International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Elliptic Curve Elgamal Encryption Scheme using Higher-Order Golden Matrices

Ravi Kumar Bora, Simhachalam Boddana, A Chandra Sekhar, V Santosh Kumar

***Abstract:** In this paper, we proposed ElGamal encryption scheme of elliptic curves based on the golden matrices. This algorithm works with a bijective function identified as characters of ASCII from the elliptic curve points and the matrix produced the additional private key, which was obtained from golden matrices defined by A.P Stakhov.*

***Keywords**: ElGamal, decryption, elliptic curves, encryption, golden matrices*

I. INTRODUCTION

Most personal key problems have been overcome after the creation of public key cryptography. Public key authentication is the creation of enormous development in the past of cryptography. The main cryptosystem for the public key is Elliptic Curve Cryptography (ECC) that also ensures better safety bit than other public key cryptosystem known today and ECC can utilize significantly shorter key and offer the equal rate of safety as other much larger asymmetric algorithms, thereby reducing processing overhead. Protection of these public key cryptosystems depends on number of computational problems which are well known to perform as one way [1]. The cryptosystem which relies upon the discrete logarithm problem was presented by Taher ElGamal in 1984[2]. The ElGamal works with one-way functions where the encryption and decryption are done with two unique functions.

Manuscript published on January 30, 2020.
* Correspondence Author
Dr. Ravi Kumar Bora*, Department of Mathematics, GIS, GITAM (Deemed to be University), Visakhapatnam, INDIA.
Email: ravikumarbrk6@gmail.com
Dr. Simhachalam Boddana, Department of Mathematics, GITAM University, Visakhapatnam, INDIA. Email: drbschalam@gmail.com
Dr. A Chandra Sekhar, Professor & HOD Department of Mathematics, GIS, GITAM (Deemed to be University), Visakhapatnam, INDIA.Email: acs@gitam.edu
V Santosh Kumar, Assistant Professor, Department of ECE, GITAM (Deemed to be University), Visakhapatnam.

A. *Fibonacci Q_α-matrix*

The number theory of Fibonacci determines the prospect of modern utilization for technical outcomes view in last decades [3,4].

The Fibonacci Q_α -matrix was suggested in [5], where

$$Q_\alpha = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \tag{1}$$

is derive from the recurrence relation of Fibonacci,

$$G\vartheta'_{l+1} = G\vartheta'_l + G\vartheta'_{l-1}. \tag{2}$$

With $G\vartheta'_1 = G\vartheta'_2 = 1.$ (3)

Later Q_α was extended to $Q_\alpha^{\,l}$ for integer l,

$$Q_\alpha^{\,l} = \begin{pmatrix} G_{\vartheta}'_{l+1} & G_{\vartheta}'_{l} & 0 \\ G_{\vartheta}'_{l} & G_{\vartheta}'_{l-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{4}$$

consequently the similarity between $det\, Q_\alpha^{\,l}$ and the "Cassini formula",

$$Det\, Q_\alpha^{\,l} = G\vartheta'_{l+1} G\vartheta'_{l-1} - G\vartheta'^{\,2}_{l} = (-1)^l. \tag{5}$$

II. THE "GOLDEN" MATRICES

The "golden" [6] matrices which are the variables of continuous functions 'ν' described A.P Stakhov using the classical Fibonacci Q_α-matrix and the symmetrical hyperbolic Fibonacci functions, as follows [7,8,9,10].

$$Q_\alpha^{2\nu} = \begin{pmatrix} CG_{s_\kappa}(2\nu+1) & SG_{s_\kappa}(2\nu) & 0 \\ SG_{s_\kappa}(2\nu) & CG_{s_\kappa}(2\nu-1) & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{6}$$

$$Q_\alpha^{2\nu+1} = .\begin{pmatrix} SG_{s_\kappa}(2\nu+2) & CG_{s_\kappa}(2\nu+1) & 0 \\ CG_{s_\kappa}(2\nu+1) & SG_{s_\kappa}(2\nu) & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{7}$$

$$where\;\; SG_{s_\kappa}(\nu) = \frac{\tau_\eta^{\ \nu} - \tau_\eta^{\ -\nu}}{\sqrt{5}}, CG_{s_\kappa}(\nu) = \frac{\tau_\eta^{\ \nu} + \tau_\eta^{\ -\nu}}{\sqrt{5}}$$

$$and\;\; \tau_\eta = \frac{1+\sqrt{5}}{2} (the\ Golden\ proportion).$$

The inverse matrices for (6) and (7) are developed by A.P Stakhov [3] for the continuous variable 'ν' as the following form.

