ENCIPHERING SEMI GROUPS USING CYCLIC GROUP (G, +)

B. L. Raina*

Goutam Datta*

Tapas Kumar*

Manoj Kumar jain*

Abstract: *Cryptosystem is a setup such that a function f converts any plain text (P) message into cipher text © message by using enciphering transformation. We then use f^{1} deciphering transformation which reverses the above process. In this paper we extend the generalization of standard Diffie- Hellman key exchange and ElGamal cryptosystem in (Z/pZ)* by converting a semi-group under the binary operation of '+'(more simply from G(V, E) i.e. graph G) action on to a finite dimensional vector space T over F_2.*

Keywords: *Cryptosystem, cipher -text, Semi-group action, enciphering.*

---

*School of computer science and engg.,Lingayas University,Haryana,India.

1. INTRODUCTION

The generalized discrete problem (GDP) is the basic problem for many cryptosystem. Discrete logarithm problem (**DLP**) (see e.g.[1,2,3,8,9]) is the fundamental problem that is discussed in cryptosystem. Let G be a finite group where a, b Є G be the arbitrary elements. We find an integer n Є N such that a*n = b, * operation being the multiplication, that is (a*a*a…..*a=b).In the present paper , we replace this operation by addition and discrete logarithmic algorithm over a group can be seen more simply as a special instance of an action by a semi -group over (G,+).Here we find an integer n Є N such that n*a = b.that is (a+a+a……+a=b).This problem has time complexity of order n .It has been shown ,if for b belonging to < a>, the cyclic group generated by a then b Є <a> under the operation of '+' mod (m) so that there is a unique integer n satisfying 1 ≤ n ≤ ord(a) such that n *a=b. This integer is discrete in relation of b w.r.t. a Є R

DLP plays an important role in Diffe-Hellman key agreement and the Elgamal public key cryptosystem [1-3,8,9] .The Diffe – Hellman key agreement allows two persons say, Alice & Bob to exchange a secret key k. For Alice and Bob to agree in a graph (G,+) and a common base g ЄG, Alice chooses a random integer a Є N and Bob chooses a random integer b Є N , Alice transmits to Bob g^a and Bob transmits to Alice g^b. Then common secret key is g^{ab}.

2. THE ELAGAMAL PUBLIC KEY CRYPTOSYSTEM WORKS AS FOLLOWS:

Alice choose n ЄN and a, b Є G when b=n*a, the private key of Alice is (a, b, n) & the public key is (a,b). Bob chooses random integer r ЄN and applies cryptal function:

E : G→ GXG

m: (C1, C2)= (r*a, m+r*b)

={(a+a+a+……. r times),m+(b+b+b+ …r times)}

Alice computes message "m" from the cipher text (c1, c2) by

$m = c_2 + (-n*c_1)$

In this paper, we discuss these problems by converting a semi-group G and determine a semi-group action on a finite vector space of dimension q over the field F_2. Our paper is in the same vein as of G. Maze et al [7].

 ISSN: 2278-6244

3. DERIVATION OF A SEMI-GROUP FROM A GRAPH

Let G be a finite (v_i, e_i) graph and H be the sub-group of G. Let x_H denote a vector corresponding to H such that

$x_H = \{ x_1, x_2, x_3 \ldots\ldots x_q \}$, when

$x_i = \{ 1$, if $e_i \in H$

$\{0$, otherwise

Let U be the set of such vectors. Let '+' define the binary operation on U. if '+' is associated to U, then (U,+) is called semi-group and simply denoted by U

If we consider the binary operation as '+' (addition modulo 2), then we have

$x_h + y_k = (x_1, x_2, x_3 \ldots\ldots x_q),(y_1, y_2, y_3 \ldots\ldots y_q)$

$= (x_1+y_1, x_2+y_2, \ldots\ldots x_q+y_q)$

where $x_h, y_k \in U$

Illustration: - Consider the graph G in fig.1 given by:

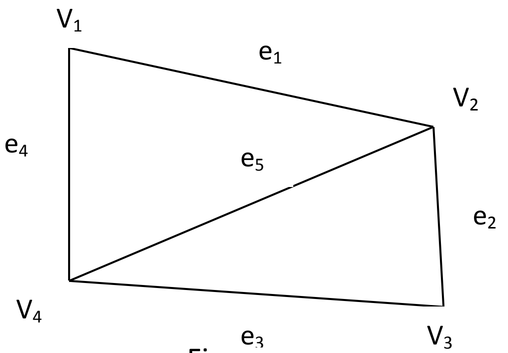


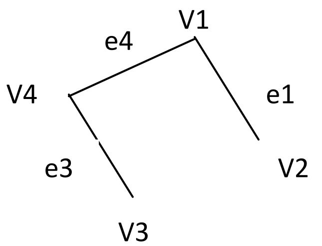
Fig 1

Here V = {V_1, V_2, V_3, V_4} i.e. v = n(V) = 4

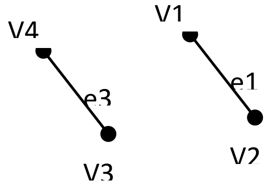
E = { e_1, e_2, e_3, e_4, e_5) i.e. e = n(E) =5 = q

We shall now consider the following 7 subgroups of G shown in fig 2 and show that (U, +) is semi –group.

