International Journal of Information & Network Security (IJINS)
Vol.2, No.4, August 2013, pp. 339~347
ISSN: 2089-3299

A Novel Approach for Enciphering Data based ECC using Catalan Numbers

F. Amounas*, E.H. El Kinani and M.Hajar*****
* R.O.I Group, Computer Sciences Department Moulay Ismaïl University,
Faculty of Sciences and Technics Errachidia, Morocco.
** A.A Group, Mathematical Department Moulay Ismaïl University,
Faculty of Sciences and Technics Errachidia, Morocco.
*** R.O.I Group, Mathematical Department Moulay Ismaïl University,
Faculty of Sciences and Technics Errachidia, Morocco.

Article Info

Article history:

Received Jun 06th, 2013
Revised Jul 15th, 2013
Accepted Jul 28th, 2013

Keyword:

Cryptography, Elliptic Curve,
Catalan numbers, Spiral Matrix,
Encryption, Decryption.

ABSTRACT

With the explosion of networks and the huge amount of data transmitted along, securing data content is becoming more and more important. Applied number theory has so many applications in cryptography. Particularly integer sequences play very important in cryptography.

The cryptosystem based on Elliptic Curve Cryptography is becoming the recent trend of public key cryptography. In the present paper novel elliptic curve encryption algorithm were proposed basing on integer sequences of Catalan numbers. The data is encrypted using a proposed approach and then scrambled the message with the help of the concept of spiral matrix, which increase the security of the message before sending across the medium. Thus the sending and receiving of message will be safe and secure with an increased confidentiality.

A comparison of the proposed technique with existing algorithms as Triple-DES and AES has been done in encryption & decryption time.

Corresponding Author:

E.H. El Kinani
Mathematical Department
Moulay Ismaïl University,
Faculty of Sciences and Technics, Box 509 Errachidia, Morocco
E-mail: elkinani_67@yahoo.com

1. INTRODUCTION

Today due to the prominence use of the internet all over the world required Network Security. Information security has become a very critical aspect of modern communication systems. Cryptography is the science of information security. Elliptic curve (EC) can be applied to cryptography as it is secure to the best of current knowledge. In the literature, many authors have tried to exploit the features of EC field to deploy for security applications (see for example [1, 2, 3, 4]). Elliptic curve cryptography bases its security on the hardness of computing discrete logarithms. More precisely, the elliptic curve discrete logarithm problem (ECDLP) consists in recovering the value of multiplier α, given points P and Q = $[\alpha]$P on an elliptic curve.

Randomness is a key ingredient for cryptography. Random bits are necessary not only for generating cryptographic keys, but are also often an integral part in the steps of cryptographic algorithms. The cryptosystem requires the generation of a new random number each time a new message is encrypted. Over the years we have come across several cryptographic algorithms designed using the integer sequences of Fibonacci numbers and Lucas numbers. This paper, however, is an attempt to propose a new elliptic curve encryption algorithm based on integer sequences of Catalan numbers [5].

In our previous works [6-12], we have presented a cryptographic algorithms based on ECC mechanism. In fact, the transformation of the message into affine points is explained. In this paper we illustrate the process of encryption/decryption based ECC using Catalan numbers.

This paper is organized as follows. Section 2 investigates the basic theory of Catalan numbers and elliptic curve. Section 3 explains the proposed technique with an example. Section 4 shows the results and comparisons of the proposed scheme with TDES [13] and AES [14]. Conclusions are drawn in the last section.

2. BACKGROUND MATHEMATICAL INFORMATION

a. Catalan Numbers

Applied Number theory has so many applications in cryptography. In 1838, Catalan numbers [5] were discovered by Belgian mathematician Eugene C. Catalan. In fact, integer sequences play very important in cryptography. Here, we are interested in integer sequences of Catalan numbers.