$$Q_{\alpha}^{-2\nu} = \begin{pmatrix} CG_{s_\kappa}(2\nu-1) & -SG_{s_\kappa}(2\nu) & 0 \\ -SG_{s_\kappa}(2\nu) & CG_{s_\kappa}(2\nu+1) & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{8}$$

$$Q_{\alpha}^{-(2\nu+1)} = \begin{pmatrix} -SG_{s_\kappa}(2\nu) & CG_{s_\kappa}(2\nu+1) & 0 \\ CG_{s_\kappa}(2\nu+1) & -SG_{s_\kappa}(2\nu+2) & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{9}$$

In this paper, we proposed ElGamal elliptic curve encryption scheme and the secret key has been formed by the matrix, acquired from higher order golden matrices defined by A.P Stakhov.

III. PROPOSED ALGORITHM

Romeo needs to deliver the message to Juliet using ElGamal's elliptic curve encryption and golden matrices. Romeo prefers the elliptic curve $y^2 = x^3 + ux + v$ over the field $Z^*_{p.}$ By selecting the elliptic curve point $Q' = (x, y)$ and a private key *'l'*, Romeo has generated the public key β = *'lQ'*. In this regard, Juliet also has chosen a personal key *'m'* and generates the public key γ = *'m Q''*.

A. Encryption

Romeo prefers a random integer α and maintains it secret. He computes α*Q'* and selects Juliet's public key γ = *mQ'*, then evaluates αγ= α*(mQ')*, in addition to *l*γ = *l(m Q')*.As Romeo requires sending the message to Juliet, the message becomes the points on the elliptic curve and adopts a point 'ρ' as the generator of the elliptic curve cyclic group. Let $A' = \{1þ', 2þ', 3þ' \ldots \ldots nþ'\}$ and set B' characters of ASCII. Set $h': A' \rightarrow$ B' as $h'(n\rho') = \grave{a}'_n$, where $n = 1, 2, \ldots$.and $\{\grave{a}'_1, \grave{a}'_2, \grave{a}'_{3,\ldots\ldots}\}$ are the characters of ASCII which is the first step of protection.

Then the set

$\mu = \{\grave{a}'_1(æ_1, ý_1), \grave{a}'_2(æ_2, ý_2), \grave{a}'_3(æ_3, ý_3), \grave{a}'_4(æ_4, ý_4), \ldots\}$ (10)

where $\grave{a}'_i \in$ A and $(æ_i, ý_i) \in E$ and arranges in a 3×3-square matrix.

$$\vartheta = \begin{pmatrix} \grave{a}'_1 & \grave{a}'_2 & \grave{a}'_3 \\ \grave{a}'_4 & \grave{a}'_5 & \grave{a}'_6 \\ \grave{a}'_7 & \grave{a}'_8 & \grave{a}'_9 \end{pmatrix} \tag{11}$$

Romeo prefers a direct "golden matrices" (6), (7) and then the enciphering matrix by taking the personal key '$\nu = y_1$', which is the third step of protection of ElGamal elliptic curve encryption method, based on "golden" matrices.

