Bol. Soc. Paran. Mat.
©SPM –ISSN-2175-1188 ON LINE
SPM: www.spm.uem.br/bspm

(3s.) **v. 37** 3 (2019): 75–83.
ISSN-00378712 IN PRESS
doi:10.5269/bspm.v37i3.34542

Cryptography Based on the Matrices

M. Zeriouh, A. Chillali and A. Boua

ABSTRACT: In this work we introduce a new method of cryptography based on the matrices over a finite field $\mathbb{F}_q$, were q is a power of a prime number p. The first time we construct the matrix $M = \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix}$ were A_1, A_2 and A_3 are matrices of order n with coefficients in $\mathbb{F}_q$ and 0 is the zero matrix of order n. We prove that $M^l = \begin{pmatrix} A_1^l & (A_2)_l \\ 0 & A_3^l \end{pmatrix}$ were $(A_2)_l = \sum_{k=0}^{l-1} A_1^{l-1-k} A_2 A_3^k$ for all $l \in \mathbb{N}^*$. After we will make a cryptographic scheme between the two traditional entities Alice and Bob.

Key Words: Matrices, Conjugate Problem, Exchange of Keys, Cryptosystem.

Contents

1. Introduction

Cryptography, the science of encrypting and deciphering messages written in secret codes, has played a vital role in securing information since ancient times. In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929 (see [4] and [5]), it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once. The following discussion assumes an elementary knowledge of matrices, not to mention cryptography based on elliptic curves, for more details see the following references [1], [2] and [3]. The article entitled-Encryption Schemes based on Hadamard Matrices with Circulant Cores-Christos Koukouvinos and Dimitris E. Simos propose in [6] two encryption schemes based on Hadamard matrices with one and two circulant cores. This article describes an activity built around one of the techniques that illustrates an application of

Submitted December 14, 2016. Published April 10, 2017

matrices.
A cipher's strength is determined by the computational power needed to break it. The computational complexity of an algorithm is measured by two variables: T for time complexity which specifies how the running time depends on the size of the input, and S for space complexity or memory requirement. Both T and S are commonly expressed as functions of n, when n is the size of the input. Generally, the computational complexity of an algorithm is expressed in what is called " big $\mathcal{O}$ " notation; the order of magnitude of the computational complexity. We use $\mathcal{O}$-notation to give an upper bound on a function, to within a constant factor [7]. $\mathcal{O}$-notation For a given function $g(n)$ we denote by $\mathcal{O}(g(n))$ the set of functions

$$\mathcal{O}(g(n)) = \big\{f(n)|\exists \text{ constants } c, n_0 \geq 0 \text{ such that } 0 \leq f(n) \leq cg(n) \text{ for all } n \geq n_0\big\}.$$

We give a necessary brief definition for an encryption scheme.

Definition 1.1. [8] *An encryption scheme consists of three sets: a key set K, a message set M, and a ciphertext set C together with the following three algorithms.*

(i) *A key generation algorithm, which outputs a valid encryption key $k \in K$ and a valid decryption key $k^{-1} \in K$.*

(ii) *An encryption algorithm, which takes an element $m \in M$ and an encryption key $k \in K$ and outputs an element $c \in C$ defined as $c = E_k(m)$.*

(iii) *A decryption function, which takes an element $c \in C$ and a decryption key $k^{-1} \in K$ and outputs an element $m \in M$ defined as $m = D_{k^{-1}}(c)$. We require that $D_{k^{-1}}(E_k(m)) = m$.*

2. The matrices $M_B(X, Y)$

In this section, we present the theoretical concept for our encryption scheme by using the Block matrix $M_B(X, Y)$ in the following form: $M_B(X, Y) = \begin{pmatrix} X & B \\ 0 & Y \end{pmatrix}$ where B, X, Y are three square matrices of same order.

Lemma 2.1. *Let $M_B(X, Y) = \begin{pmatrix} X & B \\ 0 & Y \end{pmatrix}$ where B, X, Y are three square matrices of same order. Then $(M_B(X, Y))^l = \begin{pmatrix} X^l & B_l \\ 0 & Y^l \end{pmatrix}$ for all $l \in \mathbb{N}^*$ with $B_l = \sum_{k=0}^{l-1} X^{l-1-k} B Y^k$.*

