ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

An ElGamal Encryption Scheme of Adjacency Matrix and Finite Machines

B.Ravi Kumar[1], A.Chandra Sekhar[2], G.Appala Naidu[3]

[1,2]Department of Mathematics,GIT,Gitam University,Visakhapatnam,INDIA.
[3]Department of Mathematics,Andhra University,Visakhapatnam,INDIA.

Abstract: Cryptography is the combination of Mathematics and Computer science. Cryptography is used for encryption and decryption of data using mathematics. Cryptography transit the information in an illegible manner such that only intended recipient will be able to decrypt the information. In the recent years, researchers developed several new encryption methods. Among such ElGamal encryption is the one laid a concede platform for the researchers in Cryptography. Ever science several mathematical models were applied for encryption/decryption. In this paper, we introduced an ElGamal encryption, which uses points on the elliptic curve, and finite state machines and adjacency matrix.

Keywords: ElGamal, adjacency matrix, Finite state machine, encryption, decryption.

I. Introduction:

In the year, 1985 Victor Miller and Neal Koblitz first introduced the Elliptic curve cryptography. Elliptic curve cryptography has proven its security by with standing to a generation of attacks. In the recent years, as the wireless communication has grown rapidly, the numerous companies have adopted Elliptic curve cryptography as an innovative security technology. Elliptic curve employs a relatively short encryption key and the shorter key size is faster and requires less compelling power than the other. Elliptic curve cryptography encryption key provides the same security as '1024'-bit RSA encryption key [1][2][3][4][8].

In general, cubic equations for elliptic curves take the following form, known as Weierstrass equation[5]:

$$y^2 + gxy + hy = x^3 + ix^2 + jx + k$$

Where g,h,i,j,k are real numbers and x,y take on values in the real numbers. For our purpose, it is sufficient to limit ourselves to equations of the form $y^2 = x^3 + gx + h$ where x,y,g,h belong to R, Q, C or Fp. Also include in the definition of an elliptic curve is a single element denoted by O and called the point at infinity or the zero point. There is also a requirement that the discriminant $\Delta = 4g^3 + 27h^2 \neq 0$[4][5].

II. The ElGamal Cryptosystem:

Two communicating parties 'A' and 'B' initially agree upon the Elliptic curve $E_p(x,y)$ and p is sufficiently large prime number and (x,y) is the point on the Elliptic curve. For secure communication over insecure channels both A and B fix a point $C(x_1,y_1)$. A initially selects a private key 'K_A' and generates the public key $P_A = K_A \times C$. Next 'B' selects a private key K_B and generates the public key $P_B = K_B \times C$. Now A wants send a message M to B for this purpose A choose a random integer 'n' now A encrypts M as $CT_m = \{nC, M + nP_B\}$ and sends to B.

Then 'B' decrypts the CT_m as

$$M + nP_B - K_B(nC) = M + n(K_BC) - K_B(Cn) = M[12].$$

III. Finite state Machine:

Automata theory is a key to software for verifying systems of all types that have a finite number of distinct states, such as communication protocols or protocol for secure exchange of information. Finite state machines (FSM), also known as finite state automation (FSA), at their simplest, are models of the behaviours of a system or a complex object, with a limited number of defined conditions or modes, where mode transitions change with circumstance[6][7].

A deterministic finite automation (DFA) is a quintuple $M = (Q, \Sigma, q_0, \delta, F)$, where

- Q is a finite set of states.
- Σ is a finite set of input symbols.
- q_0 is the start state indicated by an arrow $\rightarrow$.
- δ is a transition function $\delta : Q \times \Sigma \rightarrow Q$ i.e., $\delta(q_0, a) = q_i \in Q$.
- $F \subset Q$ is a finite set of final states.

Generally the input symbols of Σ are either letters or digits. i.e., $\Sigma = \{a, b\}$ *or* $\{0,1\}$ and Σ^* is the set of strings formed out of Σ. Sometimes we refer strings as languages also. We say that a string x is accepted by a DFA if $\delta(q_0, x) \in F$. The set of languages accepted by a DFA 'M' is denoted by L(M). In a DFA there will be only one transition out of each state on the same input symbol. The nondeterministic finite automation (NDFA) is also a mathematical model $M = (Q, \Sigma, \delta, q_0, F)$ where Q, Σ, q_0, F are as in DFA except δ, is a transition function from $Q \times \Sigma^* \rightarrow Q$. In NDFA there may be Moore machine is a sixtuple $M = (Q, \Sigma, \delta, \Delta, \lambda, q_0)$ Where Q, Σ, δ, q_0 are as before and λ is a output function and Δ is the set of output symbols. In a More machine the output depend on the transition.