$$\vartheta \times Q^{2y_1} = \begin{pmatrix} \grave{a}'_1 & \grave{a}'_2 & \grave{a}'_3 \\ \grave{a}'_4 & \grave{a}'_5 & \grave{a}'_6 \\ \grave{a}'_7 & \grave{a}'_8 & \grave{a}'_9 \end{pmatrix} \times \begin{pmatrix} CG_{s_\kappa}(2y_1+1) & SG_{s_\kappa}(2y_1) & 0 \\ SG_{s_\kappa}(2y_1) & CG_{s_\kappa}(2y_1-1) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} \chi_1 & \chi_2 & \chi_3 \\ \chi_4 & \chi_5 & \chi_6 \\ \chi_7 & \chi_8 & \chi_9 \end{pmatrix}. \tag{12}$$

where

$$\chi_1 = \grave{a}'_1 CG_{s_\kappa}(2y_1+1) + \grave{a}'_2 SG_{s_\kappa}(2y_1), \tag{13}$$
$$\chi_2 = \grave{a}'_1 SG_{s_\kappa}(2y_1) + \grave{a}'_2 CG_{s_\kappa}(2y_1-1), \tag{14}$$
$$\chi_3 = \grave{a}'_3, \tag{15}$$
$$\chi_4 = \grave{a}'_4 CG_{s_\kappa}(2y_1+1) + \grave{a}'_5 SG_{s_\kappa}(2y_1), \tag{16}$$
$$\chi_5 = \grave{a}'_4 SG_{s_\kappa}(2y_1) + \grave{a}'_5 CG_{s_\kappa}(2y_1-1), \tag{17}$$
$$\chi_6 = \grave{a}'_6, \tag{18}$$
$$\chi_7 = \grave{a}'_7 CG_{s_\kappa}(2y_1+1) + \grave{a}'_8 SG_{s_\kappa}(2y_1), \ . \tag{19}$$
$$\chi_8 = \grave{a}'_7 SG_{s_\kappa}(2y_1) + \grave{a}'_8 CG_{s_\kappa}(2y_1-1), \tag{20}$$
$$\chi_9 = \grave{a}'_9. \tag{21}$$

Or

$$\vartheta \times Q^{2y_1+1} = \begin{pmatrix} \grave{a}'_1 & \grave{a}'_2 & \grave{a}'_3 \\ \grave{a}'_4 & \grave{a}'_5 & \grave{a}'_6 \\ \grave{a}'_7 & \grave{a}'_8 & \grave{a}'_9 \end{pmatrix} \times \begin{pmatrix} SG_{s_\kappa}(2y_1+2) & CG_{s_\kappa}(2y_1+1) & 0 \\ CG_{s_\kappa}(2y_1+1) & SG_{s_\kappa}(2y_1) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} \chi_1 & \chi_2 & \chi_3 \\ \chi_4 & \chi_5 & \chi_6 \\ \chi_7 & \chi_8 & \chi_9 \end{pmatrix}. \tag{22}$$

Then the encrypted points are,

$$\xi = \{\chi_1, \chi_2, \chi_3, \chi_4, \chi_5, \chi_6, \chi_7, \chi_8, \chi_9\}. \tag{23}$$

Romeo finally computes $\lambda_i = \chi_i$ + α*(mQ')* + *l(mQ')* to send the encrypted message (αQ', λ_i) publicly to Juliet.

B. Decryption

To reclaim the plaintext from 'λ_i', Juliet has executed the decryption method.

First, Juliet selects the Romeo public key β = *lQ'* and multiplies with her own private key *m*β i.e. *m(lQ')* and finds the inverse of *m(lQ')* i.e.*–m(lQ')*. She also adds *–m(lQ')* to the part two of the message i.e. χ_i + α*mQ'* + *lmQ'* – *lmQ'* = χ_i + α*mQ'*. Now she multiplies his own personal key '*m*' with the part one of the text α*Q'*, i.e. α*mQ'* and then finds the inverse of α*mQ'* i.e. –α*mQ'* and finally she adds –α*mQ'* to the part two of the message i.e. χ_i + α*mQ'* – α*mQ'* = χ_i.

