IMM

Journal of New Frontiers in Mathematics and Statistics

ISSN 2719- 2415 (Online)

Volume 2 (1) 2021, 1 - 10

Home page: www.imathm.edu.lk/publications

Action of a Semiring to Encrypt Asymmetric Key – Elgamal

S. Nivetha[1*], M. Chandramouleeswaran[2]

Department of Mathematics, Sri Ramanas college of Arts and Science for Women, India [1,2]

nivethasoundar9127@gmail.com*

ABSTRACT

In 1934, H.S.Vandiver formally defined the notion of a semiring. Even though, the concept of a semiring was introduced in 1934, the study on semirings got more attraction only in early 1960's. Since then, many research works have been continued because of the applications of semirings in various fields of Mathematics such as optimization techniques, automata theory, networks, cryptography and so on. The applications of semiring in public key cryptography were initiated by Atani, Monico and so on. Cryptography is a method of protecting information and sharing it in more secured way, so that the information cannot be accessed by a third party. It has two types namely, symmetric key cryptosystem and asymmetric key cryptosystem. The symmetric key cryptosystem contains only one secret key common to both the parties, whereas, the asymmetric key cryptosystem contains two secret keys, namely, a private key and a public key. The public key exchange between two parties in a more secured way was initiated by Diffie and Hellman in the year 1976. The idea of using semigroup actions for the purpose of building one way trapdoor function has been used by several researchers. In 2017, Sundar, Victor and Chandramouleeswaran, discussed a generalization of Diffie Hellman key exchange protocol, in which they considered the action of multiplicative semigroup of a semiring on some finite semimodule over a semiring. The same procedure was applied to Elgamal encryption by Thiruveni in the year 2018. In our earlier papers, we extended these works on multiplicative subsemigroups and multiplicative left ideals of a semiring.

Keywords: Semiring, Exponential Semiring, Multiplicative left ideal, Public key, Encryption and decryption

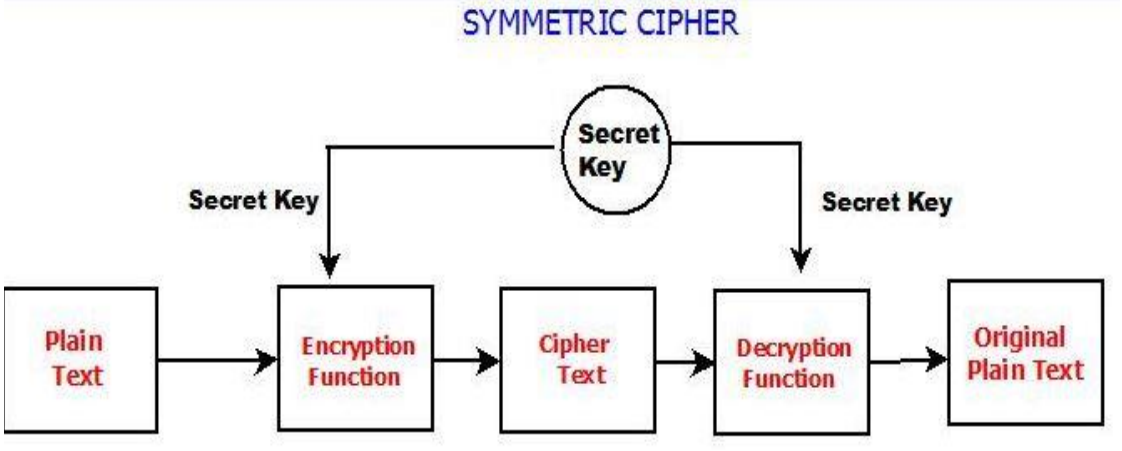
AMS Classification: 16Y60, 11T71, 14G50, 94A60

1. INTRODUCTION

The first step in a cryptosystem is to label all possible plaintext message units and all possible ciphertext message units by means of mathematical objects from which enciphering transformation and deciphering transformation can easily be constructed. There are several techniques available in the literature to construct these structural informations. In practice one can have an equipment for enciphering and deciphering which is constructed to implement only one type of cryptosystem. Over a period of time the information about the type of system they are using be leak out. To increase the security, they need to change frequently the choice of parameters used with the system. The parameter is called a key (secret key).

If in the system the two parties agree on a common key prior to transmitting the information such a scheme is called symmetric cipher system. In the symmetric key encryption the plain text is encrypted by using a key and the same key is used to decrypt the message. The system is depicted in the following diagram.