- **Binomial Coefficients:** Let n and r be nonnegative integers. The binomial coefficient is defined as $\binom{n}{r}$:

$$\binom{n}{r} = \begin{cases} \dfrac{n!}{r!(n-r)!} & \text{if } 0 \le r \le n \\ 0 & \text{If } r>n \end{cases}$$

- Catalan numbers are sequence of natural numbers. The Catalan number C_n is defined as:

$$C_n = \frac{2n!}{(n+1)!n!} = \frac{1}{n+1}\binom{2n}{n},\ n\geq 0. \qquad (1)$$

Every Catalan number is an integer. The set of first Catalan numbers are:

C_0= 1, C_1= 1, C_2= 2, C_3= 5, C_4= 14, C_5= 42, C_6= 132, C_7= 429, C_8= 1430, C_9= 4862, …

b. Elliptic Curve Cryptography

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz [15] and Victor Miller [16]. An elliptic curve over a field K is a nonsingular cubic curve in two variables, f(x,y) =0 with a rational point (which may be a point at infinity). The field K is usually taken to be the complex numbers, reals, rationals, and algebraic extensions of rationals or a finite field. Here we investigate elliptic curve group with the underlying field of F_p, given by the following equation:

$$y^2 = x^3 + ax + b \bmod p. \qquad (2)$$

(where p≠2,3 is a prime).

If P_1 and P_2 are on E, we can define addition $P_3 = P_1 + P_2$ as shown in Figure 1.
Multiplication is defined as repeated addition,
for example: 3P=P+P+P.

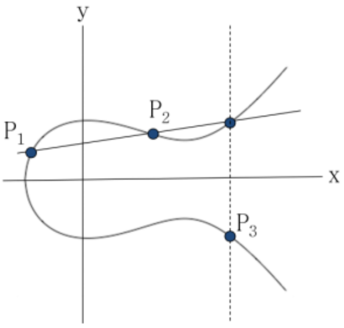

Figure 1. addition of points on elliptic curve.

Elliptic curve cryptography [ECC] is a public-key cryptosystem. Every user has a public and a private key. Public key is used for encryption/signature verification. Private Key is used for encryption/signature generation. For more details, we refer interested reader to [17].

3. MAIN RESULTS

a. New Approach using Catalan Numbers

In this section, three algorithms have been described. First technique explains the concept of session based key where as second one explains encryption technique. Third algorithm explains the decryption process.

In the proposed method, the original message is converted into points on elliptic curve noted Q_i with the help of Catalan numbers generated. Here, each character is replaced with another point on EC based on the Catalan number and security key chosen. Any one point is chosen as a first security key to generate cipher text. The characters in the cipher text depend on the security key chosen, and the Catalan numbers generated. Also, the use of randomization technique based on spiral matrix scrambles information by rearrangement and substition of content making it unreadable to anyone except the person capable of unscrambling it.

a) Generation of Session Key

During the encryption process a session based key is generated for to ensure much more security to this algorithm. The set of points follows a circular tehnique and the point which falls below the Catalan number will be taken as the secure key K_i on the elliptic curve.

We need to generate the secret integer k and compute $K=kP_B$ (with P_B is the public key of the receiver).

The results points based Catalan numbers are given by:

$$K_i = C_i K, \ i=1, 2, 3 \ldots$$

where K is the secure key.

Since the selection of the point K_i depends on the Catalan number, it provides more security for the system, and any unknown person cannot decode the message easily.

b) Steps involved in Enciphering process

Suppose that we have some elliptic curve E defined over a finite field F_p and a point P on E (F_p) that P has prime order n. The curve E and P are publicly known, as is the embedding system $M \rightarrow P_M$ which imbed plain text on an elliptic curve E. Bob chooses a random integer n_B, and publishes the point $P_B=n_BP$ (while n_B remains secret).

Then when Alice wishes to send a message M to Bob, she proceeds thus:

Step 1. Chooses a random integer k with $1 \leq k \leq n-1$ and compute a secure key $K=kP_B$.

Step 2. Imbed the original message called “plaintext” into points on elliptic curve, noted P_i, i=1..m.

Step 3. Generate Catalan sequence. By using the obtained sequence and K, we get the secure keys K_i.

