.) India.
[2]Department of Applied Mathematics, Rungta College of Engineering and Technology, Bhilai- 490024 (C.G.) India.

Accepted 4 October, 2010

Proposed paper gives a secure key exchange scheme using block upper triangular matrices of higher order. By using this method it is possible to generate keys of large orders without the need of large primes thereby avoiding the common ciphertext attacks. The element used for generating shared key is the element of (1, 3) block of the matrix which depends upon the elements of (1, 2) as well as on the (2, 3) blocks thereby increasing the hardness of the problem and providing greater security. Moreover our proposal is compared with the method proposed by Alvarez et al. (2009)

Key words: Block upper triangular matrices, public key cryptography, polynomial matrices, DH key exchange.

INTRODUCTION

With the invention of the World Wide Web and its rapid spread, the need for authentication and secure communication became still more acute. The introduction of the public key cryptography (PKC) by Diffie and Hellman (1976) entirely changed the secure communications. In PKC scheme, a key pair consisting of a public and a private (secret) key is selected so that the problem of deriving the private key from the corresponding public key is equivalent to solving a computational problem that is believed to be intractable. The discrete logarithm problem (DLP) Menezes and Wu (1997) and Stallings (2003), is one such problem upon which the public key crypto-systems are built.

Thus efficiently computable groups where the DLP is hard to break are very important. PKC solves the key exchange problem of establishing a common key between two parties that may have never met. It also finds use in specialized algorithms for digital signatures and message authentication. Many key exchange protocols have been proposed since the DH protocol was proposed which is most popularly used. In this paper we have defined a group of block upper triangular and derived a key exchange protocol which can be used for exchanging keys with greater security. Unlike the key exchange scheme proposed by Alvarez et al. (2005, 2008, 2009), our proposed scheme uses the element of the (1, 3) block of the matrix which depends upon the elements of (1, 2) as well as on the (2, 3) block thereby increasing the hardness of the problem and providing greater security.

DESCRIPTION OF THE SYSTEM

Given p a prime number and r, s, t $\in Z^+$ let $Gl_r(Z_p)$, $Gl_s(Z_p)$ and $Gl_t(Z_p)$ represent invertible matrices of order r×r, s×s and t×t respectively, Z_p being the set of integers modulo p Koblitz (1987). Further let $mat_{r\times s}(Z_p)$, $mat_{r\times t}(Z_p)$ and $mat_{s\times t}(Z_p)$ denote matrices of size r×s, r×t and s×t respectively also with elements in Z_p. We define a set of block upper triangular matrices.

$$\Theta = \left\{ \begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix}, \begin{matrix} A \in Gl_r(\mathbb{Z}_p), B \in Gl_s(\mathbb{Z}_p), \\ C \in Gl_t(\mathbb{Z}_p), X \in mat_{r\times s}(\mathbb{Z}_p), \\ Y \in mat_{r\times t}(\mathbb{Z}_p), Z \in mat_{s\times t}(\mathbb{Z}_p) \end{matrix} \right\}$$

*Corresponding author. E-mail: manjusanghi13@gmail.com.

Theorem 1

The set Θ forms a non-abelian group with respect to multiplication of matrices.

Proof

Closure and associative: Obvious by the definition.

Identity: The identity element is

$$\begin{bmatrix} I_r & 0 & 0 \\ 0 & I_s & 0 \\ 0 & 0 & I_t \end{bmatrix},$$

I_r, I_s and I_t being Identity matrices of order r × r, s × s and t × t respectively.

Inverse: For every element M = $\begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix}$ ∈ Θ there exists an element

$$M^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}XB^{-1} & A^{-1}XB^{-1}ZC^{-1} - A^{-1}YC^{-1} \\ 0 & B^{-1} & B^{-1}ZC^{-1} \\ 0 & 0 & C^{-1} \end{bmatrix}.$$

Also for M_1, M_2 ∈ Θ , $M_1M_2 \neq M_2M_1$.