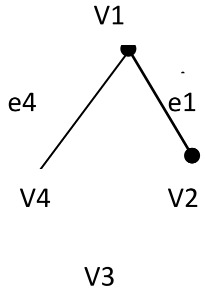
(i) H1:



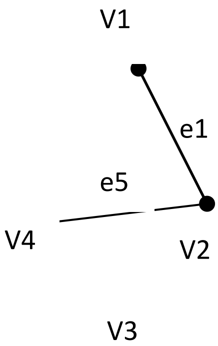
(ii) H2:



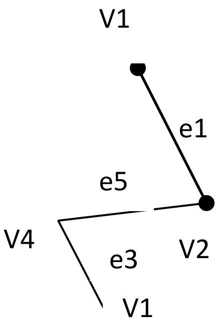
(iii) H3:



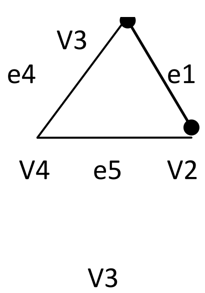
(iv) H4:



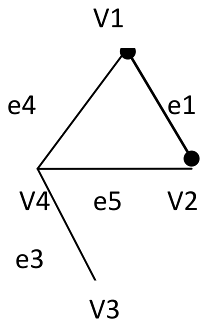
(v) H5:



(vi) H6:



(vii) H7:



Let $x_{Hi,}$ i = 1…….7 be the vector corresponding to $H_{i,}$ respectively given by U = { x_{Hi} }, i = 1,..,7

Now let

x_{H1} = {1, 0, 1, 1, 0}, $x_{H2\,j}$= {1,0,1,0,0}, x_{H3} = {1,0,0,1,0}, x_{H4} = {1,0,0,0,1}, x_{H5} = {1,0,10,1}, x_{H6} = {1, 0, 0, 1, 1}, x_{H7} = {1, 0, 1,1,1},

It is now easy to see that:

$x_{H1} + x_{H2} = x_{H1}$, $x_{H1} + x_{H3} = x_{H1}$, $x_{H1} + x_{H4} = x_{H6}$, $x_{H1} + x_{H5} = x_{H6}$, $x_{H1} + x_{H6} = x_{H6}$, $x_{H1} + x_{H7} = x_{H7}$, $x_{H2} + x_{H3} = x_{H1}$, $x_{H2} + x_{H4} = x_{H7}$, $x_{H2} + x_{H5} = x_{H5}$, $x_{H2} + x_{H6} = x_{H7}$, $x_{H2} + x_{H7} = x_{H7}$, $x_{H3} + x_{H4} = x_{H6}$, $x_{H3} + x_{H5} = x_{H6}$, $x_{H3} + x_{H6} = x_{H6}$, $x_{H3} + x_{H7} = x_{H7}$, $x_{H4} + x_{H5} = x_{H5}$, $x_{H4} + x_{H6} = x_{H6}$, $x_{H4} + x_{H7} = x_{H7}$, $x_{H5} + x_{H6} = x_{H7}$, $x_{H5} + x_{H7} = x_{H7}$, $x_{H6} + x_{H7} = x_{H7.}$It is easy to verify that (U,+) is a semi-group.

4. USAGE OF U ACTION TO DERIVE COMMON KEY

Let T be a q dimensional vector space over F_2 . Define the left action of U on T , ψ : U X T -→ T such that ψ (x, t) = x + t, we call this action as U action on the vector space T. Let G be (v_i, e_i) be the graph such that (U, +) is an abelian semi –group associated to graph G, T be a q dimensional vector space over F2 and plus sign be U action on T as defined above. We define Diffie-Hellman key exchange using U-action as follows:

1. Alice and Bob agrees on an element t Є T.
2. Alice chooses x Є U and computes x + t. Alice's private key is x , her public is x + t
3. Bob choose y Є U and computes y + t
4. Their common secret key is then

   x +(y + t) = (x + y) + t = (y + x) + t = y + (x + t)

Example:

Consider the graph G given in fig 1 and H_i, i = 1,2,3,…..7 be the seven graph of G as in fig 2. Then (U, +) is a semi – group.

Let T be the 5- dimensional vector space over F_2 . suppose Alice & Bob want to agree on a key. For they choose t Є T as t = (1, 0,0,0,0) then Alice choose X_{H1} =(1,0,1,1,0) Є U and computes x_{H1} + t = (1,0,1,1,0) . then sends it to Bob.