Step 4. Perform addition operation between the selected point and K_i to obtain a point Q_i. Then, the encrypted block is formed.

Step 5. The binary bits of the block are taken from MSB to LSB to fit into this square matrix following the rules of spiral matrix along clock-wise direction starting from the cell (1, 1) as shown in Figure 2.

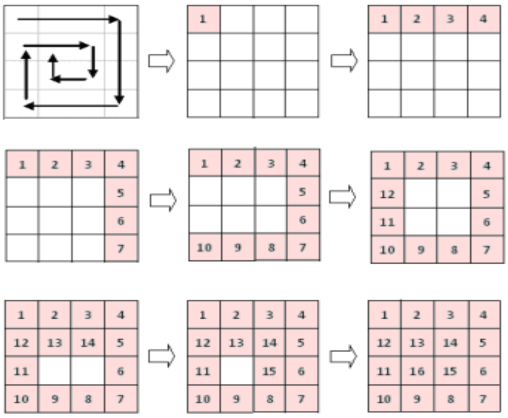

Figure 2. Example of spiral matrix (4×4)

Therefore, the cipher text is formed after combining kP with the results blocks. Then, it will be sending to the receiver. The above steps are summarized in the encryption chart shown in Figure 3.

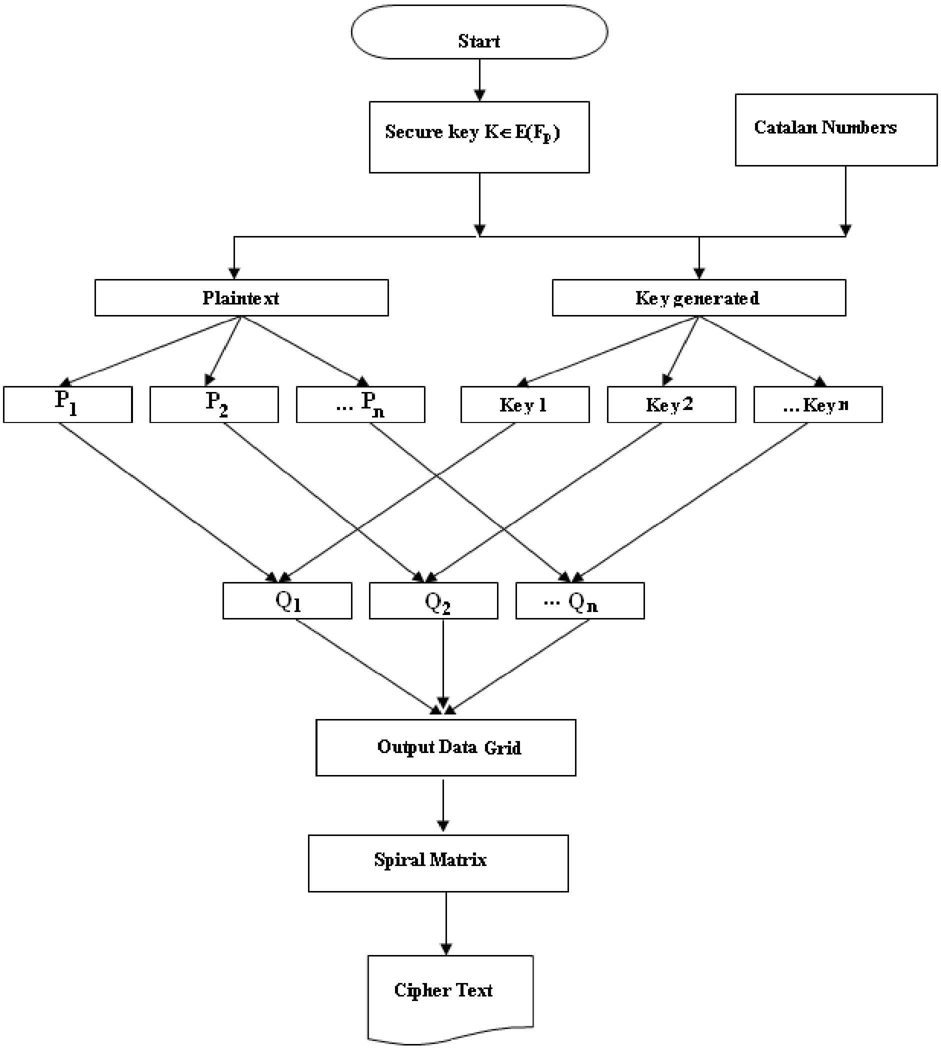

Figure 3: Flowchart – Encryption

c) Steps involved in Deciphering process

This algorithm takes encrypted stream (cipher text) as input and generates source stream (plain text) as output. In fact, the cipher text is considered as a binary bit stream.

When Bob received the above series of bits, he does the following:

