Security Scheme for Data Authentication Based on Elliptic Curve Cryptography

Dr.K.Thamodaran,
Professor,
Dept. of Computer Science,
Marudupandiyar College,
Thanjavur, Tamilnadu, India-6.
k_thamodharan@rediffmail.com

Dr K.Kuppusamy
Professor and Chair,
Dept. of Computer Science and Engineering,
Alagappa University,
Karaikudi, Tamilnadu, India-630 003.
kkdiksamy@yahoo.com

Abstract— **An encryption is providing authentication and security for illicit manipulation of digital data. In this paper the security scheme for authentication and secrecy of digital data through ElGamal public key cryptographic algorithm and Elliptic Curve Cryptography is offered. To compare them with group, elliptical curve concepts are considered and generate the points. This scheme provides solutions to the issues such as authentication, robustness, security and statistical attacks. An Elliptic Curve Cryptography is employed to perform encryption with help of secret key. The experimental results are calculated and presented to demonstrate the strength of the proposed scheme.**

Keywords- Authentication, ECC, ElGamal, Encryption, Key Exchange, Security.

I. INTRODUCTION

The liability of data encryption technique has expanded the necessity to limit the illegitimate access of digital contents. Digital contents such as data can be modified simply either intentionally or unintentionally. In the direction of exchange data between two parties on the network, it is very important to provide confidentiality. Cryptography is very important to provide confidentiality and security against statistical attacks and other types of attacks when exchange data between two parties on the network. In 1976, Stanford University Professor Martin Hellman and graduate student Whitfield Diffie first publicly described public key cryptography. The diffie Hellman protocol defines a secure method for exchanging the keys that will encrypt or decrypt the data. The diffie HellMan scheme solves secret key cryptography's key exchange problem by employing two keys. One key is used to encrypt the plaintext and other key is used to decrypt the cipher text [1],[2].

Elliptic Curve Cryptography (ECC) is a public key cryptography algorithm which involves some high level calculation using mathematical curves to encrypt and decrypt data. Alessandro Cilardo et al expresses the concept of Elliptic Curve Cryptography as a complex interdisciplinary research field including such fields as computer science and electrical engineering [3]. Kristin Lauter has offered about the role of Elliptic Curve Cryptography for security of wireless communication [4]. Lawrence C. Washington has proposed proofs to many theorems to understand the concept of elliptic curves [5].O.S. Rao and S.P. Setty have offered static mapping method and dynamic mapping method. In static mapping method one-to-one was found which is weak; but in dynamic mapping, for one character, different options were available to choose as a point which is s very difficult to find the corresponding character of the plain message[6].

The researchers have identified alternative system to provide the same level of security by means of smaller keys instead of having large keys like RSA and Diffie-Hellman asymmetric key cryptosystem [7]. S.V.Sathyanarayana,M.Aswatha Kumar and K.N.Hari Bhat have suggested the properties of finite fields and elliptic curves to design the stream cipher system. Additive and Affine encryption key sequences are derived and investigated from random elliptic curve points using six schemes [8]. The RSA algorithm engaged with a public key and a private key for encryption and decryption process. Reasonable amount of time is required to decrypt the message using the private key when compared with encryption using public key[9]. S. Gupta, P.S. Gill, A. Mishra and A. Dwivedi have illustrated the security system for transmission of medical image, in which the DCT transform, quantization, compression, elliptic curve cryptography are employed. Error detection and correction methods are played vital role and compressed images are considered as plaintext and encrypted[10]. Loai Tawalbeh, Moad Mowafi and Walid Aljoby have applied elliptic curve cryptography for encryption process along

with multimedia compression. An encryption efficiency, compression efficiency, codec compliance and security are measured and analysed [11].

Sonia Goyat has suggested the security scheme with help of genetic algorithm and cryptography. In this scheme modified approach is applied to generate keys that have more strength. There is no repetition of random values used in key generation [12]. Ali Soleymani, Md Jan Nordin, Azadeh Noori Hoshyar, Elankovan Sundararajan have offered cryptosystem through elliptic curves and public key system. The Add, Double, Multiply operations are applied on the points that lie on a predefined elliptic curve. The conversion of a message or pixel to a coordinate on the affined curve is essential for any ECC-based encryption. In this scheme the novel proposed mapping method is used to convert the pixels of a plain image into the coordinates of points on the curve[13]. Omotheinwa T.O, Ramon S.O have proposed the structure of magic rectangle in the sums of all the elements in every row as well as columns are to be equal. The order of the matrix is even but not divisible by four such as 4x6, 8x12, 16x24, 32x48 etc. The size of the rectangle is purely based on the rules of perfect rectangle or golden rectangle and also the singly even magic rectangle [14]. Balamurugan. R, Kamalakannan. V, Rahul Ganth. D and Tamilselvan.S have recommended the fast mapping technique using a non singular matrix. During the first step they map the message to points on elliptic curve and the next step an ElGamal encryption method is applied to encode the points using a non singular matrix. During decryption inverse of the non singular matrix is used[15].