After decryption, the recovered points has been arranged in 3×3 matrices,

$$\sigma = \begin{pmatrix} \chi_1 & \chi_2 & \chi_3 \\ \chi_4 & \chi_5 & \chi_6 \\ \chi_7 & \chi_8 & \chi_9 \end{pmatrix}. \tag{24}$$

Now Juliet multiplies the recovered points with the inverse of golden matrix which is a private key.

$$\sigma \times Q^{-2y_1} = \begin{pmatrix} \chi_1 & \chi_2 & \chi_3 \\ \chi_4 & \chi_5 & \chi_6 \\ \chi_7 & \chi_8 & \chi_9 \end{pmatrix} \times \begin{pmatrix} CG_{s_\kappa}(2y_1-1) & -SG_{s_\kappa}(2y_1) & 0 \\ -SG_{s_\kappa}(2y_1) & CG_{s_\kappa}(2y_1+1) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} \rho_{11} & \rho_{12} & \rho_{13} \\ \rho_{21} & \rho_{22} & \rho_{23} \\ \rho_{31} & \rho_{32} & \rho_{33} \end{pmatrix}. \tag{25}$$

where

$$\rho_{11} = \chi_1 CG_{s_\kappa}(2y_1 - 1) - \chi_2 SG_{s_\kappa}(2y_1), \quad (26)$$

$$\rho_{12} = -\chi_1 SG_{s_\kappa}(2y_1) + \chi_2 CG_{s_\kappa}(2y_1 + 1), \quad (27)$$

$$\rho_{13} = \chi_3, \quad (28)$$

$$\rho_{21} = \chi_4 CG_{s_\kappa}(2y_1 - 1) - \chi_5 SG_{s_\kappa}(2y_1), \quad (29)$$

$$\rho_{22} = -\chi_4 SG_{s_\kappa}(2y_1) + \chi_5 CG_{s_\kappa}(2y_1 - 1), \quad (30)$$

$$\rho_{23} = \chi_6, \quad (31)$$

$$\rho_{31} = \chi_7 CG_{s_\kappa}(2y_1 - 1) - \chi_8 SG_{s_\kappa}(2y_1), \quad (32)$$

$$\rho_{32} = -\chi_7 SG_{s_\kappa}(2y_1) + \chi_8 CG_{s_\kappa}(2y_1 - 1), \quad (33)$$

$$\rho_{33} = \chi_9. \quad (34)$$

By replacing $\chi_1, \chi_2, \chi_3, \chi_4, \chi_5, \chi_6, \chi_7, \chi_8, \chi_9$ in the above expressions we get.

$$\begin{aligned}\rho_{11} &= [\grave{a}'_1\, CG_{s_\kappa}(2y_1+1) + \grave{a}'_2\, SG_{s_\kappa}(2y_1)]CG_{s_\kappa}(2y_1-1) - \\ &\quad [\grave{a}'_1\, SG_{s_\kappa}(2y_1) + \grave{a}'_2\, CG_{s_\kappa}(2y_1-1)]SG_{s_\kappa}(2y_1) \\ &= \grave{a}'_1\, CG_{s_\kappa}(2y_1+1)\, CG_{s_\kappa}(2y_1-1) + \\ &\quad \grave{a}'_2\, SG_{s_\kappa}(2y_1)\, CG_{s_\kappa}(2y_1-1) - \grave{a}'_1\, SG_{s_\kappa}(2y_1)\, SG_{s_\kappa}(2y_1) \\ &\quad - \grave{a}'_2\, CG_{s_\kappa}(2y_1-1) SG_{s_\kappa}(2y_1) \\ &= \grave{a}'_1 \{CG_{s_\kappa}(2y_1+1)\, CG_{s_\kappa}(2y_1-1) - \{SG_{s_\kappa}(2y_1)\}^2. \quad (35)\end{aligned}$$

Using the fundamental identity [6] the decrypted point is,

$$\rho_{11} = \grave{a}'_1, \quad (36)$$

$$\rho_{12} = \grave{a}'_2, \quad (37)$$

$$\rho_{13} = \grave{a}_3, \quad (38)$$

$$\rho_{21} = \grave{a}'_4, \quad (39)$$

$$\rho_{22} = \grave{a}'_5, \quad (40)$$

$$\rho_{23} = \grave{a}'_6, \quad (41)$$

$$\rho_{31} = \grave{a}'_7, \quad (42)$$

$$\rho_{32} = \grave{a}'_8, \quad (43)$$

$$\rho_{33} = \grave{a}'_9. \quad (44)$$

Juliet recovers the plaintext through the decrypted points on the elliptic curve by using the inverse procedure over characters of ASCII.