Step 1. Extract the first block from the received cipher text. It is mapped to find its equivalent point noted P_1=kP. Then, applies his secret key and Compute K=$n_B P_1$.

Step 2. Extract the remaining blocks and stored into square matrix of (m×m). The decrypted block of length m is generated after taking the bits from the square matrix following the reverse rule of spiral matrix.

Step 3. Generate the secure keys (K_i) basing K and Catalan numbers.

Step 4. Substract it from the selected point to obtain the embedding point P_M. The plain text is regenerated after converting the obtained points into characters.

The above steps are summarized in the decryption chart shown in Figure 4.

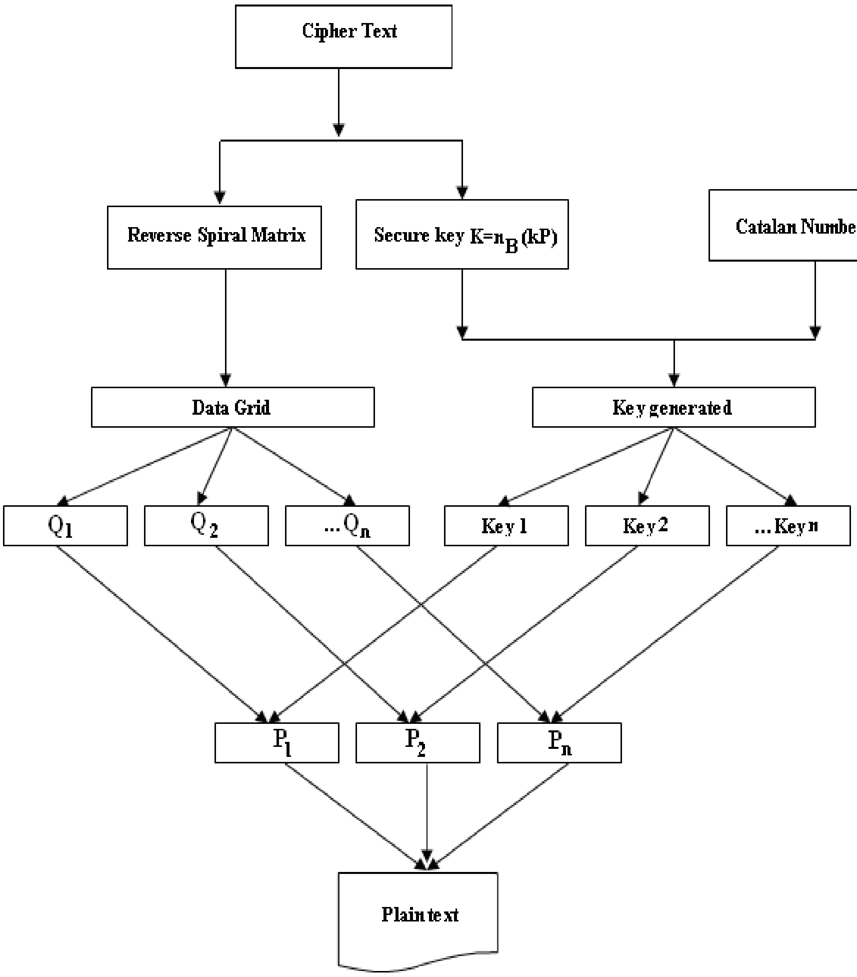

Figure 4: Flowchart – decryption

b. Illustration and Results

Now consider an example to illustrate our technique easily. In our case, the elliptic curve is represented by the Weierstrass equation:

$$y^2=x^3+ 2x+9 \bmod 37.$$

The graph of the function is shown in figure 5.