The rest of this paper is organized as follows. Section II provides the information about Elliptic Curve Cryptography. Section III describes our proposed data encryption system based on ElGamal public key cryptographic algorithm and Elliptic Curve Cryptography. The experimental results and security analysis are presented in Section IV and Section V concludes this paper.

II. ELLIPTIC CURVE CRYPTOGRAPHY

In 1985, Neal Koblitz and Victor Miller independently proposed using elliptic curves to design public-key cryptographic systems. An elliptic curve is naturally a group and the group properties are constructed geometrically. Elliptic curve cryptography works with points on curve. The security of this type of public key cryptography depends on the elliptic curve discrete logarithm problem. An ECC is an asymmetric cryptography algorithm which involves some high level calculation using mathematical curves to encrypt and decrypt data. Elliptic curves are materialized in various areas of mathematics, ranging from number theory to complex analysis, and from cryptography to mathematical physics. Since then an abundance of research has been published on the security and efficient implementation of elliptic curve cryptography. In the late 1990's, elliptic curve systems started receiving commercial acceptance when accredited [1], [16].

Elliptic curves are simple functions that can be drawn as gently looping lines in the (x, y) plane. ECC represent a different way to perform public key cryptography and alternative to the older RSA algorithm and also offers some benefits. The main advantage of elliptic curve cryptography is that the keys can be much smaller. Elliptic curve cryptography affords a methodology for achieving high speed, efficient, scalable implementation of networks security protocols. The most important of these benefits is greater security and a more computationally efficient performance with smaller key sizes than other public keys. This characteristic changed ECC into an acceptable choice for real time multimedia applications. Due to large sizes and high data rates of multimedia data types, such as images, videos, and audio, a cryptosystem using a small key size, with high security was needed[17], [18]. An elliptic curve is shown in figure(1) must satisfy the equation (1) .

$$4a^3 + 27b^2 \bmod p \neq 0 \quad \text{for} \quad 0 \leq x < p \tag{1}$$

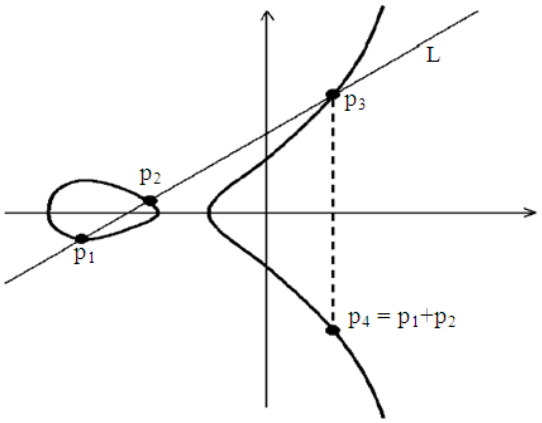

Figure 1. An elliptic curve.

III. PROPOSED DATA ENCRYPTION SYSTEM

A. Cryptography Based On Group

The protocols are necessitating the use of a finite abelian group G, of order #G, which is assumed to be cyclic. The group of interest in this work is the additive group of points on an elliptic curve. However, it is convenient to assume the group is multiplicative, with generator g, and that the order #G, is a prime. If this is not the case, always take a prime order subgroup of G as our group, with no loss of security. Elliptic curve cryptosystems are just another way of implementing discrete logarithm methods. An elliptic curve is basically a set of points that satisfy the equation (2).

$$y^2 = x^3 + ax + b \tag{2}$$

When considered in finite field of characteristic p (where p must be larger than 3). A slightly different equation is needed for the case of small characteristic, p = 2 and p = 3. The points on elliptic curves can be added together and they form a structure called a group (in fact an abelian group). The arithmetic operations such as addition and subtraction are performed with elliptic curves.