Similarly Bob choose $\mathbf{x_{H4}}$ = {1,0,0,0,1} and computes x_{H4} + t = {1,0,0,0,1} Є U. Then sends it to Alice so that their common key is

$x_{H1} + (x_{H4} + t) = x_{H4} + (x_{H1} + t) = \{1,0,1,1,1\}$.

5. USAGE OF U-ACTION OF DI FFE – HELLMAN PROBLEM TO DERIVE MESSAGE

Let G = (v_i, e_i) be the graph and (U, +) be a semi group associated to graph G. Let T be a q-dimensional vector space over F_2 and '+' be U action on t defined by :

Given r,s,t Є T with s= x+ r and t= y + r for some x, y Є U to find (x + y) + r Є T. We now use cryptosystem, using U- action on T.

Let G, (U, +), T be as defined above such that U-action on T be also defined as above . Then we define :

ElGamal Crytosystem using U-action as follows :

1. Alice chooses element t ЄT and x Є U. Alice's public key is (t, x+t).
2. Bob chooses random element y Є U and encrypt a message'm' using encryptive function
3. f (m,y) = ((y+t, y + (x + t)) +m) = (c_1,c_2)
4. Alice can decrypt the message using :

   m = - (y + (x + t)) + (y + (x + t)) + m = - (x + c_1) +c_2.

Remark : Here message 'm' is expressed in terms of vector where each letter in the message represents a vector (x_1, x_2, x_3, …….x_q), q >= 26 such that

x_i = { 1 if corresponding letter is in the ith position of alphabet

0. Otherwise.

For example if q = 26 then each letter is English alphabet represents as follow:

A = {1, 0, 0, 0, …………0}

B= {0,1,0,0,0…………..0}

C = {0,0,1,0,…………….0}

…………………………..

……………………………

……………………………

Z = {0,0,0,……………0,1}

Illustration

Let G = (v_i,e_i) = (v_i, q) with q=26 ie T be a 26 dimensional vector space over F2, (T, +) is an additive abelian group and (U,+) be the semi group associated with the group G. The action of U on T is as defined above.

1.Suppose Alice chooses t = {0,1,1,0,1,0,0,1,0,0,….,0} Є T then choose x = {1,0,1,0,0,1,0,0,0,…….,0,0} ЄU corresponding to one sub graph H1 of G and compute

x + t ={1,1,1,0,1,0,0,1,0, ……., 0,0,0,0}. Her public key is (t, x+t)

2. Bob wishes and sends a message m “SEE ME TODAY” to Alice. He sends it letter by letter. So, first he wants to send the letter

S = m’(m) = (0,0,0,………,0, 1,0……..0)

For he chooses y = {0,0,1,0,1,0,0,0,0,0,…………0} ЄU that is a vector corresponding to one sub graph H2 of G and compute

y+t = {0,1,1,0,1,0,0,1,0……0,0,0,0} = c1

also compute y + (x+t) ={1,1,1,0,1,0,0,1,0,0,0,0,…..,,0,0}

and y + (x+t) + m’ = {1,1,1,0,1,0,0,1,0….0,0,0,0,0,0,0…0) + {0,0,0,0,0……1,0,0,0,0,…..0,0,0} ={1,1,1,0,1,0,0,1,0,…0,1,…0,0,0,0}=c_2

Then he sends (c_1, c_2) to Alice

3. After receiving this Alice decrypts the message by computing

$c_2 – (x + c_1)$

Here $x + c_1$ = {1,1,1,0,1,0,0,1,0,0,0,0,…0,0,0,0,0,0}

Now $c_2 – (x + c_1)$ = {0,0,0,0,0,0,0……0,1,0, …..,0} = m’m = S

Similarly he transfers each letter of message m.

REFERENCES:

1. H. Cohen, A course in Computational Algebraic Number Theory,Gaduate Text in Mathematics ,138,Springer Verlag,Berlin,1993.
2. W.Diffie and M.E.Hellman, New Directions in cryptography, IEEE Trans. Inform. Theory,22(1976,644-654)
3. J.B.Fraleigh,”A first course of Abstract Algebra’c,7th Edition,Pearson Inc,Singapore 2003.

4. M.Gavalec,Computing matrix period in max- min algebra, Discrete applied math,75(1997),63-70.
5. C.Monico, On finite congruence-simple semirings,J.Algebra271(2004,846-854).
6. G .Maze, C.Monico and J.Rosenthal, Public key cryptography based on semigroup actions,Advances in mathematics and communication,vol.1,No.4 2007,489-507
7. G. Maze,Chris Monic & Joachem Rosenthal," Public Key Cryptography Basis on Semi-group action"Advances in Mathematics of Communication,v1,N0.4,2007,489-507.
8. F.Harry. "Graph Theory"Addison-Wesley Publishing Company Inc,1969.
9. I.N.Herstein,"Topics in Algebra"Wiley Eastern Ltd ,New Delhi,1975.
10. N.Koblitz A Course in Number Theory & Cryptography "2nd edition Springer Verlag 1994.