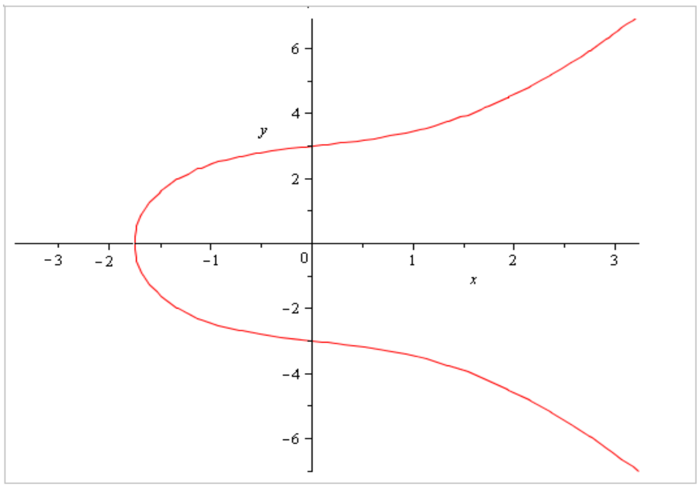

Figure 5. Elliptic curve: $y^2=x^3+ 2x+9$

The points on elliptic curve are:

$$\left\{\begin{array}{l}\propto,(5,25), (1,30), (21,32), (7,25), (25,12), (4,28), (0,34), (16,17), (15,26), (27,32), (9,4),(2,24), (26,5), (33,14),\\ (11,17), (31,22), (13,30), (35,21), (23,7), (10,17), (29,6), (29,31), (10,20), (23,30), (35,16), (13,7), (31,15),\\ (11,20), (33,23), (26,32),(2,13),(9,33), (27,5), (15,11), (16,20), (0,3), (4,9), (25,25), (7,12), (21,5), (1,7), (5,12).\end{array}\right\}$$

The elliptic curve contains 43 points. P is a point generator. It is the point with represents the letter “a”, as well as 2P represents the letter “b”,…, 43P represents space. In our case we use the letters 'a' to 'z', the digits 0 to 9 with some of the other symbols like ';', ',', '.' , '?', ‘(‘,’)’ and space for illustration purpose only.
The base point P is selected as (5, 25).

a. Generation key Phase

Here we take the plain text to be “cryptography” and establish via case study.
We need to generate the secret integer k and compute K=kP$_B$ (with P$_B$ is the public key of the receiver).

Hence we shall assume that n$_B$=13, k=29, P$_B$= (26, 5), K= (27, 5), for instance,

Catalan numbers: 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012, …
Generated points: (27, 5), (10, 20), (0, 3), (9, 33), (27, 32), (26, 5), (27, 32), (0, 1), (26, 5), (1, 7), (0, 3), (25,12).

In our case, the secure key is selected as (27, 5). The point set follows a circular rotation based secure key. The corresponding point which falls below the Catalan number will be taken as a secure key noted K$_i$.

b. Encryption process

Each character of the original message is transformed into an affine point of the elliptic curve. The Table 1 shows the encryption information for embedding of “cryptography” by using Catalan numbers:

Table 1. Encrypted points based Catalan numbers for "cryptography".