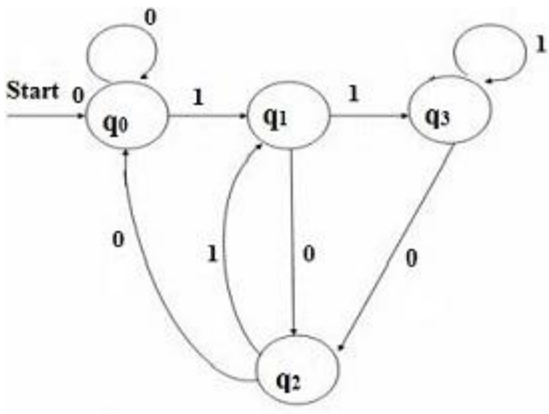

Fig1.1 - Moore machine with residue mod4

Transition table, as well as transition diagram can also represent Moore machine.

In this paper, consider Moore machine, which calculates residue mod4.

IV. Adjacency matrix:

Let $G = (V, E)$ be a simple directed graph where $V = \{v_1, v_2, v_3, ...v_n\}$ be the set of nodes and E is the set of edges. Then

$$A = [a_{ij}]_{n \times n} = \begin{cases} 1 & if \ (v_i, v_j) \in E \\ 0 & otherwise \end{cases}$$

The adjacency matrix is a Boolean matrix as the entries are 0's or 1's.

The number elements in the ith row whose value is 1 in a column, say the jth column, is equal to the indegree of the node v_j. an adjacency matrix completely defines a simple digraph.

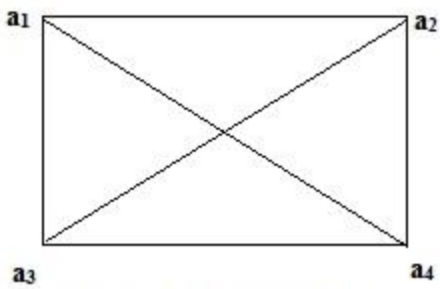

Figure 1.2 Simple graph

$$B = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

- The entries along the principal diagonal of B are all 0's if and only if the graph as no self loops. A self-loop at the ith vertex corresponds to x_{ij}=1.
- The definition of adjacency matrix makes no provision for parallel edges. This is why the adjacency matrix B was defined for graphs without parallel edges.
- If the graph has no self-loops the degree of a vertex equals the number of 1's in the corresponding row or column of B.

V. PROPOSED ALGORITHM:

Alice wants to send the message to Bob using elliptic curve ElGamal encryption by using adjacent matrix. Alice chooses the elliptic curve $y^2 = x^3 + gx + h$ over the field z_p.

Choose the point G on the elliptic curve. Alice selects a private key 'a' and generates the public key A='aG' and Bob selects a private key 'b' and generates the public key B= 'bG'.

Encryption:

Step 1: Alice chooses a random integer k, and keeps it secret.

Step 2: Compute kG.

Step 3: Alice selects the Bob's public key $B = bG.$

Step 4: Compute $kB = k(bG) = l.$

Step 5: Compute $aB = a(bG) = m.$

Step 6: Alice wants to send the message q_i to Bob.

Step 7: Alice wants to convert the message into the points on the elliptic curve. She chooses a point Q, which is the generator of the elliptic curve. By using ASCII characters of upper case letter into the points on the elliptic curve.

Let $A = \{1P, 2P, 3P................255P\}$
$B = \{set\ of\ all\ ASCII\ characters\}$

Alice defines one to one correspondence $f : A \to B$ by $f(nP) = x_n$

Where n=1,2………255 and $\{x_1, x_2, x_3, ...x_{255}\}$ *are the ASCII characters.*

Step 8: To create 4×4 matrix with entries are the points on the elliptic curve.

$$m_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \\ a_9 & a_{10} & a_{11} & a_{12} \\ a_{13} & a_{14} & a_{15} & a_{16} \end{pmatrix} \text{ and so on}$$

additional which is obtained depending upon the length of the message.