Proof. It is obvious that

$$\begin{aligned} (M_B(X, Y))^1 &= \begin{pmatrix} X^1 & B_1 \\ 0 & Y^1 \end{pmatrix} \\ &= \begin{pmatrix} X & B \\ 0 & Y \end{pmatrix} \\ &= M_B(X, Y), \end{aligned}$$

then our Lemma is true for $l = 1$.
We assume the recurrence hypothesis: $(M_B(X,Y))^l = \begin{pmatrix} X^l & B_l \\ 0 & Y^l \end{pmatrix}$, for certain l, and we prove that:
$(M_B(X,Y))^{l+1} = \begin{pmatrix} X^{l+1} & B_{l+1} \\ 0 & Y^{l+1} \end{pmatrix}$ were $B_{l+1} = \sum_{k=0}^{l} X^{l-k} B Y^k$.
We have

$$\begin{aligned}
(M_B(X,Y))^{l+1} &= (M_B(X,Y))^l . M_B(X,Y) \\
&= \begin{pmatrix} X^l & \sum_{k=0}^{l-1} X^{l-1-k} B Y^k \\ 0 & Y^l \end{pmatrix} \cdot \begin{pmatrix} X & B \\ 0 & Y \end{pmatrix} \\
&= \begin{pmatrix} X^{l+1} & X^l B + (\sum_{k=0}^{l-1} X^{l-1-k} B Y^k) Y \\ 0 & Y^{l+1} \end{pmatrix} \\
&= \begin{pmatrix} X^{l+1} & X^l B Y^0 + \sum_{k=0}^{l-1} X^{l-(k+1)} B Y^{k+1} \\ 0 & Y^{l+1} \end{pmatrix} \\
&= \begin{pmatrix} X^{l+1} & \sum_{k=0}^{l} X^{l-k} B Y^k \\ 0 & Y^{l+1} \end{pmatrix} .
\end{aligned}$$

Thus the relation is true for $l+1$. The principe of recurrence allows to conclude.□

Notation 1. *Let $m, n \in \mathbb{N}^*$. We denote:*

(i) $(M_B(X,Y))^m = \begin{pmatrix} X^m & M_m(X,Y) \\ 0 & Y^m \end{pmatrix}$ *where* $M_m(X,Y) = \sum_{k=0}^{m-1} X^{m-1-k} B Y^k$

(ii) $\begin{pmatrix} A & M_m(X,Y) \\ 0 & C \end{pmatrix}^n = \begin{pmatrix} A^n & M_{m,n} \\ 0 & C^n \end{pmatrix}$ *where A and C are two matrices of order equal to X and Y.*

(iii) $\begin{pmatrix} X & M_n(A,C) \\ 0 & Y \end{pmatrix}^m = \begin{pmatrix} X^m & M_{n,m} \\ 0 & Y^m \end{pmatrix}$

Theorem 2.2. *Let A, B, C, X, Y be a square matrices of same order. If $AX = XA$ and $CY = YC$, then $M_{m,n} = M_{n,m}$.*

Proof. we have :

$$\begin{aligned} M_{m,n} &= \sum_{l=0}^{n-1} A^{n-1-l} M_m(X,Y) C^l \\ &= \sum_{l=0}^{n-1} A^{n-1-l} (\sum_{k=0}^{m-1} X^{m-1-k} B Y^k) C^l \\ &= \sum_{l=0}^{n-1} \sum_{k=0}^{m-1} A^{n-1-l} X^{m-1-k} B Y^k C^l \end{aligned}$$

and

$$\begin{aligned} M_{n,m} &= \sum_{k=0}^{m-1} X^{m-1-k} M_n(A,C) Y^k \\ &= \sum_{k=0}^{m-1} X^{m-1-k} (\sum_{l=0}^{n-1} A^{n-1-l} B C^l) Y^k \\ &= \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} X^{m-1-k} A^{n-1-l} B C^l Y^k. \end{aligned}$$

If $AX = XA$ and $CY = YC$, then $M_{m,n} = M_{n,m}$.

3. Encryption Schemes using Matrices

We will be divide this section into five sub-sections; by constructing an encryption scheme using the matrix $M_B(X,Y)$. The first is devoted to the exchange of keys between the traditional entities Alice and Bob based on the constructed matrices, in the second we prove the security of this protocol, in the third and fourth sub-section we construct a cryptosystem based on matrices and which is homomorphic, we end with a numerical example whose calculations are done by the Maple software.