Theorem 2

Let M = $\begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix}$ ∈ Θ

then for any non negative integer h

$$M^h = \begin{bmatrix} A^h & X^{(h)} & Y^{(h)} \\ 0 & B^h & Z^{(h)} \\ 0 & 0 & C^h \end{bmatrix} \tag{1}$$

where

$$X^{(h)} = \sum_{i=0}^{h-1} A^{h-1-i} X B^i \tag{2}$$

$$Z^{(h)} = \sum_{i=0}^{h-1} B^{h-1-i} Z C^i \ , \tag{3}$$

$$Y^{(h)} = \sum_{i=0}^{h-1} A^{h-1-i} Y C^i + \sum_{\substack{i=0 \\ i+j\leq h-2}}^{h-2} A^i X B^j Z C^{h-i-j-2} \tag{4}$$

Particular case

If X = 0 or Z = 0, then

$$Y^{(h)} = \sum_{i=0}^{h-1} A^{h-1-i} Y C^i . \tag{5}$$

By induction method on h, for h = 2

we have

$$M^2 = \begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix} \begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix}$$

$$= \begin{bmatrix} A^2 & AX + XB & AY + YC + XZ \\ 0 & B^2 & BZ + ZC \\ 0 & 0 & C^2 \end{bmatrix}$$

$$= \begin{bmatrix} A^2 & X^{(2)} & Y^{(2)} \\ 0 & B^2 & Z^{(2)} \\ 0 & 0 & C^2 \end{bmatrix},$$

where $X^{(2)}$ = AX + XB, $Y^{(2)}$ = AY + YC + XZ, $Z^{(2)}$ = BZ + ZC which is true.

Assuming that the above equations are true for h - 1,

So that $M^{h-1} = \begin{bmatrix} A^{h-1} & X^{(h-1)} & Y^{(h-1)} \\ 0 & B^{h-1} & Z^{(h-1)} \\ 0 & 0 & C^{h-1} \end{bmatrix}$

We prove it for h.

Now, $M^h = M.M^{h-1} = \begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix} \begin{bmatrix} A^{h-1} & X^{(h-1)} & Y^{(h-1)} \\ 0 & B^{h-1} & Z^{(h-1)} \\ 0 & 0 & C^{h-1} \end{bmatrix},$

$$= \begin{bmatrix} A^h & AX^{(h-1)} + XB^{h-1} & AY^{(h-1)} + XZ^{(h-1)} + YC^{h-1} \\ 0 & B^h & BZ^{(h-1)} + ZC^{h-1} \\ 0 & 0 & C^h \end{bmatrix}.$$

Considering the term $AY^{(h-1)} + XZ^{(h-1)} + YC^{h-1}$ using equations (2), (3) and (4) we have

$$AY^{(h-1)} + XZ^{(h-1)} + YC^{h-1}$$

$$= A\left(\sum_{i=0}^{h-2} A^{h-2-i} YC^{i} + \sum_{\substack{i=0 \\ i+j \leq h-3}}^{h-3} A^{i} XB^{j} ZC^{h-i-j-3} \right)$$

$$+ X\left(\sum_{i=0}^{h-2} B^{h-2-i} ZC^{i} \right) + YC^{h-1}$$

$$+ \left(\sum_{i=0}^{h-2} XB^{h-2-i} ZC^{i} \right) + YC^{h-1} = \left(\sum_{i=0}^{h-2} A^{h-1-i} YC^{i} + YC^{h-2} \right)$$

$$+ \left(\sum_{\substack{i=0 \\ i+j \leq h-3}}^{h-3} A^{i+1} XB^{j} ZC^{h-i-j-3} \sum_{i=0}^{h-2} XB^{h-2-i} ZC^{i-1} \right)$$

$$= \sum_{i=0}^{h-1} A^{h-1-i} YC^{i} + \sum_{\substack{i=0 \\ i+j \leq h-2}}^{h-2} A^{i} XB^{j} ZC^{h-i-j-2} = Y^{(h)}.$$

which is similar to equation (4). Equations (2) and (3) can be proved in the same way.

Proof of particular case

If either X or Z = 0 then $Y^{(h)} = AY^{(h-1)} + 0 + YC^{h-1}$

$$= \sum_{i=0}^{h-1} A^{h-1-i} YC^{i},$$

which is analogus to Equation (5). This expression is similar to $X^{(h)}$ as obtained by Alvarez et al. (2005,2008). Hence the proposed method can be considered as an extension of Alvarez et al. (2008, 2009), with increased hardness and security. Expressions (2) and (3) can be proved in the same way.

