ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 2, No. 4, 56-58 (2016)
www.astesj.com

ASTES Journal
ISSN: 2415-6698

Matrix Encryption Scheme

Abdelhakim Chillali*

Sidi Mohamed Ben Abdellah University, Mathematics Physics and Computer Science, LSI, FP, Taza, Morocco

ARTICLEINFO

Article history:
Received: 12 April, 2017
Accepted: 04 May, 2017
Online: 14 May, 2017

Keywords:
Public key cryptography
Discrete logarithm problem
Finite field

ABSTRACT

In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra. In this work, we proposed a new problem applicable to the public key cryptography, based on the Matrices, called "Matrix discrete logarithm problem", it uses certain elements formed by matrices whose coefficients are elements in a finite field. We have constructed an abelian group and, for the cryptographic part in this unreliable group, we then perform the computation corresponding to the algebraic equations, Returning the encrypted result to a receiver. Upon receipt of the result, the receiver can retrieve the sender's clear message by performing the inverse calculation.

1 Introduction

Public key cryptographic is the fundamental technology in secure communications. It was devised by Diffie and Hellman in 1976 to secret key distribution. The mathematical problems more used are the discrete logarithm problem (DLP). In 1985 the elliptic curve discrete logarithm problem (ECDLP) was proposed independently by Koblitz and Miller. In this paper, we present the Matrix discrete logarithm problem in a new cryptographic scheme. Consider a finite field $L = \mathbb{F}_q$, where q is a power of p the characteristic of L.[1, 2, 3]
Throughout this work, we denote:
L^* multiplicative group *of* L.
Let $a, b \in L^*$ and let $x, y \in L$,

$$M_y^x = \begin{pmatrix} \frac{x}{a} - 1 & \frac{y}{b} - 1 \\ \frac{y}{b} + 1 & \frac{x}{a} + 1 \end{pmatrix}$$

$$G = \{M_y^x / det(M_y^x) = 1\}$$

$$G_q = G \mod p.$$

$$M_{y_1}^{x_1} \triangle M_{y_2}^{x_2} = M_{y_3}^{x_3}$$

where,

$$(1): \begin{cases} x_3 = \frac{b^2 x_1 x_2 + a^2 y_1 y_2}{ab^2} \\ y_3 = \frac{x_1 y_2 + x_2 y_1}{a} \end{cases}$$

$$M_k = \begin{pmatrix} \frac{k^2+1}{2k} - 1 & \frac{k^2-1}{2k} - 1 \\ \frac{k^2-1}{2k} + 1 & \frac{k^2+1}{2k} + 1 \end{pmatrix}, k \in L^*.$$

$$m = |G_q|$$

The next theorem whose proof is evident.

Theorem 1 *The set G_q with the operator $\triangle$ defined by* (1) *is a abelian group.*
The identity element is M_0^a, that if $M = M_y^x$ then $N = M_{-y}^x$ is the invertible element of M.

Remark 1 *The MDLP consists of following for two elements $M, N \in G_q$, determine the scaler $k \in \mathbb{Z}_m$ such that $M^{\triangle k} = N$. It is necessary that M be a generator of the group G_q.*

Assumption 1 *Given a group G_q and tow elements M and $N \in G_q$, there exists non polynomial time algorithm $\theta(logq)$ deciding the integer k such that $M^{\triangle k} = N$ if such a k exists.*

Assumption 2 *Given a group G_q and $\theta(logq)$ elements N_i on G_q, there exists non polynomial time algorithm $(\theta(logq))$ deciding the integers k_i, such that*

$$N_1^{\triangle k_1} \triangle N_2^{\triangle k_2} \triangle ..... \triangle N_{\theta(logq)}^{\triangle k_{\theta(logq)}} = M$$

if such k_i exist, where M is a random element on G_q.

*Abdelhakim Chillali , FP , Taza, Morocco & abdelhakim.chillali@usmba.ac.ma

https://dx.doi.org/10.25046/aj020408

2 Matrix Cryptosystem

2.1 Key distribution protocols

Let M_y^x be a generator of the group G_q.
Alice take a private key $1 < l < m$, and computes $M_{y_l}^{x_l} = M_y^{x \triangle l}$, then she transmits $M_{y_l}^{x_l}$ to Bob.
Similar, Bob takes a private key $1 < t < m$, and computes $M_{y_t}^{x_t} = M_y^{x \triangle t}$ and transmits $M_{y_t}^{x_t}$ to Alice.
In the same way Alice and Bob compute $M_{y_{tl}}^{x_{tl}} = M_{y_t}^{x_t \triangle l}$ and $M_{y_{lt}}^{x_{lt}} = M_{y_l}^{x_l \triangle t}$ respectively.