B. Construction of an Elliptic Group

Let the prime number p = 23 and let the constants a = 1 and b = 1 as well. Preliminary verify that

$(4a^3 + 27b^2) \bmod p = (4\times 1^3 + 27\times 1^2) \bmod 23$

$(4a^3 + 27b^2) \bmod p = (4+27) \bmod 23 = 31 \bmod 23$

$(4a^3 + 27b^2) \bmod p = 8 \neq 0$

Then determine the quadratic residues Q_{23} from the reduced set of residues $Z_{23} = \{1, 2, 3,...,21, 22\}$:

Table 1. Construction of $(x^2 \bmod P)$ and $(p-x)^2 \bmod P$.

S.No.	$(x^2 \bmod P)$	$(p-x)^2 \bmod P$.	=
1	$1^2 \bmod 23$	$22^2 \bmod 23$	1
2	$2^2 \bmod 23$	$21^2 \bmod 23$	4
3	$3^2 \bmod 23$	$20^2 \bmod 23$	9
4	$4^2 \bmod 23$	$19^2 \bmod 23$	16
5	$5^2 \bmod 23$	$18^2 \bmod 23$	2
6	$6^2 \bmod 23$	$17^2 \bmod 23$	13
7	$7^2 \bmod 23$	$16^2 \bmod 23$	3
8	$8^2 \bmod 23$	$15^2 \bmod 23$	18
9	$9^2 \bmod 23$	$14^2 \bmod 23$	12
10	$10^2 \bmod 23$	$13^2 \bmod 23$	8
11	$11^2 \bmod 23$	$12^2 \bmod 23$	6

Therefore set of (p-1) / 2 = 11 quadratic residues $Q_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16,18\}$. For 0 = x < p, calculate $y^2 = (x^3 + x + 1) \bmod 23$ and determine if y^2 is in the set of quadratic residues Q_{23}:

Table 2. Construction of $y^2 = (x^3+x+1) \bmod 23$

x.	y^2	$y^2 \in Q_{23}$?	y_1	y_2	x.	y^2	$y^2 \in Q_{23}$?	y_1	y_2
0	1	Yes	1		12	16	Yes	4	19
1	3	Yes	7		13	3	Yes	7	16
2	11	No	-	-	14	22	No	-	-
3	8	Yes	10	13	15	10	No	-	-
4	0	No	0	0	16	19	No	-	-
5	16	Yes	4	19	17	9	Yes	3	20
6	16	Yes	4	19	18	9	Yes	3	20
7	6	Yes	11	12	19	2	Yes	5	18
8	15	No	-	-	20	17	No	-	-
9	3	Yes	7	16	21	14	No	-	-
10	22	No	-	-	22	22	No	-	-
11	9	Yes	3	20					

The elliptic group Ep (a,b)=E_{23}(1,1) thus include the points (including also the additional single point (4,0)):

E_{23}(1,1) = { (0,1), (0,22), (1,7), (1,16), (3,10), (3,13), (4,0), (5,4), (5,19), (6,4), (6,19), (7,11), (7,12), (9,7), (9,16), (11,3), (11,20), (12,4), (12,19), (13,7), (13,16), (17,3), (17,20), (18,3), (18,20), (19,5), (19,18) }

In this proposed method ElGamal public key cryptographic algorithm is used for encryption and decryption process based on with group and without group.

C. Elgamal Encryption without Group

Alice wishes to send a message to Bob. Her message, m, is assumed to be encoded as an element in the group. Bob has a public key consisting of g and $h = g^x$, where x is the private key.

Step 1. Alice generates a random integer $k \in \{1,\ldots,\#G-1\}$ and computes $a = g^k$, $b = h^k m$.

Step 2. Alice sends the cipher text (a, b) to Bob.

Step 3. Bob can recover the message from the equation $ba^{-x} = h^k mg^{-kx} = g^{xk-xk} m = m$.

The Numerical Example is given in this section for Elgamal encryption without group.

To Encrypt a character, say 'A', consider its ASCII value. The ASCII value for 'A' is 65. Thus m = 65.

Procedure:

Let the private key x = 3 and the public key g=5 then $h = g^x = 53 = 125$.

Step 1. Let the random integer k = 4 ,

$a = g^k = 5^4 = 625$.

$b = h^k m = 125^4 \times (65) = (244140625 \times 65) = 15869140625$.