Figure 1

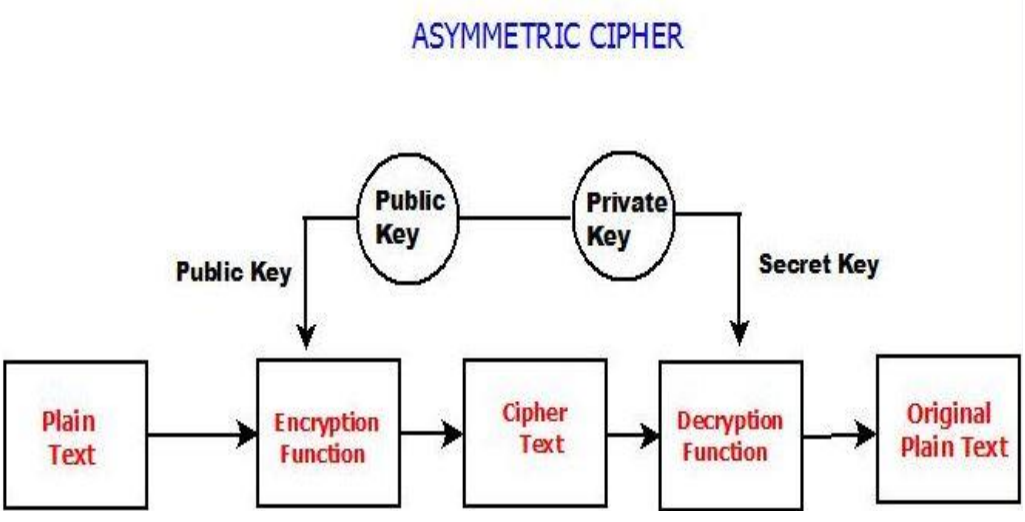


This technique is easier to use but less secured moreover a safe method of transferring the key from one party to another has to be identified. This system is more suitable for organizations such as Government, Military and big financial corporations. The spread of more unsecure computer networks in the recent era we need a more reliable method to use cryptography at larger scale. A brilliant and important cryptographic system is the RSA system introduced by Rivest-Shmir-Adleman which is an asymmetric cryptographic algorithm. Asymmetric means that there are two keys involved namely public key and private key. Each recipient could have both the keys. A recipient announces his public key to everyone but keeps the private key secret. Anyone can encode messages for a particular recipient using the public key however, one having the knowledge of private key can decode the messages. This system uses the notion of a trapdoor function - function whose output can be computed in a reasonable amount of time but whose inverses are inordinately difficult and time consuming to compute.

ISSN 2719-2415 (Online)

In the Asymmetric cipher system the plaintext will be encrypted by using two keys, namely public key and private key. This technique uses two different key to encrypt and decrypt the plaintext. This process of this scheme is slower but it provides confidentiality and authenticity. Examples of asymmetric key encryptions are Diffie-Hellman, Elgammal and RSA techniques. This scheme is described by the following diagram.

Figure 2.



Data that can be read and understood without any special measures is called a plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called an encryption. Encrypting a plaintext results in a cipher text

Diffie and Hellman (1976) gave a completely different and new direction to cryptography by introducing the concept of public key cryptography. Since then it became a noticeable area of research, and a lot of research have been carried. The concept of the Discrete Logarithmic Problem (DLP) in which one picks up two elements g,h from a group G (preferably a cyclic group) and a very large integer n such that $h=g^n$ and proposed a semigroup action problem (SAP) (Monico, 2002). He defined the Diffie–Hellman key exchange protocol and ElGamal cryptosystem (Elgamal, 1985) using this new computational problem SAP.

This problem of SAP was transferred to the action of a semiring (quotient semiring) over a semimodule in (Atani et.al, 2008). To improve the security, of the public key encryption, the authors generalized the semigroup action problem into a semiring action problem where they used the action of a semiring on a semi module over a given semiring (Sundar et.al.,2017). We have used the action of a semiring over a multiplicative sub semi group where the semiring under consideration is an exponential semiring (Nivetha et.al, 2019).

In this paper we extend the secret key sharing of Elgamal procedure by using the action of an exponential semiring over its multiplicative left ideal. This paper is divided into 5 sections. The next section recalls the basic definitions that are needed for our work.

ISSN 2719-2415 (Online)

In the section 'Algorithm' we propose a new technique of the action of a semiring over its multiplicative left ideals to share the public key.
The protocol is illustrated with an example and also the difficulty and advantage of the system is presented.