Theorem 2

$$\frac{x_{lt}}{a} + \frac{y_{lt}}{b} = \frac{x_{tl}}{a} + \frac{y_{tl}}{b} \mod p$$

The secret key is $\alpha = \frac{x_{tl}}{a} + \frac{y_{tl}}{b} \mod p$

2.2 Description of This Cryptosystem

Let $L = \mathbb{F}_q$ with $q = p^n$.
1)Space of lights: $P = G_q$.
2)Space of quantified: $C = G_q$.
3)Space of the keys: $K = L^*$.
4)Function of encryption:$\forall \alpha \in K$,

$$e_\alpha : \left| \begin{array}{ccc} P & \longrightarrow & C \\ M_y^x & \longmapsto & e_\alpha\,(M_y^x) = M_y^x \triangle M_\alpha \end{array} \right.$$

5)Function of decryption:$\forall \alpha \in K$,

$$d_\alpha : \left| \begin{array}{ccc} C & \longrightarrow & P \\ M_y^x & \longmapsto & d_\alpha(M_y^x) = M_y^x \triangle M_{-\alpha} \end{array} \right.$$

Remark 2

$$d_\alpha o e_\alpha(M_y^x) = M_y^x \triangle M_\alpha \triangle M_{-\alpha} = M_y^x$$

Remark 3 *a) Secret key :α*
b) Public keys:
1) Space of lights; P
2) Space of quantified; C
3) Space of the keys; K
4) Generator of the group P; M_y^x
5) Function of encryption; e_α
6) Function of decryption; d_α

Remark 4 *The $M_{y_l}^{x_l}$, $M_{y_t}^{x_t}$ and m are public and can known by another person, but to obtain the private key α, it is necessary to solve the Matrix problem discrete logarithm in G_q, what returns the discovery of the difficult key α.*

2.3 Numerical Example

Alice and Bob Choose the following public numbers; $p = 41$, $a = 2$, $b = 5$, and $n = 1$. They determine the group $G_{41} =< M_{31}^{26} >$, with the identity element M_0^2.

1) Exchange of the key deprived between Alice and Bob:
Alice take a private key; $l = 13 < 39$, calculation; $M_{23}^{13} = M_{31}^{26 \triangle 13}$ and send to Bob M_{23}^{13}. In turn, Bob take a private key; $t = 21 < 39$, calculation; $M_{10}^{15} = M_{31}^{26 \triangle 21}$ and send it to Alice. Alice and Bob calculate separately : $M_{18}^{13} = M_{10}^{15 \triangle 13}$ and $M_{18}^{13} = M_{23}^{13 \triangle 21}$. They determine their secret key:

$$\alpha = \frac{13}{2} + \frac{18}{5} = 6 \mod 41$$

2) Message to send:
Alice wants to send the following message

$$me = \{M_{18}^{28}, M_4^0, M_{27}^{23}, M_{36}^{34}\}$$

It encrypts it using the encryption function

M_y^x	$e_6(M_y^x)$
M_{18}^{28}	$\begin{pmatrix} 39 & 40 \\ 1 & 0 \end{pmatrix}$
M_4^0	$\begin{pmatrix} 15 & 37 \\ 39 & 17 \end{pmatrix}$
M_{27}^{23}	$\begin{pmatrix} 28 & 13 \\ 17 & 30 \end{pmatrix}$
M_{36}^{34}	$\begin{pmatrix} 28 & 25 \\ 27 & 30 \end{pmatrix}$

3) Message received:
Bob receives message crypt send by Alice

$$mr = \{\begin{pmatrix} 28 & 25 \\ 27 & 30 \end{pmatrix}, \begin{pmatrix} 28 & 13 \\ 17 & 30 \end{pmatrix}, \begin{pmatrix} 15 & 37 \\ 39 & 17 \end{pmatrix}, \begin{pmatrix} 39 & 40 \\ 1 & 0 \end{pmatrix}\}$$