Corollary (1)

If t be any integer such that 0 ≤ t ≤ h, then by easy computation we can obtain

$X^{(h)} = A^{t} X^{(h-t)} + X^{(t)} B^{h-t}$, $Y^{(h)} = A^{t} Y^{(h-t)} + X^{(t)} Z^{(h-t)} + Y^{(t)} C^{h-t}$,

$Z^{(h)} = B^{t} Z^{(h-t)} + Z^{(t)} C^{h-t}$.

In particular if t = 1

$Y^{(h)} = AY^{(h-1)} + XZ^{(h-1)} + YC^{h-1}$.

GENERATION OF HIGHER ORDER ELEMENTS

To get the orders of elements sufficiently large we use the concept of primitive polynomials as given by Odoni and Vardharajan (1984).

Let $f(x) = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} + x^n$

be a monic polynomial in $Z_p[x]$ whose companion n × n matrix is given by

$$\overline{A} = \begin{bmatrix} 0 & 1 & 0 & ... & 0 & 0 \\ 0 & 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & ... & 1 & 0 \\ 0 & 0 & 0 & ... & 0 & 1 \\ -a_0 & -a_1 & -a_2 & ... & -a_{n-2} & -a_{n-1} \end{bmatrix}.$$

If f is a primitive polynomial in $Z_p[x]$ then the order of the matrix $\overline{A}$ is equal to the order of any root of f in $F_p{}^n$ and the order of $\overline{A}$ divides p^{n-1}.Moreover assuming that f is a primitive polynomial in Zp[x] the order of is exactly pn-1. We define

$$\overline{A} = \begin{pmatrix} \overline{A}_1 & 0 & \cdots & 0 \\ 0 & \overline{A}_2 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \overline{A}_k \end{pmatrix}$$

proposed by Odoni where $\overline{A}$ is the companion matrix of f_i. The order of each block $\overline{A}_i$ is $p^{n}{}_{i}$ -1 for i =1, 2...k. Therefore the order of $\overline{A}$ is lcm ($p^{n}{}_{1}$ -1, $p^{n}{}_{2}$ -1,... , $p^{n}{}_{k}$ -1).

If Q is any invertible matrix then A can be defined as A = $Q\overline{A}Q^{-1}$ with the same order as $\overline{A}$

Let $f(x) = a_0 + a_1x + a_2x^2 + ... + a_{r-1}x^{r-1} + x^r$,

$g(x) = b_0 + b_1x + b_2x^2 + ... + b_{s-1}x^{s-1} + x^s$,

$h(x) = c_0 + c_1x + c_2x^2 + ... + c_{t-1}x^{t-1} + x^t$,

be primitive polynomials in $Z_p[x]$ and $\overline{A}, \overline{B}, \overline{C}$ be the corresponding companion matrices. Let Q, R, S be

Table 1. Values of order of M in bits for large values of p.

r	s	t	p=2^{50}bits	p=2^{80}bits	p=2^{100}bits
2	3	5	2^{400}	2^{640}	2^{800}
3	4	7	2^{600}	2^{960}	2^{1200}
3	5	8	2^{700}	2^{1120}	2^{1400}
4	5	9	2^{800}	2^{1280}	2^{1600}
5	6	11	2^{1000}	2^{1600}	2^{2000}

Table 2. Values of order of M in bits for small values of p.

r	s	t	p=3bits	p=7bits	p=11bits
31	32	29	2^{145}	2^{230}	2^{302}
47	48	41	2^{219}	2^{348}	2^{457}
60	61	59	2^{279}	2^{445}	2^{584}
130	131	127	2^{605}	2^{963}	2^{1264}
216	217	207	2^{1004}	2^{1599}	2^{2099}

Table 3. Comparison of o(M) by Alvarez et.al and proposed method.