2. PRELIMINARIES

Encoding is a one to one function from an arbitrary set into a set of finite sequences over some alphabets. The inverse mapping of the encoding function is called a decoding function. Encryption is the process of encoding a message (plaintext) to a ciphertext with an encryption key that allows only the authorized entities can access the contents of the message. The reverse process of encryption converting a ciphertext to the original message using a secret key is called the decryption. Encoding is for maintaining data usability and can be reversed by employing the same algorithm that encoded the content without the use of a secret key. On the other hand encryption is for maintaining data confidentiality and requires the use of a secret key to return to the plaintext. Elgamal encryption is a public key cryptosystem that uses asymmetric key encryption for message communication. This system is based on the difficulty of finding discrete logarithm in a cyclic group. If the plaintext is small, that is, the plaintext contains a single block, we may use a single key to encrypt it. The process of obtaining the original plaintext from an encrypted cipher text is called a decryption. This uses, preferably the inverse of the secret key used to encrypt the plaintext.

Definition 2.1 (Jonathan Golan, 1999) A semiring is a nonempty set S on which operations of addition and multiplication have been defined such that the following conditions are satisfied:
(i) $(S,+)$ is a commutative monoid with identity element? 0.
(ii) $(S,\cdot)$ is a monoid with identity element? 1_S.
(iii) Multiplication distributes over addition from either side.
(iv) $0 \cdot r = 0 = r \cdot 0$ for all $r \in S$.
(v) $1_S \neq 0, 1_S \cdot s = s \cdot 1_S = s$ for all $s \in S$

Example 2.2 Let $n > 1$ be an integer and let $0 \leq i \leq n-1$. Set $B(n,i) = \{0,1,2,\cdots,n-1\}$. Define an operation $\oplus$ on $B(n,i)$ as, if $a,b \in B(n,i)$ then $a \oplus b = \begin{cases} a+b & \text{if } a+b \leq n-1 \\ c & \text{otherwise} \end{cases}$ where c is a unique element of $B(n,i)$ satisfying, $c \equiv a+b \bmod(n-i), i \leq c \leq n-1$. Define an operation $\otimes$ on $B(n,i)$ as, if $a,b \in B(n,i)$ then $a \otimes b = \begin{cases} ab & \text{if } ab \leq n-1 \\ c & \text{otherwise} \end{cases}$ where c is a unique element of $B(n,i)$ satisfying, $c \equiv ab \bmod(n-i), i \leq c \leq n-1$.

Definition 2.3 (Jonathan Golan, 1999) A semiring $(S,+,\cdot)$ is said to be additively commutative if $(S,+)$ is a commutative monoid. It is said to be multiplicatively

ISSN 2719-2415 (Online)

commutative if $(S,\cdot)$ is a commutative semigroup. A semiring $(S,+,\cdot)$ is said to be a commutative semiring if it is both additively and multiplicatively commutative.

Definition 2.4 (Jonathan Golan, 1999) Consider a semiring $(S,+,\cdot)$. A non-empty subset A of S is said to be a sub semiring if $(A,+,\cdot)$ is itself is a semiring under the induced operations. $\phi \neq A \subseteq S$ is called an ideal (two sided) if

1. $1 \notin A$
2. $x+a, a+x \in A$
3. $xa, ax \in A$

for all $x \in S$ and $a \in A$.

Definition 2.5 (Jonathan Golan, 1999) Consider a semiring $(S,+,\cdot)$. Let $a \in S$. The multiplicative order (additive order) of a is the least positive integer n such that $a^n = 1 (na = 0)$. It is denoted by $o(a) = n$.

Definition 2.6 (Jonathan Golan, 1999) Consider a semiring $(S,+,\cdot)$. Let $a \in S$. An element $0 \neq b \in S$ is said to be an additive inverse of a if $a+b = 0 = b+a$. $b \in S$ is said to be a multiplicative inverse of a if $ab = 1_S = ba$.

Definition 2.7 (Maze et.al., 2007) **(Semigroup Action Problem)** Given a semigroup G acting on a set S and elements $x \in S$ and $y \in Gx$, find $g \in G$ such that $gx = y$.

Definition 2.8. (Sundar et.al., 2017) **(Semiring Action Problem):** Given a semiring $A = S_1 \times S_2$ acting on a left semimodule $M = M_1 \times M_2$. Let $n = (n_1, n_2) \in M$ and $r = (r_1, r_2) \in \phi(A)$ where $\phi : A \to M$. The problem is to find $q = (q_1, q_2) \in A$ such that $\phi(q) = r$ that is, $\phi|_{S_1}(q_1) = r_1$, $\phi|_{S_2}(q_2) = r_2$.