Step 2. Thus the Cipher text for 'A' is (625, 5869140625)

Step 3. To recover the message $ba^{-x} = 15869140625 \times (625)^{-3} = 65$, m = 65 = 'A'.Thus the character 'A' is recovered.

D. Elgamal Encryption With Group

To generate the points, the curve $y^2 = (x^3+x+1) \bmod 256$ is considered. To encrypt a character say 'A'.Consider its ASCII value. The ASCII for 'A'is 65. But the points are generated by the Elliptic curve in a pair,say (x,y), in this example y value is taken. Thus for character 'A' , m= (65,197) is taken.

Procedure:

The numerical example is given in this section for Elgamal encryption with group.

Let the private key x=3 and the public key g = (70,40) then $h = g^x = (70,4)^3 = (113,75)$.

Step 1. Let the random integer k=4.

$a = g^k = (70, 4)^4 = (192, 120)$,

$b = h^k m = (113, 75)^4 \times 197 = (54, 115)$.

Step 2. Thus the cipher text for 'A' is (192,120) and (54, 115),

Step 3. To recover the message $Ba^{-x} = (54, 115)\ (192, 120)^{-3} = (65, 197)$. Thus the character 'A' is recovered.

IV. Experimental Results and Security Analysis

The proposed data encryption scheme explained in section III is implemented through ECC and ElGamal algorithm using with and without group. Experimentation is performed with different capacity of data bytes and observed results are presented in this section. For the given plaintext the corresponding ciphertext and decrypted text are produced by means of proposed algorithm. The plaintext is shown in figure 2. The ciphertext is created through Elgamal algorithm without using group is shown in figure 3. The decrypted Text created through Elgamal without using group is shown in figure 4. The ciphertext is created through Elgamal algorithm with group is shown in figure 5. The decrypted Text is created using Elgamal with group is shown in figure 6.

In computer science, a parallel algorithm, as opposed to a traditional serial algorithm, is an algorithm which can be executed a piece at a time on many different processing devices, and then combined together again at the end to get the correct result.

Figure 2. Plaintext

T5a 鋪 5鱖鐖 r5d5 5鈦 r5罵 p5t5鐖鎮 r5鄟 p5a 罵 5鈦鐖鍒鋪鷙 5f5r5鐖鍒 5e 鄟 t5釂 g 5鈦 r5罵 p5t5% 鍒鋪鄟 g 釂 g 鎮 5鷙鋪鈦 r5鋪 t5 5鄟 g d5 5鎮 r5鄟 p5a 釂 鄟% 鍒鋪鄟 g 釂 g 鎮 5鱖 r5釂 t5釂 g 鎮 5鈦 r5罵 p5t5鐖鎮 r5鄟 p5a 罵 滿**鷙** 5e 釂 t5鋪 r5鄟 e e 罵% 5t5a 鋪 5鷙鈦釂鋪 g 鈦鋪 5鐖 f5 5鷙鋪鈦 r5鋪 t5 5鱖 r5釂 t5釂 g 鎮 5% t5a 鋪 5鷙 t5魰 d5罵 5鐖 f5 5a 鐖鱖 5t5鐖 5鐖 b5鷙鈦魰 r5 鋪 5 5鱖 a 鄟 t5 5罵鐖魰 5鱖 r5釂 t5鋪 5鷙鐖 5鄟鷙 5t5鐖 5r5鋪 g d5鋪 r5 5釂 t5 5鷙 鋪 e 鋪鈦 t5釂 v5鋪 e 罵 5 5魰 g 釂 g t5鋪 e e 釂鎮釂 b5e 鋪 5'

Figure 3. Ciphertext created using ElGamal without group

In computer science, a parallel algorithm, as opposed to a traditional serial algorithm, is an algorithm which can be executed a piece at a time on many different processing devices, and then combined together again at the end to get the correct result.