p(bits)	r	s	t	o(M_A)bits	o(M_P) bits
5	31	32	29	2^{145}	2^{209}
13	130	131	127	2^{963}	2^{1429}
29	216	217	207	2^{2099}	2^{3059}
2^{100}	3	4	7	2^{600}	2^{1200}
2^{160}	4	5	9	2^{1280}	2^{2560}
2^{200}	5	6	11	2^{2000}	2^{4000}

invertible matrices and let

$$A = P\overline{A}P^{-1}, B = Q\overline{B}Q^{-1}, C = R\overline{C}R^{-1}$$

Then the order of M $\in \Theta$ is given by

o(M) = lcm (p^r -1, p^s -1, p^t -1)

which will be maximum if p^r-1, p^s-1 and p^t-1are relatively prime.

Tables 1 and 2 gives the values of order of M in bits obtained for small and large values of p. In Table 3 column o(M_A) gives the order of the matrix M obtained by Alvarez et al. (2009), for different values of p, r and s and the column o(M_P) gives the values obtained by our proposed method for different values of p, r, s and t. For example for p = 2^{200} bits by taking r = 5 and s = 6 the order of the matrix obtained by Alvarez et al. (2005) is 2^{2000} bits which is indeed very large but by adding a matrix of order t = 11 the order of M obtained by our proposed method is 2^{4000} which is double the value obtained by Alvarez et al. (2009)

KEY EXCHANGE SCHEME

The two parties Alice and Bob who wish to exchange their secret data first generate a shared key for which they perform the following steps.

1. First Alice and Bob agree on two square matrices

$$M_1 = \begin{bmatrix} A_1 & X_1 & Y_1 \\ 0 & B_1 & Z_1 \\ 0 & 0 & C_1 \end{bmatrix} \text{ and } M_2 = \begin{bmatrix} A_2 & X_2 & Y_2 \\ 0 & B_2 & Z_2 \\ 0 & 0 & C_2 \end{bmatrix}$$

of orders m_1 and m_2 respectively.

2. Alice generates two private keys r, s $\in Z^+$ where $1 \le r \le m_1$, $1 \le s \le m_2$ computes $C = M_1^r M_2^s$

$$= \begin{bmatrix} A_1^r & X_1^{(r)} & Y_1^{(r)} \\ 0 & B_1^r & Z_1^{(r)} \\ 0 & 0 & C_1^r \end{bmatrix} \begin{bmatrix} A_2^s & X_2^{(s)} & Y_2^{(s)} \\ 0 & B_2^s & Z_2^{(s)} \\ 0 & 0 & C_2^s \end{bmatrix}$$

$$= \begin{bmatrix} A_C & X_C & Y_C \\ 0 & B_C & Z_C \\ 0 & 0 & C_C \end{bmatrix}$$

and sends C to Bob as her public key.

3. Bob also generates private keys $1 \le u \le m_1$ and $1 \le v \le m_2$ computes

$D = M_1^u M_2^v$

$$= \begin{bmatrix} A_1^u & X_1^{(u)} & Y_1^{(u)} \\ 0 & B_1^u & Z_1^{(u)} \\ 0 & 0 & C_1^u \end{bmatrix} \begin{bmatrix} A_2^v & X_2^{(v)} & Y_2^{(v)} \\ 0 & B_2^v & Z_2^{(v)} \\ 0 & 0 & C_2^v \end{bmatrix}$$

$$= \begin{bmatrix} A_D & X_D & Y_D \\ 0 & B_D & Z_D \\ 0 & 0 & C_D \end{bmatrix}$$

and sends D as his public key.

4. Alice calculates $K_a = A_1^r A_D Y_2^{(s)} + (A_1^r X_D + X_1^{(r)} B_D) Z_2^{(s)} + (A_1^r Y_D + X_1^{(r)} Z_D + Y_1^{(r)} C_D) C_2^S$

5. Bob calculates $K_b = A_1^u A_C Y_2^{(v)} + (A_1^u X_C + X_1^{(u)} B_C) Z_2^{(v)} + (A_1^u Y_C + X_1^{(u)} Z_C + Y_1^{(u)} C_C) C_2^v$