3. ALGORITHM

In this section we describe the protocol for Elgamal procedure by using semiring action problem. Here we consider a semiring to be an exponential semiring and M to be a multiplicative left ideal of S. We start with the definition of exponential semiring.

Definition 3.1 Exponential Semiring Let $(S,+,\cdot)$ be a semiring. Let B be the multiplicative ideal of S. Define a binary operation $E : B \times S \to B$ by $E(b,s) = b^s$ for all $b \in B$ and $s \in S$ satisfying the following conditions:

(1) $b^{s_1} \cdot d^{s_1} = (bd)^{s_1}$
(2) $b^{s_1 \cdot s_2} = (b^{s_1})^{s_2}$
(3) $b^{s_1+s_2} = b^{s_1} . b^{s_1}$
(4) $b^1 = b$

Then (S, B) is called an exponential semiring.

ISSN 2719-2415 (Online)

Example 3.2.
Consider the semiring $S = B(27,3)$, it is easy to verify that it is an exponential semiring. On the other hand $B(27,5)$ is not an exponential semiring, for $[(3)^4]^7 \neq 3^{4\cdot 7}$ ($3^{4\cdot 7} = 3^6 = 3$ but $(3^4)^7 = 15^7 = 5$).

With this definition of exponential semiring S considering the action on a multiplicative left ideal we discuss the Elgamal protocol for sharing the secret message between two parties in a more secured way.

The ElGamal Algorithm provides an alternative to the RSA for public key encryption.

1. Security of the RSA depends on the (presumed) difficulty of factoring large integers.
2. Security of the ElGamal algorithm depends on the (presumed) difficulty of computing discrete logs in a large prime modulus.

ElGamal has the disadvantage that the ciphertext is twice as long as the plaintext. This problem is solved in our protocol given below. It has the advantage the same plaintext gives a different ciphertext (with near certainty) each time it is encrypted. We choose the language of communication as English. Hence the alphabet set A is

A =$\{ A, B, \cdots Z, \square\}$ where $\square$ represents the blank space. Let $S^*(A)$ denote the collection of all strings using alphabets from A. Thus it is an infinite set. Let $\tilde{S} = sub(S^*(A))$ where $sub(S^*(A))$ denote the collection of all subsets of $sub(S^*(A))$. In $\tilde{S}$ we define two operations $+$ and $\cdot$ as follows: For $L_1 + L_2 \in \tilde{S}$

(i) $L_1 + L_2 = L_1 \cup L_2$

(ii) $L_1 \cdot L_2 = \{w_1 w_2 / w_1 \in L_1 \text{ and } w_2 \in L_2\}$

Then $(\tilde{S}, +, \cdot)$ forms a semiring. If P is a given plaintext, let $A_P \subseteq A$ be the set of vowles included in the plaintext P.
We choose the semiring $S = \tilde{S}$ formed with the alphabets $A_P \subseteq A$.

The Protocol

- Let S be a semiring and B be a multiplicative left ideal of S.
- Define a mapping $\Phi : S \to B(n,i)$ where $0 \leq i \leq n-1, n = |A|, |A|$ is the set of alphabets in the language used for communication including blank space.
- Alice chooses $p \in B$ and $x \in S$ Then she finds $\Phi|_B(p)$ (first part of the public key) and $\Phi(x)$ (private key).
- Alice calculates second part of the public key as $(\Phi|_B(p))^{\Phi(x)}$.
- Alice announces $(\Phi|_B(p), (\Phi|_B(p))^{\Phi(x)})$ as her public key.
- Now Bob wants to send a message M containing r blocks $B_1, B_2, \cdots\cdots, B_r$ to Alice.

ISSN 2719-2415 (Online)

- Bob encodes the message M using the function $\chi : A_p \to B(n,i)$ where A_p is the set of alphabets in M. By this way he gets the encoded blocks $m_1, m_2, \cdots\cdots, m_r$.
- He splits $\Phi|_B(p)$ into r parts as $(\Phi|_B(p))^2, (\Phi|_B(p))^3, \cdots\cdots, (\Phi|_B(p))^{r+1}$.
- Now he chooses $y_1, y_2, \cdots\cdots, y_r \in S$ and finds $\Phi(y_1), \Phi(y_2), \cdots\cdots, .\Phi(y_r)$.
- Bob sends the cipher text to Alice as $c = (a_i, b_i)$, $1 \le i \le r$ where $a_i = (\Phi|_B(p))^{(i+1)\Phi(y_i)}$ and $b_i = m_i[(\Phi|_B(p))^{\Phi(x)}]^{(i+1)\Phi(y_i)}$.
- Alice decrypts the encoded message as, $m_i = b_i(a_i^{\Phi(x)})^{-1}$, $1 \le i \le r$.
- She decodes the original message by using the function $\chi^{-1} : R(\chi) \to A_p$.

