J. Nat. Scien. & Math. Res. Vol. 1 No.2 (2015) 51-54.51

JOURNAL OF NATURAL SCIENCES AND MATHEMATICS RESEARCH

Available online at http://journal.walisongo.ac.id/index.php/jnsmr

Construction of Key Echange Protocol over Max-Plus Algebra to Encrypt and Decrypt Arabic Documents

Any Muanalifah
Jurusan Matematika, FST UIN Walisongo, Semarang, Indonesia

Corresponding author :
any.math13@gmail.com
Telp. (+62-24-7601295)
received: 15 November 2015
revised : 30 November 2015
Accepted: 30 December 2015

Abstract

In this paper, we consider the operation of matrix in Max-plus Algebra to construct a key public to encrypt and decrypt arabic document. Matrix operation in max-plus algebra is slight different with matrix operation in classical. In this paper, we also use a modular 37 to translate it into arabic text (arabic letter with number and special character).

Keywords **:** Cryptography, max-plus algebra , key exchange , arabic text

1 INTRODUCTION

Cryptography is one of mathematics subject which provides some techniques to secure data in communication. Nowadays, the development of internet allow people to communicate more efficient. Unfortunately, this invention encourage people to steal data for their private needs. The encryption of data is important way to secure online transmission throughout the internet. Therefore, many researcher developed cryptography as a technique for secure information which has two systems to build key public are symmetric and asymmetric key.

During this time, cryptography is built on classical algebra and number theory. In 70s, a Brazil Mathematician, Imre Simon introduced Tropical Algebra. Tropical algebra known as max-plus algebra or min-plus algebra. In max-plus scheme, tropical algebra is defined by a semiring $\mathbb{T} = \mathbb{R}_{\max} \cup \{- \propto\}$ endowed with $\oplus$ (maximum) and $\otimes$ (addition), for min-plus algebra $\oplus$ is replaced by minimum.

In this paper, we will define Tropical algebra as max-plus algebra. There are many application of max-plus algebra such as job scheduling, transportation, communication and networking system. Max-plus algebra has some properties look like classical algebra but $\oplus$ is non invertible since there does not an element x in $\mathbb{R}$ such that $a \oplus x = x \oplus a = - \propto$. Therefore, tropical algebra has idempotency property, $a \oplus a = \max(a, a) = a$.[8]

A few research discuss appplication of cryptography to secure arabic documentation. The new modification of arabic text was introduced by adapting the classical cipher of modular 26 and change it with modular 37. [1]

In Order to encrypt and decrypt arabic documents, we will construct key public with matrices over max-plus algebra dan use classical modular 37.

Cryptography has two methods key exchange protocols that are called symmetric key and asymmetric key. In this research, we consider symmetric key as a method to encrypt and decrypt plain text. Symmet-

ric key applies the same key in the process to encrypt and decrypt plain text as the following table

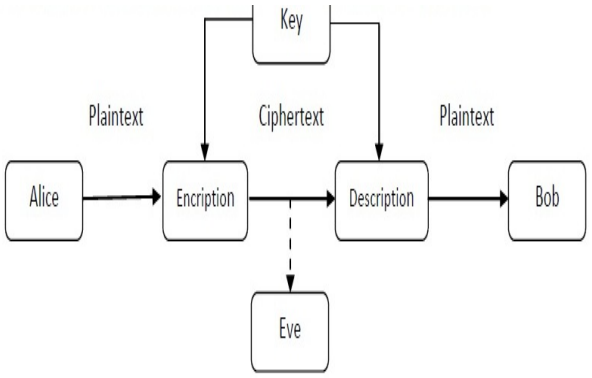

FIGURE 1: Symmetric Key

2 MAX-PLUS ALGEBRA

In this chapter, we introduce basic concepts of max-plus algebra.

DEFINISI 1 *Algebra max-plus is a semiring* $\mathbb{R}_{\max} = \mathbb{R} \cup \{- \propto\}$ *endowed with two biner operations* $\oplus$ *and* $\otimes$ *and define as follow*

$$a \oplus b = \max(a, b)$$

and

$$a \otimes b = a + b$$

Identity element of addition and multiplication are $- \propto$ and $0 \in \mathbb{R}$, respectively. The properties of max-plus algebra analogue with classical algebra as follow:

1. Associative
   For all a, b, c are elements in $\mathbb{R}_{\max}$ then
   $$a \oplus (b \oplus c) = (a \oplus b) \oplus c$$
   and
   $$a \otimes (b \otimes c) = (a \otimes b) \otimes c$$
2. commutative
   For all a, b are elements in $\mathbb{R}_{\max}$ then
   $$a \oplus b = b \oplus a, a \times b = b \otimes a$$
3. Distributive
   $$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c), \forall a, b, c \in \mathbb{R}_{\max}$$
4. Zero element (ε)
   $$a \oplus \varepsilon = \varepsilon \oplus a, \forall a \in \mathbb{R}_{\max}$$
5. Unit element (e)
   $$a \otimes \varepsilon = \varepsilon \otimes a, \forall a \in \mathbb{R}_{\max}$$
6. Idempotent
   $$a \oplus a = a, \forall a \in \mathbb{R}_{\max}$$