Step 9: Alice selects m, where's' is the x-coordinate of m and the binary value's' is secret key.

Step 10: Alice define Moore machine with input is secret key.

Compute

$$q_{k+1} = q_k \times [adjency\ \ matrix]^{output at\ q_{k+1}\ state.}$$

The resultant sets of points are

$R = \{q_1(x_1, y_1), q_2(x_2, y_2), q_3(x_3, y_3)...........q_i(x_i, y_i)$

where i=1,2,3……

Step 11: Compute $C_i = q_i + l + m..$

Step 12: Now Alice sends the encrypted message (kG, C_i) to Bob.

Decryption:

To recover the plain text q_i from C_i, Bob should do following:

Step 1: First Bob selects the Alice public key A=aG.

Step 2: Compute bA=b(aG)=m.

Step 3: Now Bob computes the inverse element of b(aG) is - b(aG).

Step 4: Add - b(aG)to the second part of the message: $q_i + kbG + abG - abG = q_i + kbG$

Step 5: Multiply the Bob's own private key 'b' with the first part of the message kG, we get: kbG.

Step 6: Now Bob computes the inverse element of kbG, which is –kbG.

Step 7: Bob adds -kbG to the second part of the message: $q_i + kbG - kbG = q_i$.

Step 8: after decryption, the obtained points are stored in 4×4 matrix.

$$S_1 = \begin{pmatrix} q_1 & q_2 & q_3 & q_4 \\ q_5 & q_6 & q_7 & q_8 \\ q_9 & q_{10} & q_{11} & q_{12} \\ q_{13} & q_{14} & q_{15} & q_{16} \end{pmatrix}, \ldots.$$

Step 9: Bob selects m, where's' is the x-coordinate of m which is the secret key and the binary value's' is input key.

Step 10: Now Bob multiplies q_i with inverse of key matrices 'R' and Bob applies the reverse process and by using ASCII characters of upper case letters, he can recover the message.

EXAMPLE:

Alice wants to send the message to Bob using elliptic curve ElGamal encryption by using adjacency matrix. Alice chooses the elliptic curve $y^2 = x^3 - 4$ over the field z_{271}. Then the points on the elliptic curve are E={0,(1,57),(1,214),(2,2),(2,269),(5,11),(5,260),(6,36),(6,235),(7,135),(7,136),…..

………………………………………………

………...…………………

…………..(264, 174), (269,114), (269,157)}.

The number of points on the elliptic curve is 271 and the prime number is 271. Therefore each point is a generator of an elliptic curve E[9][10][11].

Choose the point G=(68,136) on the elliptic curve. Alice selects a private key 'a'=6, and generates the public key A='aG' = 6(68,136)= (85, 199) and Bob selects a private key 'b'=8, and generates the public key B= 'bG' = 8(68,136)= (122 , 259).

Encryption:

Step 1: Alice chooses a random integer k =4, and keeps it secret.

Step 2: Compute kG= 4(68,136)= (250 , 189).

Step 3: Alice selects the Bob's public key B=bG= (122, 259).

Step 4: Compute kB=k(bG)=4(122 , 259)= (132,248).

Step 5: Compute aB=a(bG)=6(122 , 259)= (215,157)=m.

Step 6: Alice wants to send the message q_i to Bob.

Step 7: Alice wants to convert the message into the points on the elliptic curve. She chooses a point Q=(172,240) which is the generator of the elliptic curve. By using ASCII characters, of upper letters into the points on the elliptic curve.