4. ATTACK

In this section we are going to present how our key chosen can be more secured and it is impossible for any invader to decode the message sent. We choose our private key from the whole semiring and the public key from the a multiplicative ideal of the given semiring we are embedding the semiring chosen into the semiring $B(n,i)$, where n is equal to the number of alphabets of the language chosen for the communication including a blank space and $0 \le i \le n-1$. The above embedding can be represented by $\Phi : S \to B(n,i)$, $0 \le i \le n-1$ we make the following definition:

Definition 4.1 Consider the semiring $(S,+,\cdot)$ from which both the private and public keys are selected. Consider the semiring $B(n,i)$, $0 \le i \le n-1$. if k is any key then its orbit is defined as $orbit(k) = \{\Phi(i) / \Phi : S \to B(n,i)\}$.

To confirm the security of information and key shared we will be finding the orbit of the public key and private key in the semiring. When the size of the orbit of k in $B(n,i)$ is large enough it is very difficult for any invader to tap the key and decode the message to be transmitted since the number of embedding of S in $B(n,i)$ is equal to $|B(n,i)|^{|S|}$, any invader should identify the embedding first, then calculate the orbit of k, hence the size of the orbit is large enough it will be more difficult for the invader to identify the key to decode the message. So, we can confirm that the message transmission and the public key are more secured.

5. ILLUSTRATION

The above protocol can be illustrated by the following example. Let $(S,+,\cdot)$ be a semiring, $S = \{0,1,a,b,c,d,e,f,g,h,i,j\}$ where the addition and the multiplication operations are defined as follows:

ISSN 2719-2415 (Online)

Table: 1

$+$	0	1	a	b	c	d	e	f	g	h	i	j
0	0	1	a	b	c	d	e	f	g	h	i	j
1	1	f	1	d	f	g	i	i	j	i	i	j
a	a	1	a	b	1	d	f	f	g	i	i	j
b	b	d	b	b	d	d	g	g	g	j	j	j
c	c	f	1	d	e	g	h	i	j	h	i	j
d	d	g	d	d	g	g	j	j	j	j	j	j
e	e	i	f	g	h	j	h	i	j	h	i	j
f	f	i	f	g	i	j	i	i	j	i	i	j
g	g	j	g	g	j	j	j	j	j	j	j	j
h	h	i	i	j	h	j	h	i	j	h	i	j
i	i	i	i	j	i	j	i	i	j	i	i	j
j	j	j	j	j	j	j	j	j	j	j	j	j

$\cdot$	0	1	a	b	c	d	e	f	g	h	i	j
0	0	0	0	b	0	b	0	0	b	0	0	b
1	0	1	a	b	c	d	e	f	g	h	i	j
a	0	a	a	b	0	b	0	a	b	0	a	b
b	0	b	b	b	0	b	0	b	b	0	b	b
c	0	c	0	b	c	d	e	c	g	h	i	j
d	0	d	b	b	c	d	e	g	g	h	j	j
e	0	e	0	b	e	g	h	h	j	h	h	j
f	0	f	a	b	e	g	h	i	j	h	i	j
g	0	g	b	b	e	g	h	j	j	h	j	j
h	0	h	0	b	h	j	h	h	j	h	h	j
i	0	i	a	b	h	j	h	i	j	h	i	j
j	0	j	b	b	h	j	h	j	j	h	j	j

Let $B=\{0,a,b,c,d,e,g,h,i,j\}$ be a multiplicative left ideal of S. Define $\Phi: S \to B(27,5)$ by,

$\Phi(0)=00$, $\Phi(1)=01$, $\Phi(a)=03$, $\Phi(b)=11$, $\Phi(c)=09$, $\Phi(d)=07$, $\Phi(e)=04$, $\Phi(f)=05$, $\Phi(g)=13$, $\Phi(h)=17$, $\Phi(i)=21$, $\Phi(j)=23$.

Alice chooses $d \in B$ and $f \in S$, then she finds $\Phi|_B(d)=07$ and $\Phi(f)=05$.