IV. EXAMPLE

Romeo requires sending the message to Juliet using ElGamal elliptic curve encryption by using golden matrices. Romeo prefers the elliptic curve $y^2 = x^3 - 4$ over the field Z_{271}. Then the points on the elliptic curve are

E={O,(1,57),(1,214),(2,2),(2,269),(5,11),……………………

…………………………………………………………………

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

On the elliptic curve, the number of points is 271, which is a prime and then each point is the generator of the elliptic curve E selected [11,12,13,14].

By selecting the point *Q = (64, 246)* on the elliptic curve and a personal key *'l' = 42,* Romeo has generated the public key *β = 'lQ' = 42(64, 246) = (158, 101).* In this regard Juliet also has chosen a personal key *'m' = 72* and creates the public key *γ = 'mQ'= 72(64, 246) = (183, 38).*

A. *Encryption*

Romeo prefers arbitrary integer α = *32* and maintains it secret. He evaluates α*Q = 32(64, 246) = (38, 111)* and selects Juliet's public key *γ = 'mQ'= (183, 38).* He evaluates α*γ* = α*(mQ) = 32(183, 38) = (257, 222)* in addition to *lγ = l(mQ) = 42(183, 38) = (7, 136).*

Romeo requires sending the message *'*BEAUTIFUL*'* to Juliet. He transforms the text into the points on the elliptic curve $y^2 = x^3 - 4$ and chooses a point *ρ = (132, 248)* which is the generator of the cyclic group of elliptic curve E. By using characters of ASCII, the uppercase letter have been converted into points then,

B → 66(132, 248) = (59, 162),
E → 69(132, 248) = (151, 71),
A→ 65(132, 248) = (231, 43),
U → 85(132, 248) = (262, 132),
T → 84(132, 248) = (1, 214),
I → 73(132, 248) = (245, 199),
F → 70(132, 248) = (38, 160),
U → 85(132, 248) = (262, 132),
L → 76(132, 248) = (203, 174).

The converted points are

μ = {*(59, 162),(151, 71),(231, 43),(262, 132),((1, 214),(245, 199),(38, 160),(262, 132),(203, 174)}.*

Romeo creates 3×3 matrix with the converted point's i.e.

$$\vartheta = \begin{pmatrix} (59,162) & (151,71) & (231,43) \\ (262,132) & (1,214) & (245,199) \\ (38,160) & (262,132) & (203,174) \end{pmatrix}.$$

Romeo has chosen a direct "golden matrix" (6) for enciphering matrix by taking the personal key 'y_1 = 4',

$$Q^8 = \begin{pmatrix} 34 & 21 & 0 \\ 21 & 13 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

and enciphering matrix,

$$\vartheta \times Q^8 = \begin{pmatrix} (59,162) & (151,71) & (231,43) \\ (262,132) & (1,214) & (245,199) \\ (38,160) & (262,132) & (203,174) \end{pmatrix} \times \begin{pmatrix} 34 & 21 & 0 \\ 21 & 13 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} (34,238) & (48,66) & (231,43) \\ (95,210) & (163,71) & (245,199) \\ (140,11) & (72,211) & (203,174) \end{pmatrix}.$$

The points are,

ξ = *{(34, 238),(48, 66),(231, 43),(95, 210),(163, 71), (245, 199), (140, 11), (72, 211),(203, 174)}.*

Romeo finally evaluates $\lambda_i = \chi_i + \alpha(mQ) + l(mQ)$.

λ_1 = *(34, 238) + (257, 222) + (7, 136) = (65, 130),*

λ_2 = (48, 66) + (257, 222) + (7, 136) = (179, 220),
λ_3 = (231, 43) + (257, 222) + (7, 136) = (253, 160),
λ_4 = (95, 210) + (257, 222) + (7, 136) = (2, 269),
λ_5 = (163, 71) + (257, 222) + (7, 136) = (36, 103),
λ_6 = (245, 199)+ (257, 222) + (7, 136) = (135, 222),
λ_7 = (140, 11) + (257, 222) + (7, 136) = (225, 189),
λ_8 = (72, 211) + (257, 222) + (7, 136) = (215, 114),
λ_9 = (203, 174)+ (257, 222) + (7, 136) = (113, 233).