Shared key is $K_a = K_b$

Theorem 3

With the above notation $K_a = K_b$

Proof

Let

$$M_1 = \begin{bmatrix} A_1 & X_1 & Y_1 \\ 0 & B_1 & Z_1 \\ 0 & 0 & C_1 \end{bmatrix} \text{ and } M_2 = \begin{bmatrix} A_2 & X_2 & Y_2 \\ 0 & B_2 & Z_2 \\ 0 & 0 & C_2 \end{bmatrix}$$

$$C = M_1^r M_2^s = \begin{bmatrix} A_C & X_C & Y_C \\ 0 & B_C & Z_C \\ 0 & 0 & C_C \end{bmatrix}$$

$$D = M_1^u M_2^v = \begin{bmatrix} A_D & X_D & Y_D \\ 0 & B_D & Z_D \\ 0 & 0 & C_D \end{bmatrix}$$

$$\begin{aligned} M_a &= M_1^r D M_2^s \\ &= M_1^r M_1^u M_2^v M_2^s \\ &= M_1^u M_1^r M_2^s M_2^v \\ &= M_1^u \, C \, M_2^v \\ &= M_b \end{aligned}$$

$$\text{Also, } M_a = \begin{bmatrix} A_a & X_a & K_a \\ 0 & B_a & Z_a \\ 0 & 0 & C_a \end{bmatrix}$$

$$M_b = \begin{bmatrix} A_b & X_b & K_b \\ 0 & B_b & Z_b \\ 0 & 0 & C_b \end{bmatrix}$$

Hence $K_a = K_b$.

Data encryption and decryption

1. Alice encrypts the message in the form of matrices Δ_1 and Δ_2 of order r×s such that

$\Delta = (\Delta_1 + \Delta_2) \bmod 2$.

Here the message Δ is broken into 2 matrices Δ_1 and Δ_2 in which the integers are encoded as follows. 1 in Δ_1 is encoded as 1+0 or 0+1 so that 1 and 0 are put in two different matrices Δ_1 and Δ_2. Similarly 0 in Δ is encoded as 1+1 so that each 1 is entered in Δ_1 and Δ_2.

2. Generates the matrices

$$T_1 = \begin{bmatrix} A_1 & \Delta_1 & K_a \\ 0 & B_1 & Z_1 \\ 0 & 0 & C_1 \end{bmatrix} \quad T_2 = \begin{bmatrix} A_2 & \Delta_2 & K_a \\ 0 & B_2 & Z_2 \\ 0 & 0 & C_2 \end{bmatrix}$$

3. Computes the cipher text $\beta_1 = M_1^r T_1$, $\beta_2 = M_1^s T_2$, r and s being the private keys of Alice and sends this to Bob.

4. Bob computes $\beta_1 M_2^u$ and $\beta_2 M_2^v$ by taking u and v as his private key and sends it back to Alice.

5. Alice computes $M_1^{-r} \beta_1 M_2^u$ and $M_1^{-s} \beta_2 M_2^v$ and sends $T_1 M_2^u$ and $T_2 M_2^v$ to Bob.

Table 4. Execution time for different sizes.

r	s	t	p	o(M)bits	Time(s)
2	3	271	5167	1024	1.54
2	3	293	3197	1024	1.7
3	5	297	3127	1024	1.85
3	5	319	2567	1024	1.96
5	7	319	1867	1024	2.11
5	7	397	1237	1024	2.41

6. Bob finally calculates $T_1M_2^{u}M_2^{-u} = T_1$ and $T_2M_2^{v}M_2^{-v} = T_2$ gets the blocks Δ_1 , Δ_2 and the shared key K_a .
7. Bob compares $K_a = K_b$ and if this is true decodes the message $(\Delta_1 + \Delta_2) \bmod 2 = \Delta$.

Table 4 and Figure 1 give the execution time required for calculating the values of order of M. The time is calculated by using gmp library by taking the values of r, s, t and the required values of p for getting the order of about 1024 bits which is the minimum key size for being secured.

Security analysis

Tables 1 and 2 show that matrices of very large orders greater than 1024 bits can be generated easily by using small primes and hence the present scheme is infeasible against the Brute force attacks.