Figure 4. Decrypted Text created using ElGamal without group

```
Tş\—na^ér)Dä¼F9İ1 Dfö’ >wçw4wsr¯x‹$dÕ9-= V\SHâù‘*Š.r.O?uUñ¥Ö}Üpy
OtyÙ-¹NçÜĞ&†væƒ)]u`r)IÂà¥¶zpÓáO oaÎ 5W7ñ+Ulp ¿r9âóì@M+çXS-
,4åØê9„Fä«-wÜ~òÍNœdP}f7g‰~rüî?DDç“ó+-å`TçN
Pğue]ÿ…àòjIf_t4[EßáësW8glùK): B—2©â Â`èdrö«ùñœêpâàçVtØ»—%"O(b
      åhp¾~äKé(õDàFÄ*î/gW¨/e5áNáBbBg Û5 5æ‘Ôf^6 *DLLòÏ5IÙGä-}yâ×br—
‘8O7äõ‡\ftÖõ3ƒ1 KÜ|CàZBuI]gjQ3Ød°Û-Ü{
Ì;d*æ³ï¦Crr¸fõTàÌl+ySp»]\»a¸Q¡|á@ tàŸFå+%µ‡pÚIåàÎr-äÍ5`!-àÖŸYİ
¥¶ +áå`1g:øƒIæ25-M Ï3b7ö³=5yrA"¿sá†-h~t8šb áêZgÒ¦iü8æ °Z?-
‡x™TâÕÑvQrF’(ëkñpw-¡p \h5tP BQeç@êğæ"—
¸rfy]@2àg"JâpĞü,ga‰R}Añ[rKö\¦¼jsı ò¾ö#ĞP
S˜5(+e Ì7½dáøMPt«»O|Zä5Vo¾3r-î
±àM(s3eÔóM /eYò çQñ1‰y˜h%+p5'+ bJ>%tâÙanNæ'ä~˜ï
 €|P(FòÓ»S}Fâ~LcŸáê1=äš6Zs{gXT_,âB-ÁväTRTI Z;çÓnR(;f_ÅC*
K8ËjòK²T4^ä“$TÜPâÅÂVØ*r„.=äúä\Õt-jPZc :YRö
      °3³#áPËót?Œj¡?áFÌdÌ/g…¿,n5æĞr!9J YY%¡É•-t ‰æa/mzäéEW÷2
Rkò‘nçdt-.uyôØ1Xd94vvñ¼[$} vS&gçx
™Af—OÙ \TÍa[¨CnçOW4zö8·oŠ2 }Ãt|klüç²v³3
ïUT çPR0¯DbEĞIcbòœxuSâÄ wjôÄ¿UOr¥Æ:äyä:·29
+õ{çÅN£cöæùû`az4mCàäÑ'î t ¿0 L'ñhz5œVçVhÊôò&À CZ$-
“rbijrwqT Má=ém-ntÚ=['äQ6X6a |fªòîY¡2çó hx ØÜ-àí()FòÈl((
¯yF5tãµv´ç"! b¨|èNræ9+jä .ÙLgÅBftd!Ø9,äÖ|ùqr+—W-«C0á¦m?¸Ft«Ğ=u
1n›ò§eW.ä_+HÑHeX|&ƒcä®ÎâÁ³òt"bS:Aál^*&~v›#ıDä&a ÂfetÇQoñ»ÙeiC ó
xá!ÅjdSô‡†-g,h|Sá9ïdug]'4tX-
Az}äô·~"e"¨7=+e.ìVEoá-Nbæ©~™pá°aOGb VW2ek5iT6ä¯q™< »U^Y}'ö9
```

Figure 5. Encrypted Text created using ElGamal with group

In computer science, a parallel algorithm, as opposed to a traditional serial algorithm, is an algorithm which can be executed a piece at a time on many different processing devices, and then combined together again at the end to get the correct result.

Figure 6: Decrypted Text created using ElGamal with group

The performance of the proposed encryption scheme is appraised by calculating the time consumption for each encryption and decryption process and the derived results are offered in the table 3. According to encryption process with group scheme is produced different cipher text for the same plan text at different places. Even though Encryption with group takes more time, the security of information is superior, because in the group concept, different cipher text are produced for the same plaintext but not in the without group scheme.

TABLE 3. PERFORMANCE OF ELGAMMAL WITH AND WITHOUT GROUP

Cipher Data Size	ElGamal Algorithm			
	Without Group		With Group	
	Encryption Time	Decryption Time	Encryption Time	Decryption Time
0.5956 KB	2.4665 Sec	1.7939 Sec	5.0114 Sec	3.6447 Sec
1.5748 KB	11.5754 Sec	8.4185 Sec	23.5183 Sec	17.1042 Sec
2.9463 KB	42.7714 Sec	31.1065 Sec	86.9007 Sec	63.2005 Sec
13.6545 KB	1981.6005 Sec	975.3190 Sec	2724.7007 Sec	1981.6005 Sec

A.Comparison of Encryption and Decryption Process

i. ElGamal Encryption without group takes 0.375 times more than its Decryption process.
ii. ElGamal Encryption with group takes 0.375 times more than its Decryption process.