3.1. Key exchange protocol

Alice and Bob agree on public prime number p and B is a square matrix with coefficients in the finite field $\mathbb{F}_q$, were q is a power of p. Alice choose a private keys: $l \in \mathbb{N}^*$, the matrix $A \in \mathcal{M}(\mathbb{F}_q)$ and publish the set E_A determined by the matrices of same order than A which between them do all commute such that the zero-matrix and the unit matrix are not in E_A. In turn, Bob choose a private keys: $k \in \mathbb{N}^*$, the matrix $Y \in \mathcal{M}(\mathbb{F}_q)$ and publish the set E_Y determined by the matrices of same order than Y which between them do all commute such that the zero-matrix and the unit matrix are not in E_Y. Alice choose an other private key: $C \in E_Y$. She calculated a matrix $(M_B(A,C))^l$ and send $M_l(A,C)$ to Bob. Similarly, Bob

choose an other private key: $X \in E_A$. He calculated a matrix $(M_B(X,Y))^k$ and send $M_k(X,Y)$ to Alice. With their private keys l and k, Alice and Bob calculate separately the matrices: $M_{k,l}$, $M_{l,k}$.
According to the theorem 2.2, we have: $M_{k,l} = M_{l,k}$.

Corollary 3.1. *The secret key of Alice and Bob is the matrix* $K = M_{k,l}$.

3.2. Security of this protocol

The set E_A and the matrix B are public. If another person wants to compute the secret key K, it must solve the following equation: $\sum_{i=0}^{l-1} A^{l-1-i}BC^i = M_l(A,C)$ whose unknowns the matrices A, C and the natural number l.

Proposition 3.2. *If B be a matrix of order n, then the complexity to calculate the key K is $\mathcal{O}(n^{lk})$.*

Proof. The encryption scheme using a matrix B of order n, will use a key K of size $\mathcal{O}(n)$, as described previously in section 2. Since

$$K = M_{k,l} = \sum_{i=0}^{k-1}\sum_{j=0}^{l-1} A^{l-1-j}X^{k-1-i}BY^iC^j$$

, we have the complexity to calculate the key K is $\mathcal{O}(n^{lk})$. □

3.3. Encryption of message

Let K be a secret key exchanged by Alice and Bob. If K is not invertible or equal unit matrix, then we return to the key exchange protocol. Else let m is the message that Alice wants to send to Bob, m is the matrix of the same order as K. The encryption message

$$c = e_K(m) = K.m.K^{-1}.$$

Lemma 3.3. *Let m_1, m_2 be two messages and for all invertible key not equal to unit matrix; K, we have:*

$$e_K(m_1 + m_2) = e_K(m_1) + e_K(m_2)$$

$$e_K(m_1.m_2) = e_K(m_1).e_K(m_2)$$

Proof. We have:

$$\begin{aligned} e_K(m_1 + m_2) &= K.(m_1 + m_2).K^{-1} \\ &= (K.m_1 + K.m_2).K^{-1} \\ &= K.m_1.K^{-1} + K.m_2.K^{-1} \\ &= e_K(m_1) + e_K(m_2) \end{aligned}$$

and

$$\begin{aligned} e_K(m_1.m_2) &= K.(m_1.m_2).K^{-1} \\ &= K.m_1.K^{-1}.K.m_2.K^{-1} \\ &= e_K(m_1).e_K(m_2). \end{aligned}$$

□

Remark 3.1. This encryption message is Homomorphic encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.

3.4. Decryption of message

When Bob receives the encrypted message c sent by Alice, it uses a decryption function to decrypt it. This function noted d_K is defined as follows: $d_K(c) = K^{-1}.c.K$.

Lemma 3.4. *For all message m, we have $d_K \circ e_K(m) = m$.*

Proof. We have:

$$\begin{aligned} d_K \circ e_K(m) &= d_K(e_K(m)) \\ &= K^{-1}.e_K(m).K \\ &= K^{-1}.K.m.K^{-1}.K \\ &= m \end{aligned}$$

□

Remark 3.2. The security of this homomorphic Cryptosystem is based on the difficulty in computing the key K.

3.5. Numerical example

Alice and Bob agree on public prime number $p = q$, where

$$p = 5434555555676775533459754563897654328989765644311766534437628947 1$$

and the matrix

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix},$$

where

b_{11} =5434555555676775533459754563897654328989765644311766534437628937 8

b_{12} =5434555555676775533459754563897654328989765644311766534437628939 9

b_{21} =5434555555676775533459754563897654328989765644311766534437628939 5

b_{22} =5434555555676775533459754563897654328989765644311766534437628946 9.