Romeo sends the encrypted message in the form of points {((38, 111), (65, 130)), ((38, 111), (179, 220), ((38, 111), (253, 160)), ((38, 111)), (2, 269)), ((38, 111), (36, 103)),((38, 111), (135, 222)), ((38, 111), (225,189)), ((38, 111), (215, 114)), ((38, 111), (113, 233))} publicly to Juliet.

B. Decryption

To reclaim the plaintext 'BEAUTIFUL' from 'λ_i', Juliet has executed the decryption method.

Juliet selects ((38, 111), (65, 130)) the first encrypted point and decrypts the plain text by using the following:

Juliet selects the Romeo public key β = 'lQ' = (158, 101) and multiplies with her own private key $m(lQ)$= 72(158, 101)) = (7, 136) and finds the inverse of (7, 136) i.e. (7, 135). She also adds (7, 135) part two of the message i.e. (7, 135) + (65, 130) = (221, 61). Now she multiplies her own private key 'm = 72' with the first part of the message αQ = (38, 111), i.e. m(αQ) = (257, 222) and finds the inverse of (257, 222) is (257, 49). Juliet adds (257, 49) part two of the message i.e. (257, 49) + (221, 61) = (34, 238).
Then she got the decrypted point χ_1 = (34, 238).
In the same manner, the decrypted points are
χ_2 = (48, 66), χ_3 = (231, 43), χ_4 = (95, 210), χ_5 = (163, 71), χ_6 = (245, 199), χ_7 = (140, 11), χ_8 = (72, 211), χ_9 = (203, 174).
ξ = {(34, 238), (48, 66), (231, 43), (95, 210), (163, 71), (245, 199), (140, 11), (72, 211),(203, 174)}.
After decryption, the recovered points have been arranged in 3×3 matrix.

$$\sigma = \begin{pmatrix} \chi_1 & \chi_2 & \chi_3 \\ \chi_4 & \chi_5 & \chi_6 \\ \chi_7 & \chi_8 & \chi_9 \end{pmatrix} = \begin{pmatrix} (34,238) & (48,66) & (231,43) \\ (95,210) & (163,71) & (245,199) \\ (140,11) & (72,211) & (203,174) \end{pmatrix}.$$

Now, Juliet multiplies the recovered points with the inverse of the golden matrix.

$$\sigma \times Q^{-8} = \begin{pmatrix} (34,238) & (48,66) & (231,43) \\ (95,210) & (163,71) & (245,199) \\ (140,11) & (72,211) & (203,174) \end{pmatrix} \times \begin{pmatrix} 13 & -21 & 0 \\ -21 & 34 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$= \begin{pmatrix} (59,162) & (151,71) & (231,43) \\ (262,132) & (1,214) & (245,199) \\ (38,160) & (262,132) & (203,174) \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{pmatrix}.$$

Then Juliet retrieves the text as:

a_1 = (59, 162) → B
a_2 = (151, 71) → E
a_3 = (231, 43) → A
a_4 = (262, 132) → U
a_5 = (1, 214) → T
a_6 = (245, 199) → I
a_7 = (38, 160) → F
a_8 = (262, 132) → U
a_9 = (203, 174) → L

Ultimately, Juliet receives the message "BEAUTIFUL" from Romeo.
Using this algorithm Romeo securely sends "BEAUTIFUL" to Juliet by modified ElGamal encryption scheme over elliptic curve cryptography. He encrypted the text "BEAUTIFUL" by using characters of ASCII and higher order golden matrices and send to Juliet. She decrypts the text by using inverse procedure over elliptic curve Elgamal encryption scheme and golden matrices.