$I \to 73(172,240) = (183, 38),$

$N \to 78(172,240) = (69,18),$

$T \to 84(172,240) = (126,260),$

$E \to 69(172,240) = (225, 189),$

$R \to 82(172,240) = (168,235),$

$N \to 78(172,240) = (69,18),$

$A \to 65(172,240) = (64,246),$

$T \to 84(172,240) = (126,260),$

$I \to 73(172,240) = (183, 38),$

$O \to 81(172,240) = (93,5),$

$N \to 78(172,240) = (69,18),$

$A \to 65(172,240) = (64,246),$

$L \to 76(172,240) = (120, 261),$

$1 \to 61(172,240) = (97,235),$

$2 \to 62(172,240) = (55,93),$

$3 \to 63(172,240) = (256,259).$

Then the points are

$$T = \{(183, 38), (69,38), (126,260), (225,189), (168,235), (69,18), (64,246), (126,260), (183,38), (93,5), (69,18), (64,246), (120,261), (97,235)(55,93)(256,259)\}$$

Step 8: To create 4×4 matrix with entries are the points on the elliptic curve.

$$m_1 = \begin{pmatrix} (183,38) & (69,18) & (126,260) & (225,189) \\ (168,235) & (69,18) & (64,246) & (126,260) \\ (183,38) & (93,5) & (69,18) & (64,246) \\ (120,261) & (97,235) & (55,93) & (256,259) \end{pmatrix}$$

Step 9: Alice selects $m = (215,157)$, where $s = 215$ and the binary value of 215 is 11010111which is input key.

Step 10: Alice define Moore machine with input is secret key. And compute $q_{k+1} = q_k \times [adjency\ \ matrix]^{output\ \ q_{k+1}\ state}$

S. No	I/P	Previous State	Preset State	O/P	n= O/P+1	Cipher text
1	1	q_0	q_1	1	2	$\begin{pmatrix} (182,258) & (170,151) & (260,66) & (147,226) \\ (251,160) & (40,168) & (36,168) & (153,151) \\ (30,80) & (164,12) & (36,103) & (40,103) \\ (32,100) & (231,43) & (228,71) & (71,244) \end{pmatrix}$
2	1	q_1	q_3	3	4	$\begin{pmatrix} (142,258) & (107,173) & (173,23) & (68,135) \\ (262,132) & (59,109) & (64,25) & (134,51) \\ (183,233) & (64,25) & (107,98) & (93,266) \\ (123,155) & (48,205) & (91,244) & (246,38) \end{pmatrix}$
3	0	q_3	q_2	2	3	$\begin{pmatrix} (159,162) & (168,235) & (153,151) & (60,268) \\ (139,33) & (122,12) & (1,214) & (120,10) \\ (230,198) & (207,73) & (228,200) & (208,95) \\ (151,71) & (35,253) & (17,64) & (56,2) \end{pmatrix}$
4	1	q_2	q_1	1	2	$\begin{pmatrix} (132,248) & (230,73) & (40,103) & (262,239) \\ (133,176) & (168,36) & (225,82) & (38,111) \\ (161,31) & (67,82) & (109,244) & (168,36) \\ (25,170) & (126,260) & (258,194) & (119,60) \end{pmatrix}$
5	0	q_1	q_2	2	3	$\begin{pmatrix} (170,120) & (135,222) & (237,23) & (38,160) \\ (229,51) & (253,111) & (88,101) & (237,248) \\ (2,269) & (156,171) & (122,12) & (85,199) \\ (30,191) & (228,71) & (182,13) & (164,12) \end{pmatrix}$
6	1	q_2	q_1	1	2	$\begin{pmatrix} (195,168) & (194,141) & (182,258) & (256,12) \\ (228,71) & (43,10) & (28,214) & (134,220) \\ (13,5) & (212,199) & (67,189) & (40,168) \\ (161,31) & (36,168) & (213,269) & (192,116) \end{pmatrix}$
7	1	q_1	q_3	3	4	$\begin{pmatrix} (123,116) & (35,18) & (185,93) & (257,222) \\ (107,98) & (221,210) & (7,135) & (260,205) \\ (229,220) & (153,151) & (38,160) & (15,98) \\ (242,214) & (221,210) & (167,18) & (234,205) \end{pmatrix}$

8	1	q_3	q_3	3	4	$\begin{pmatrix} (59,109) & (168,36) & (153,120) & (135,222) \\ (139,238) & (122,259) & (1,57) & (120,261) \\ (80,211) & (150,49) & (69,253) & (60,3) \\ (51,45) & (237,23) & (135,222) & (235,43) \end{pmatrix}$

Then the points are

$$R = \{(59,109)(168,36)(153,120)(135,222)(139,238)(122,259)(1,57)(120,261)(80,211)(150,49)(69,253)(60,3)(51,45)(237,23)(135,222)(235,43)\}.$$