She calculates $(\Phi|_B(d))^{\Phi(f)}=(07)^{05}=21$.

Alice announces $(07,21)$ as her public key.

Now Bob wants to send a message $STAY\_HOME\_STAY\_SAFE$ containing 4 blocks B_1, B_2, B_3, B_4 to Alice.

He encodes these blocks using the function $\chi: A_p \to B(27,5)$, $A_p=\{A,E,F,H,M,O,S,T,Y,\_\}$ and χ maps elements of A_p to the elements of $B(27,5)$ in their sequential order.

m_1 :1920012500; m_2 :0815130500; m_3 :1920012500; m_4 :1901060500.

Bob splits 07 into 4 parts by, $(07)^2,(07)^3,(07)^4,(07)^5=$ 05,13,03,21.

Now Bob chooses $y_1=1$, $y_2=b$, $y_3=d$, $y_4=f$ in S and finds $\Phi(1)=01$, $\Phi(b)=11$, $\Phi(d)=07$, $\Phi(f)=05$.

$a_1=(05)^{01}=05$, $a_2=(13)^{11}=13$, $a_3=(03)^{07}=09$, $a_4=(21)^{05}=21$.

$b_1=(1920012500)(21)^{2(01)}=(1920012500)(01)=1920012500$

$b_2=(0815130500)(21)^{3(11)}=(0815130500)(21)=1407091700$

$b_3=(1920012500)(21)^{4(07)}=(1920012500)(01)=1920012500$

$b_4=(1901060500)(21)^{5(05)}=(1901060500)(21)=0321161700$

ISSN 2719-2415 (Online)

Bob sends $c = \begin{bmatrix} 05\ 19\ 20\ 01\ 25\ 00 \\ 13\ 14\ 07\ 09\ 17\ 00 \\ 09\ 19\ 20\ 01\ 25\ 00 \\ 21\ 03\ 21\ 16\ 17\ 00 \end{bmatrix}$ to Alice.

Alice decrypts the encoded text by using $b_i(a_i{}^{\Phi(x)})^{-1}$.

$m_1 = (1920012500)(05^{05})^{-1} = (1920012500)(01) = 1920012500$

$m_2 = (1407091700)(13^{05})^{-1} = (1407091700)(21) = 0815130500$

$m_3 = (1920012500)(09^{05})^{-1} = (1920012500)(01) = 1920012500$

$m_4 = (0321161700)(21^{05})^{-1} = (0321161700)(21) = 1901060500$

Alice decodes m_1, m_2, m_3, m_4 using the function, $\chi^{-1} : R(\chi) \to A_p$ and she gets the plaintext as,

STAY _ HOME _ STAY _ SAFE

6. CONCLUSION

In our future work we are going to study the action of a semiring over its multiplicative ideal as well as over a semimodule for other types of protocols such as Pholligrio, Phollig Hellman, etc., We have also proposed to compare different protocols in asymmetric key cryptography with the help of action of a semiring.

REFERENCES

Atani. R.E., Atani. S.E. & Mirzakuchaki.S, (2008). Public key Cryptography using semigroup actions and semirings. *J. Discrete Math. Sci. Cryptography,* Vol. 11, No. 4, 437-445.

Diffie. W & Hellman. M (1976). New directions in Cryptography. *IEEE transactions. Inform. Theory* Vol.22 472-492.

ElGamal. T, (1985). A Public key Cryptosystem and Signature Scheme based on discrete logarithms. *IEEE Transactions. Inform. Theory* Vol.31, No. 4, 469-472.

Jonathan Golan. S, (1999). *The semirings and their Applications*. Kluwer Academic Publishers, London.

ISSN 2719-2415 (Online)

Maze.G, Monico. C & Rosenthal. J, (2007). Public Key Cryptography based on semigroup Actions. *Advances in Mathematics of Communications,* Vol.1, No. 4, 489-507.

Monico. C.J,(2002). Semirings and semigroup actions in Public key Cryptography. *ProQuest LLC, Ann Arbor, Thesis (Ph.D.,) University of Notre Dame.*

Nivetha. S., Thiruveni. V & Chandramouleeswaran. M, (2019). Semiring Actions for Public key Cryptography, *Journal of Computer and Mathematical Sciences,* Vol. 10, No. 1, 238-244.

Sundar. M, Victor. P & Chandramouleeswaran. M, (2017). Public Key Cryptography Key Sharing with Semiring Action. *IJMSEA,* Vol. 11, No. 1, 195-204.

ISSN 2719-2415 (Online)