The observed results (i and ii) indicates that all encryption process takes more time than its corresponding decryption process.

B. Comparison of Group and without Group

i. ElGamal Encryption with group takes 1.032 times more than its without group.
ii. ElGamal Decryption with group takes 1.032 times more than its without group.

The observed results (i and ii) indicates that both Encryption and Decryption processes with group take more time than without group.

V. CONCLUSION

An essential information is that the efficiency of the algorithm is determined not only based on the time consumption and also its security. In this proposed security system, different cipher text is created for the same plain text at the different locations. Even though encryption with group takes more time, the security of information is elevated than without group. The common measure of efficiency of the ElGamal algorithm is its time consumption and security. When compared the time consumption, encryption process is more than its decryption in all categories. When the ElGamal with and without group are compared the group concept takes more time than its without group, but at the same time with group provides more security than without group.

REFERENCES

[1] William Stallings “Cryptography and network security principles and practice” Fifth edition , person, 2011.
[2] Behrouz A Forouzan, Debdeep Mukhopadhyay “cryptography and network security” Second edition. Mc-Graw Hill,2008.
[3] Alessandro Cilardo, Luigi Coppolino, Nicola Mazzocca, and Luigi Romano,"Elliptic Curve Cryptography Engineering", Proceedings of the IEEE, Vol. 94, no. 2, pp. 395 - 406, Feb. 2006.
[4] Kristin Lauter, "The Advantages of Elliptic Cryptography for Wireless Security", IEEE Wireless Communications, pp. 62- 67, Feb. 2006.
[5] Lawrence C. Washington, Elliptic Curves Number Theory and Cryptography, Taylor & Francis Group, Second Edition (2008).
[6] O.S. Rao and S.P. Setty, “Efficient mapping method for elliptic curve cryptosystems”, Int. J. Eng.Sci. Tech., vol. 2, pp. 3651-3656, 2010.
[7] Andrej Dujella “Applications of elliptic curves in public key cryptography” Basque Center for applied Mathematics and Universidad del Pais Vasco / Euskal Herriko Unibertsitatea, Bilbao, May 2011.
[8] S.V.Sathyanarayana,M.Aswatha Kumar and K.N.Hari Bhat , ”Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points”, International Journal of Network Security, Vol.12, No.3, PP.137-150, May 2011.
[9] Ashish Agarwala R Saravanan,” A Public Key Cryptosystem Based on Number Theory” 978-1-4673-0255-5/12,IEEE2012.

[10] S. Gupta, P.S. Gill, A. Mishra and A. Dwivedi, "A scheme for secure image transmission using ECC over the fraudulence network", International Journal Adv. Res. Comput. Sci. Soft. Eng., vol. 2, no.4, pp. 67-70, 2012.
[11] Lo'ai Tawalbeh, Moad Mowafi and Walid Aljoby, Use of Elliptic Curve Cryptography for Multimedia Encryption, IET Information Security,vol. 7, issue 2, pp. 67–74, (2012).
[12] Sonia Goyat.," Genetic key generation for public key cryptography ",International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.
[13] Ali Soleymani, Md Jan Nordin, Azadeh Noori Hoshyar, Elankovan Sundararajan, "An Image Encryption Scheme Based on Elliptic Curve and a Novel Mapping Method", International Journal of Digital Content Technology and its Applications, Volume7, Number13, September 2013.
[14] Omotheinwa T.O, Ramon S.O., " Fibonacci Numbers and Golden Ratio in Mathematics and Science", International Journal of Computer and Information Technology (ISSN"2279-0764) Volume 03-Issue 04, July 2013.
[15] R. Balamurugan, V. Kamalakannan, D. Rahul Ganth and S. Tamilselvan, Enhancing Security in Text Messages Using Matrix based Mapping and ElGamal Method in Elliptic Curve Cryptography, International Conference on Contemporary Computing and Informatics, IEEE, pp. 103–106, November (2014).
[16] Guide to Elliptic Curve Cryptography, Darrel Hankerson, Alfred Menezes,Scott Vanstone , Springer,2004.
[17] V. Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology, Springer-Verlag vol. 85, pp. 417-426, 1986.
[18] N. Koblitz, "Elliptic curve cryptosystems", Mathemathics of Computation, AMS, vol. 48, no.177, pp. 203-208, 1987.