$Step\ 11: Compute\ \ C_i = q_i + abG + kbG$

$C_1 = (59,109) + (132,248) + (215,157) = (49,207),$
$C_2 = (168,36) + (132,248) + (215,157) = (120,261),$
$C_3 = (153,120) + (132,248) + (215,157) = (156,100),$
$C_4 = (135,222) + (132,248) + (215,157) = (167,253),$
$C_5 = (139,238) + (132,248) + (215,157) = (230,198),$
$C_6 = (122,259) + (132,248) + (215,157) = (231,228),$
$C_7 = (1,57) + (132,248) + (215,157) = (83,100),$
$C_8 = (120,261) + (132,248) + (215,157) = (19,139),$
$C_9 = (80,211) + (132,248) + (215,157) = (205,64),$
$C_{10} = (150,49) + (132,248) + (215,157) = (95,210),$
$C_{11} = (69,253) + (132,248) + (215,157) = (226,61),$
$C_{12} = (60,3) + (132,248) + (215,157) = (179,51),$

$C_{13} = (51,45) + (132,248) + (215,157) = (105,73),$
$C_{14} = (237,23) + (132,248) + (215,157) = (35,18),$
$C_{15} = (135,222) + (132,248) + (215,157) = (157,268)),$
$C_{16} = (235,43) + (132,248) + (215,157) = (119,60).$

Step12: Now Alice sends the encrypted message consisting of pair of points

$$\{((250,189),(49,207))((250,189),(120,261)),((250,189),(156,100))((250,189),(167,253))(250,189),(230,198))(250,189),(231,228))(250,189),(83,100))(250,189),(19,139))(250,189),(205,64))(250,189),(95,210))(250,189),(226,61))(250,189),(179,51))(250,189),(105,73))((250,189),(35,18))(250,189),(167,253))(250,189),(119,60))\}.$$

to Bob.

Decryption:

Bob applies the reverse process and recovers the message “INTERNATIONAL123”.

VI. Conclusions:

In the proposed work, the plain text is converted to points on the elliptic curve by one to one correspondence using ASCII characters. The encryption process uses the finite state machines, adjacency matrices and the key generation process uses the ElGamal encryption taking security, confidentiality, and authenticity into consideration. The obtained cipher text becomes quite difficult to break or to extract the original information even if the algorithm is known.

References:

[1]. N.Kobliz.Elliptic curve Cryptosystem Mathematics of computation, 48203-209, 1987.

[2]. A text book of Guide to elliptic curve Cryptography by Darrel Hancott Vanstone.

[3]. N. Kobliz. Hyper Elliptic Cryptosystem. International Journal of Cryptography, 139-150, 1989.

[4]. An introduction to the theory of Elliptic Curves by Joseph H.Silverman brown University and NTRU Cryptosystems.

[5]. A text book of Cryptography and Network Security by William Stallings.

[6]. Adesh K.Pandey. reprint 2009, “An introduction to automata theory and formal languages S.K.Kararia & sons. New Delhi.

[7]. Johan E.Hopcroft, Rajeev Motwin, Jeffrey D.Uiman. “Introduction to automata theory, language, and computation ” Vanstone 3 rd impression, 2007 CRC press, Dorling Kindersley (India)Pvt.Ltd.

[8]. http://www.certicom.com/index.php/ecc-tutorial.

[9]. P.A.Jyotirmie, B.Ravi Kumar, A.Chandra Sekhar, S.Uma Devi “A One to one Correspondence in elliptic Curve Cryptography” International Journal of Mathematical archive-4(3),2013: 300-304.

[10]. B.krishna Gandhi, A.Chandra Sekhar, S.Srilaksmi. “Cryptography Scheme for Digital Signals using Finite State

Machines" International Journal of Computer Applications, September 2011.

[11] K.R.Sudha , A.chandra Sekhar ,Prasad Reddy P.V.G.D. "Cryptography Protection of Digital Signals using Some recurrence relations" International Journal of Computer Science and Network security, Vol (7) no 5 may 2007, 203-207.

[12] T.ElGamal,"A public-key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, on Information Theory, 469- 472, 1985.