Menezes and Wu (1997), gave he algorithm for the cryptanalysis of the protocols based on matrix powers in which the discrete logarithm problem $\gamma = M^r$ can be broken into simpler discrete logarithms over finite fields. This concept cannot be applied to this scheme as simple powers of matrices are not used as public key instead product of powers of two different matrices $C = M_1^rM_2^s$ is published.

By the Climent et al. (2007) technique, based on Cayley Hamilton theorem the private keys can be retrieved by solving the DLP in a finite field only if the matrices M_1 and M_2 share a common eigenvalue. It can be proved that this technique is also invalid for our present scheme.

Let $M = \begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix} \in Gl_n(Z_p)$

where n= r + s+ t Then the characteristic polynomials of the matrices M_1 and M_2 are given by $\chi_{M_1}(\lambda) = \det(M_1-\lambda I_n)$, I_n being the identity matrix of size n.

$$= \begin{vmatrix} A_1-\lambda I & X_1 & Y_1 \\ 0 & B_1-\lambda I & Z_1 \\ 0 & 0 & C_1-\lambda I \end{vmatrix}$$

= (A1-λI) [(B1-λI) (C1-λI)]

$$= a_0 + a_1\lambda + a_2\lambda^2 + \ldots\ldots + a_{n-1}\lambda^{n-1} + a_n\lambda^n.$$

$$\chi_{M_2}(\lambda) = \det(M_2-\lambda I_n)$$

$$= \begin{vmatrix} A_2-\lambda I & X_2 & Y_2 \\ 0 & B_2-\lambda I & Z_2 \\ 0 & 0 & C_2-\lambda I \end{vmatrix}$$

$$= (A_2-\lambda I)\,[\,(B_2-\lambda I)\,(C_2-\lambda I)\,]$$

$$= b_0 + b_1\lambda + b_2\lambda^2 + \ldots\ldots + b_{n-1}\lambda^{n-1} + b_n\lambda^n.$$

By Cayley Hamilton theorem

Since $\chi_{M_1}(\lambda) = \chi_{M_2}(\lambda) = 0$

$$a_0I + a_1M_1 + a_2M_1^2 + \ldots. + a_{n-1}M_1^{n-1} + a_nM_1^n = 0$$

$$(a_0/a_n)\,I + (a_1/a_n)M_1 + (a_2/a_n)\,M_1^2 + \ldots\ldots +$$

$$(a_{n-1}/a_n)\,M_1^{n-1} + (a_n/a_n)M_1^n = 0$$

$$M_1^n = b_0I + b_1M_1 + b_2M_1^2 + \ldots\ldots + b_{n-1}M_1^{n-1}$$

where $b_0 = -(a_0/a_n)$, $b_1 = -(a_1/a_n)$, ...,

$b_{n-1} = -(a_{n-1}/a_n)$.

Hence

$$M_1^h = \begin{bmatrix} A_1^h & X_1^{(h)} & Y_1^{(h)} \\ 0 & B_1^h & Z_1^{(h)} \\ 0 & 0 & C^h \end{bmatrix}$$

$$= b_0 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + b_1 \begin{bmatrix} A_1 & X_1 & Y_1 \\ 0 & B_1 & Z_1 \\ 0 & 0 & C_1 \end{bmatrix}$$