Alice choose a private keys: $l = 320$, the matrix

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

where

a_{11} =735965962629

a_{12} =245321987543

a_{21} =490643975086

a_{22} =5434555555676775533459754563897654328989765644311766509905430192 8.

and publish the set E_A. In turn, Bob choose a private keys: $k = 132$, the matrix

$$Y = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix},$$

where

y_{11} =5434555555676775533459754563897654328989765644311275890462320238 5

y_{12} =7359659629630629

y_{21} =12266099382717715

y_{22} =5434555555676775533459754563897654328989765644311521212449974592 8.

and publish the set E_Y.
Alice choose an other private key:

$$C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix},$$

where

c_{11} =5434555555676775533459754563897654328989765644311766043793720291 9

c_{12} =7359658629828

c_{21} =12266097716380

c_{22} =5434555555676775533459754563897654328989765644311766289115674619 5.

She calculated a matrix $(M_B(A,C))^l$ and send
$M_l(A,C) = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$, where

m_{11} =384582294019404331304332992579354350810712842277847253165508794 20
m_{12} =560773724183462194849031956427899405609014531236815753298152931 7
m_{21} =320816448981862465814531150345203194107830160289994277192949699 63
m_{22} =447469081161249557069881144367517901491084144306951284390707598 4,

to Bob. Similarly, Bob choose an other private key:

$$X = \begin{pmatrix} 2832139913519 & 688898897883 \\ 1377797795766 & 76544321987 \end{pmatrix}.$$

He calculated a matrix $(M_B(X,Y))^k$ and send

$M_k(X,Y) \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix}$,
where

n_{11} =547230342080823208126525997739766645223374851008817329139124 7244
n_{12} =246218283200934644116300762667612649963596203807612259902002368 40
n_{21} =530861434806278907291029155201519027910733968501648874339600739 77
n_{22} =505044126674620676569794475940449933866418545819942535652700576 62,

to Alice.
With their private keys l and k, Alice and Bob calculate separately the matrices: $M_{k,l}$ and $M_{l,k}$. The secret key is:

$K = M_{k,l} = M_{l,k} \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$,
where

k_{11} =150772623514685406594795609565026466108862736704386447896633462 79
k_{12} =532667728119181783409932374392196100517522523015928724172785645 26
k_{21} =191969564499539838851543879304521349304358396699340202868041606 61
k_{22} =288255064120674727448055897601985690965914355725765755041382814 53.

References

1. A. Chillali, *Cryptography over elliptic curve of the ring $F_q[e]$, $e_4 = 0$*, World Acad. of Sci., Eng. & Technol., 78 (2011), 848-850.
2. A. Tadmori, A. Chillali & M. Ziane, *The binary operations calculus in $E_{a,b,c}$*, Int. J. of Math. Models & Methods in Appl. Sci., 9 (2015), 171-175.

3. A. Tadmori, A. Chillali & M. Ziane, *Elliptic Curve over Ring* $A_4 = F_{2^d}[\epsilon]$; $\epsilon^4 = 0$, Appl. Math. Sci., 35 (9) (2015), 1721-1733.

4. Lester S. Hill, *Cryptography in an Algebraic Alphabet*, Amer. Math. Mon., 36 (1929), 306-312.

5. Lester S. Hill, *Concerning Certain Linear Transformation Apparatus of Cryptography*, Amer. Math. Mon., 38 (1931), 135-154.

6. C. Koukouvinos & D. E. Simos, *Encryption Schemes based on Hadamard Matrices with Circulant Cores*, J. of Appl. Math. & Bioinform., 3 (1) (2013), 17-41.

7. T.H. Cormen, C.H. Leiserson, R.L. Rivest & C. Stei, *Introduction to Algorithms*; MIT Press, 2003.

8. C. Boyd & A. Mathuria, *Protocols for Authentication and Key Establishment, Information Security and Cryptography Series*; Springer-Verlag, Heidelberg, 2003.

M. Zeriouh,
CRMEF, Fez-Meknes, Morocco.
E-mail address: zeriouhmostafa@gmail.com

and

A. Chillali,
Department of Mathematics,
Physics and Computer Science,
LSI, Polydisciplinary Faculty,
Sidi Mohamed Ben Abdellah University
TAZA; Morocco.
E-mail address: abdelhakim.chillali@usmba.ac.ma

and

A. Boua,
Department of Mathematics,
Polydisciplinary Faculty, Abdelmalek Essaadi University
Larache; Morocco.
E-mail address: abdelkarimboua@yahoo.fr; karimoun2006@yahoo.fr