It decrypts it using the decryption function

M_y^x	$d_6(M_y^x)$
$\begin{pmatrix} 39 & 40 \\ 1 & 0 \end{pmatrix}$	M_{18}^{28}
$\begin{pmatrix} 15 & 37 \\ 39 & 17 \end{pmatrix}$	M_4^0
$\begin{pmatrix} 28 & 25 \\ 27 & 30 \end{pmatrix}$	M_{36}^{34}
$\begin{pmatrix} 28 & 13 \\ 17 & 30 \end{pmatrix}$	M_{27}^{23}

3 Example for cryptography

In this example we take $p = 3$, $a = b = 1$, $n = 3$, and α root of the polynomial $X^3 + 2X + 1$. We have $P = G_{27}$, $C = G_{27}$, and $K = \mathbb{F}_{27}^*$ and $M_{\alpha^2}^{2\alpha+2}$ is a generator of the group P.

1) Exchange of the key deprived:
Alice take a private key $l = 12 < 25$, send to Bob $M_{\alpha^2}^{\alpha+1} = M_{\alpha^2}^{2\alpha+2 \triangle l}$. Bob take a private key $t = 20 < 25$, send to Alice $M_{2\alpha^2+\alpha+1}^{2\alpha^2+2} = M_{\alpha^2}^{2\alpha+2 \triangle t}$. Their secret key is

$$\beta = 2\alpha^2 + 2 + \alpha^2 + 2\alpha + 2 = 2\alpha + 1.$$

2) Message Encryption:
It is known that the encryption functions and the decryption functions are defined by:

$$e_\beta(M_y^x) = M_y^x \triangle M_{\alpha^2+2\alpha+2}^{2\alpha^2+2}$$

$$d_\beta(M_y^x) = M_y^x \triangle M_{2\alpha^2+\alpha+1}^{2\alpha^2+2}$$

Lets $x = i\alpha^2 + j\alpha + k$ and $y = l\alpha^2 + m\alpha + n$, we denote M_y^x by $ijklmn$.

Each letter is represented by a $ijklmn$ character. Often the simple The scheme a = 001000, b = 010112, ..., z = 221102 is used, but this is Not an essential feature of encryption. To encrypt a message, each letter will be decrypted by the decryption function, for a message one obtains a block of n letters (considered as an n-component vector). Consider the message 'bonjour' Which will be encrypted by the message: "crvzrng".

Table of the Symbol Encryption

M_y^x	Symbol	$e_\beta(M_y^x)$	Encrypt Symbol
001000	a	202120	h
010112	b	010220	c
010220	c	012210	d
012210	d	211110	s
012122	e	010112	b
122110	f	021210	q
122222	g	112102	m
202120	h	011101	j
202212	i	001000	a
011101	j	221102	z
011201	k	202212	i
112200	l	122110	f
112102	m	022101	w
002001	n	101212	v
020112	o	021122	r
020220	p	020112	o
021210	q	020220	p
021122	r	122222	g
211110	s	221200	y
211222	t	012122	e
101120	u	002001	n
101212	v	022201	x
022101	w	101120	u
022201	x	112200	l
221200	y	011201	k
221102	z	211222	t

4 Conclusion

Although matrix multiplication can not provide security for the encryption of a message [4, 5, 6], we have been able to construct a law of internal composition other than the law of multiplication, which allows us to create a cryptography on the matrices and which is safer for a key of reasonable length.

References

1. *A. Chillali, "Cryptography over elliptic curve of the ring $Fq[e]$, $e^4 = 0$.", World Academy of Science, Engineering and Technology., **78** , 848-850, 2011.*
2. *A. Tadmori, A. Chillali, M. Ziane, "The binary operations calculus in $E_{a,b,c}$.", International Journal of Mathematical Models and Methods in Applied Sciences., **9** , 171-175, 2015.*
3. *A. Tadmori, A. Chillali, M. Ziane, "Elliptic Curve over Ring A_4.", Applied Mathematical Sciences., **35**(9), 1721-1733, 2015.*
4. *Lester S. Hill, "Cryptography in an Algebraic Alphabet.", The American Mathematical Monthly., **36**, 1929.*
5. *Lester S. Hill, "Concerning Certain Linear Transformation Apparatus of Cryptography.", The American Mathematical Monthly., **38**(9), 1931.*
6. *Christos Koukouvinos and Dimitris E. Simos, "Encryption Schemes based on Hadamard Matrices with Circulant Cores.", Journal of Applied Mathematics and Bioinformatics., **1**(3), 17-41, 2013.*