3 MATRICES OVER MAX-PLUS ALGEBRA

Let A, B are matrices over max-plus algebra then operation of addition and multiplication are defined as below:

$$[A \oplus B]_{i,j} = max(a_{i,j}, b_{i,j})$$

and

$$[A \otimes B]_{i,j} = \max_k \in p\{a_{i,k} + b_{k,j}\}$$

EXAMPLE 1 *Let* $A = \begin{pmatrix} -1 & 2 \\ - \propto & 1 \end{pmatrix}$ *and* $B = \begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix}$

$$A \oplus B = \begin{pmatrix} 0 & 2 \\ -2 & 1 \end{pmatrix}$$

4 STICKEL'S PROTOCOL OVER MAX-PLUS ALGEBRA

The implementation of matrix over min-plus algebra in Stickel's Protocol was introduced by Dima Grigerov and Vladimir Shpilran [3][7][6]. We will adopt the protocol into max-plus algebra. We define the protocol of Stickel in max-plus algebra as follows:

1. Alice and Bob pick at random two pairs of natural numbers m,n and r,s, respectively
2. Alice computes $u = A^n B^m$ and send it to Bob
3. Bob computes $v = A^r B^s$ and send it to Bob
4. Alice and Bob compute key public $K_1 = A^n v B^m$ and $K_2 = A^r u B^s$

Therefore, we can conclude that Alice and Bob shared the same secret key $K = K_1 = K_2$

5 APPLICATION OF KEY EXCHANGE PROTOCOL TO ENCRYPT AND DECRYPT ARABIC DOCUMENT

To encrypt Arabic documents, we implement block cipher modular 37[5] into a synthetics table as follow:

1	2	3	4	5	6	7	8	9	10	11	12	13
أ	ب	ت	ث	ج	ح	خ	د	ذ	ر	ز	س ص	ش
14	15	16	17	18	19	20	21	22	23	24	25	26
ط	ظ ض	ع	غ	ف	ق	ك	ل	م	ن	هـ	و	ي
27	28	29	30	31	32	33	34	35	36	37		
٠	١	٢	٣	٤	٥	٦	٧	٨	٩	blank		

FIGURE 2: synthetics table

We use stickel's protocol over matrices in max-plus algebra to compute the key public. Let Alice and Bob choose two matrices are

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

and

$$B = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

.

We process using stickel's algorithm as below:

1. Alice and Bob pick at random two pairs of natural numbers 2,1 and 1,1, respectively

2 Alice computes

$$u = A^2B^1 = \begin{matrix} 4 & 3 \\ 3 & 2 \end{matrix}$$

and send it to Bob

3 Bob computes

$$v = A^1B^1 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$$

and send it to Bob

4 Alice and Bob compute key public

$$K_1 = A^2vB^1 = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}$$

and

$$K_2 = A^1uB^1 = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}$$

Therefore, we get key public

$$K = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}$$

Encription Process
Alice want to send a message to Bob :

فِي السَّنَتِ ٢٠١٦

and the encryption process of this message is

1	2	3	4	5	6	7	8	9	10	11	12	13
أ	ب	ت	ث	ج	ح	خ	د	ذ	ر	ز	س ص	ش
14	15	16	17	18	19	20	21	22	23	24	25	26
ط	ظ ض	ع	غ	ف	ق	ك	ل	م	ن	هـ	و	ي
27	28	29	30	31	32	33	34	35	36	37		
٠	١	٢	٣	٤	٥	٦	٧	٨	٩	blank		

FIGURE 3: synthetics table

- Divide the message into 4 characters :
  فِي السَّنَتِ ٢٠-١٦٣٠
- convert the block cipher using this table
- Alice transform the message and convert into matrices

$$\begin{pmatrix} 19 & 2 \\ 1 & 4 \end{pmatrix}, \begin{pmatrix} 12 & 1 \\ 3 & 24 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 1 & 0 \end{pmatrix}$$

- We use the key public

$$K = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}$$

to get cipher text :

سيَنَفِي ال ٣٤١٠

after we get the cipher text, Bob will decrypt the message with the same key and obtain the original message from Alice

6 COCLUSION

In this paper, we applying the cryptography over max-plus algebra to secure arabic documents based on classical stickel's protocol to generate key public. for future, we could discuss the complexity of computation and other aspect such as the possibility of attacker to break this can. Finally, max-plus algebra could be implemented into cryptography

REFERENCES

[1] Alqahtani, Y., Kuppuswamy, P., and Shah, S., 2013, New Approach of Arabic Encryption/Decryption Technique Using Vigenere Chiper On Mod 39, *International Journal of Advanced Research in IT and Egineering.*, 12(2).

[2] Butkovic, P., 2010, *Max-linear systems: theory and algorithms*, Springer Science & Business Media.

[3] Grigoriev, D., and Shpilrain, V., 2014, Tropical Geometry,*Communication in Algebra* , 42(6), 2624-2632.

[4] Kotov, M., and Ushakov, A.,2015, Analysis of a key exchange protocol based on tropical matrix algebra. Downloaded at 13^th May 2016 https://eprint.iacr.org/2015/852.pdf.

[5] Kuppuswamy, P., Alqahtani, Y., 2014, New Innovation of Arabic Languange Encryption Techinique Using New Symmetric Key Algorithm, *International Journal of Advances in Enginering and Technology*, 7(1), pp. 30-37.

[6] Mustofa., and Lestari, D., 2013, The password Agreement Method Based on Matrix Operation Over Min-Plus Algebra for Secret Information Safety.

[7] Mustofa.,2014, An application of Max-Plus Algebra in Cryptography.

[8] Viro, O. Y.,2011,. On basic concepts of tropical geometry. *Proceedings of the Steklov Institute of Mathematics*, 273(1), 252-282.