V. CONCLUSION

The ElGamal encryption scheme is developed by framing a bijective function from the points on the elliptic curve to characters of ASCII. With the matrix reaching from golden matrices, the secret key has been developed and the matrix plays a vital role in the inverse concept. This algorithm is safer in three stages of ElGamal elliptic curve security using higher-order golden matrix.

REFERENCES

1. N. Koblitz. Elliptic curve Cryptosystems. Mathematics of computation, 48203-209, 1987.
2. ElGamal. T, "A public-key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, on Information Theory, 469-472, 1985.
3. Hoggat VE. Fibonacci and Lucas numbers. Palo Alto, CA: Houghton-Mifflin; 1969.
4. T. Koshy, Fibonacci and Lucas Numbers with Applications, John Wile y and Sons, NY, 2001.
5. Stakhov OP.A generalization of the Fibonacci Q-matrix. Rep Nat Acad Sci Ukraine1999 (9):46-9.
6. Stakhov AP. "The ''golden'' matrices and a new kind of cryptography", Chaos, Solutions and Fractals 32 (2007) pp1138–1146.
7. Stakhov AP. Codes of the golden proportion. Moscow: Radio and Communications; 1984[in Russian].
8. Stakhov AP. The golden section in the measurement theory. Comput Math Appl 1989; 17(4–6):613–38.
9. Stakhov AP, Tkachenko IS. Hyperbolic Fibonacci trigonometry. Rep Ukr Acad Sci 1993; 208(7):9–14 [in Russian].
10. Stakhov AP. The golden section and modern harmony mathematics. Applications of Fibonacci numbers, 7. Kluwer Academic Publishers; pages 393–99, 1998.
11. Apostol T M, "Introduction to analytic number theory". New York: Springer-Verlag, 1976.
12. B.Ravi Kumar, A. Chandra Sekhar, G. Appala Naidu "A Novel ElGamal Encryption Scheme of Elliptic Curve Cryptography" International Journal of Computer Trends and Technology, Volume 20, Number 2, pages 70-73, 2015.
13. Darrel Hancott Vanstone, "A text book of Guide to elliptic curve Cryptography" 1965.
14. B. Ravi Kumar, A. Chandra Sekhar, G. Appala Naidu, "An Encryption Scheme of points on the Elliptic Curve and Golden Matrices" Asian Journal Mathematics and Computer Research, Volume 15, pages 113-122, 2017.

AUTHORS PROFILE

Dr. Ravi Kumar Bora obtained his Masters Degree in Applied Mathematics from Andhra University Visakhapatnam, India in 2003. He received his Ph.D from Andhra University Visakhapatnam, India in 2019. He is presently working as an Assistant Professor in the Department of Mathematics at GITAM (Deemed to be University), Visakhapatnam. His research areas include Number theory and Cryptography and image processing.

Dr. B Simhachalam, obtained his M.Sc. (Applied Mathematics, 2005), M.Phil. (Applied Mathematics, 2007) and M.Tech. (Information Technology, 2009) from Andhra University, Visakhapatnam, INDIA. He did his Ph.D. from A.K.N.U. He is presently working as an Assistant Professor in the Department of Mathematics at GITAM (Deemed to be University), Visakhapatnam. He is specialized in applied group theory in Mathematics and his area of research interest is soft computing and data mining.

Dr. A Chandra Sekhar, obtained his Masters Degree in Mathematics from Andhra University Visakhapatnam, India. He achieved the prestigious K. NAGABUSHANAM memorial award in M.Sc., for obtaining University first rank. He did his M.Phil. from Andhra University in 2000. He received his Ph.D from JNT University Hyderabad, India in 2008. He is presently working as an Professor & HOD in the Department of Mathematics at GITAM (Deemed to be University), Visakhapatnam. His research areas include Number theory and Cryptography.

V Santosh Kumar, obtained his M.Tech in R&M from Andhra University Visakhapatnam, India 2006. He is pursuing Ph.D in the area of Antennas in Department of ECE GITAM (Deemed to be University), Visakhapatnam. He is presently working as an Assistant Professor in the Department of ECE at GITAM (Deemed to be University), Visakhapatnam. His areas of interest are Signal processing, Antennas and Cryptography.