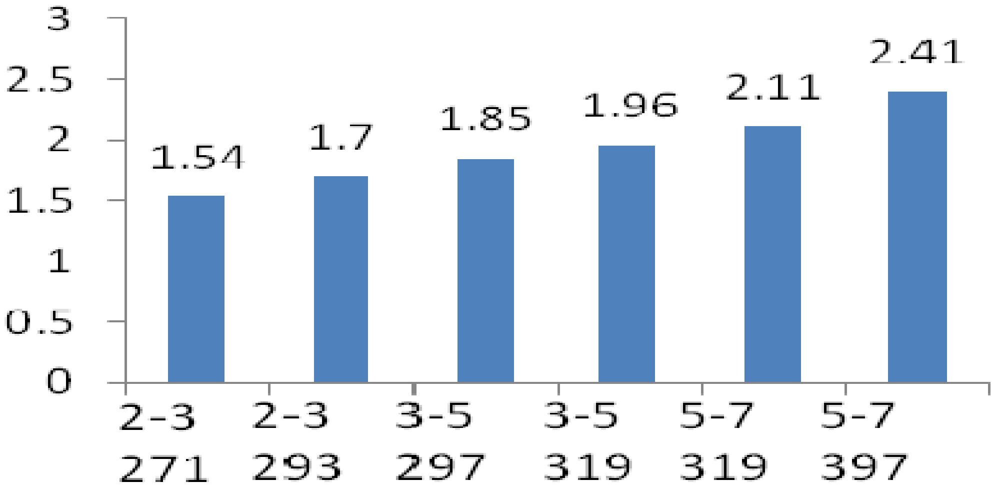

Figure 1. Execution time for different sizes.

$$+ b_2\begin{bmatrix} A_1 & X_1 & Y_1 \\ 0 & B_1 & Z_1 \\ 0 & 0 & C_1 \end{bmatrix}^2 + \text{..........}+b_{n-1}\begin{bmatrix} A_1 & X_1 & Y_1 \\ 0 & B_1 & Z_1 \\ 0 & 0 & C_1 \end{bmatrix}^{n-1} .$$

Consequently we get

$A_1^h = b_0 + b_1 A_1 + b_2A_1^2 + ...+b_{n-1}A_1^{n-1}$,

$B_1^h = b_0 + b_1 B_1 + b_2B_1^2 + ...+b_{n-1} B_1^{n-1}$,

$C_1^h = b_0 + b_1 C_1 + b_2C_1^2 + ...+b_{n-1} C_1^{n-1}$,

$Y_1^{(h)} = b_1Y_1 + b_2Y_1^{(2)} + ...+b_{n-1}Y_1^{(n-1)}$.

So the problem of getting private keys r, s from the public key $C = M_1^r M_2^s$ in the resent scheme is similar to solving the linear equations

$M_1^r = c_0I+ c_1M_1 + c_2M_1^2+ .....+ c_{n-1}M_1^{n-1}$,

$M_2^s = d_0I+ d_1M_2 + d_2M_22+ .....+ d_{n-1}M_2^{n-1}$,

$c_0, c_1, ... c_{n-1}, d_0, d_1,....,d_{n-1}, M_1^r$ and M_2^s being unknown.

CONCLUSION

In this paper we have proposed a new key exchange scheme and data encryption method based on block matrices. For this purpose we have defined a non abelian group of block upper triangular matrices of higher order. The main purpose of this scheme is to increase the hardness of the problem and provide greater security. We can generate matrices of very high orders by using very small values of p (not necessarily primes) thereby avoiding the common attacks. The scheme is also analyzed against the attacks based on Cayley Hamilton theorem.

REFERENCES

Alvarez R, Tortosa L, Vicent JF, Zamora (2005). A Public Key Cryptosystem based on Block upper Triangular Matrices. WSEAS Information security and Privacy, pp. 163-168.

Alvarez R, Tortosa L, Vicent JF, Zamora (2009). Analysis and design of a secure key exchange scheme. Inf. sci., 179: 2014-2021.

Alvarez R, Ferrandez F, Vicent JF, Zamora (2006). Applying quick Exponentiation for block upper triangular matrices. Appl. Math. Comput., 183: 729- 737.

Alvarez R, Vicent JF, Zamora A (2008). Matricial public key cryptosystem with digital signature. WSEAS Trans. Math., 4: 195-204.

Climent J, Gorla E, Rosenthal J (2007). Cryptanalysis of the CFVZ cryptosystem. Advances in Mathematics of Communications. 1: 1-11.

Diffie W, Hellman (1976). New directions in Cryptography. IEEE Trans. Inf. Theory, 22: 644-654.

Koblitz N (1987). A Course in Number Theory and Cryptography. Springer-Verlag.

Menezes A Wu YH (1997). The discrete logarithm problem in gl(n,q). Arts Combinatoria, 47: 22-32.

Odoni RWK, Varadharajan V, Sanders PW (1984). Public Key Distribution in Matrix Rings. Electron. Lett., 20: 386- 387.

Stallings W (2003). Cryptography and Network Security. Principles and Practice, Third Edition., Prentice Hall, New Jersey.