Character	Point P$_i$	Secure key K$_i$	Point Q$_i$
c	(21, 32)	(27, 5)	(0, 3)
r	(35, 21)	(10, 20)	(1, 7)
y	(35, 16)	(0, 3)	(35, 21)
p	(31, 22)	(9, 33)	(25, 12)
t	(10, 17)	(27, 32)	(26, 32)
o	(11, 17)	(26, 5)	(11, 20)
g	(0, 34)	(27, 32)	(13, 30)
r	(35, 21)	(0, 1)	(35, 21)
a	(5, 25)	(26, 5)	(33, 14)
p	(31, 22)	(1, 7)	(33, 14)
h	(16, 17)	(0, 3)	(5, 25)
y	(35, 16)	(25, 12)	(26, 32)

The grid can be formed as follows:

0	0	0	0	0	0	0	0	0	0	1	1
0	0	0	0	0	1	0	0	0	1	1	1
1	0	0	0	1	1	0	1	0	1	0	1
0	1	1	0	0	1	0	0	1	1	1	0
0	1	1	0	1	0	1	0	0	0	0	0
0	0	1	0	1	1	0	1	0	1	0	0
0	0	1	1	0	1	0	1	1	1	1	0
1	0	0	0	1	1	0	1	0	1	0	1
1	0	0	0	0	1	0	0	1	1	1	0
1	0	0	0	0	1	0	0	1	1	1	0
0	0	0	1	0	1	0	1	1	0	0	1
0	1	1	0	1	0	1	0	0	0	0	0

Now the spiral matrix rule is applied as follows:

0	0	0	0	0	0	0	0	0	0	1	1
1	1	0	0	0	0	1	0	0	1	0	0
0	0	0	0	1	0	1	0	1	1	0	0
1	1	0	0	0	0	1	0	0	0	0	0
0	0	0	0	1	1	0	1	0	0	1	0
1	1	0	0	1	1	0	1	0	1	0	0
0	0	0	0	0	1	1	0	0	0	1	1
0	1	0	1	1	0	1	1	1	1	1	1
0	0	1	0	0	0	0	0	1	1	1	1
0	0	1	0	0	1	0	0	1	0	1	0
0	1	0	0	0	1	0	0	1	0	1	0
1	1	1	0	1	1	0	1	1	0	0	1

Therefore, the cipher text is,
10000101011100000000000111100010010000001010110011000010000000001101001011001101010000000
01100011010110111111001000001111001001001010010001001010111011011001

c. Decryption process

For decryption process, exactly reverse steps of the encryption process. The decrypted block of length m is generated after taking the bits from the square matrix following the reverse rule of spiral matrix. The decrypted points are formed after taking the bits from all decrypted blocks. Next, the secure key is calculated from the first block with the secure key of the recipient. The secure key generated basing the Catalan numbers and secure key. Then, substruct it from the result point to the original point. Therefore, reverses the embedding to get back the message.

4. RESULT ANALYSIS

A good encryption procedure should be robust against all kinds of cryptanalytic such as brute-force attacks. In this section, security aspects of the present elliptic curve encryption scheme will be discussed. In fact, we analysed with existing algorithms to find out our algorithm performance.

The results include the comparisons of encryption time and decryption time. All times are in milliseconds (ms). Here, the comparative study between TDES, AES and our scheme has done on text files with different sizes (bytes). The Table 2 shows the encryption and decryption time for TDES, AES and our algorithm.

Figure 6 and Figure 7 show the graphical representation of encryption and decryption times against the file size respectively.

Table 2. File size v/s Encryption and Decryption time for .txt files

Source file size (bytes)	Encryption time			Decryption time		
	TDES	AES	Our scheme	TDES	AES	Our scheme
7168	10	2	0	10	2	2
17408	16	13	9	23	12	10
149848	31	30	29	63	31	27
982732	144	78	62	218	63	58

Table 1 shows that the encryption and decryption times increase with the increase of input stream sizes. In fact, the obtained results indicate that for any file, the proposed algorithm takes less time to encrypt and decrypt data than T-DES and takes less or same amount of time compared to AES. Also, our algorithm has other features. The proposed scheme is very straight forward and simple to implement. The key information varies from session to session for any input bit stream which enhances the security features of the proposed technique. Our algorithm is applicable to ensure high security in message transmission and very much comparable TDES and AES in termes of time complexity. Brute force attack on key is also difficult due to the increase in key size.

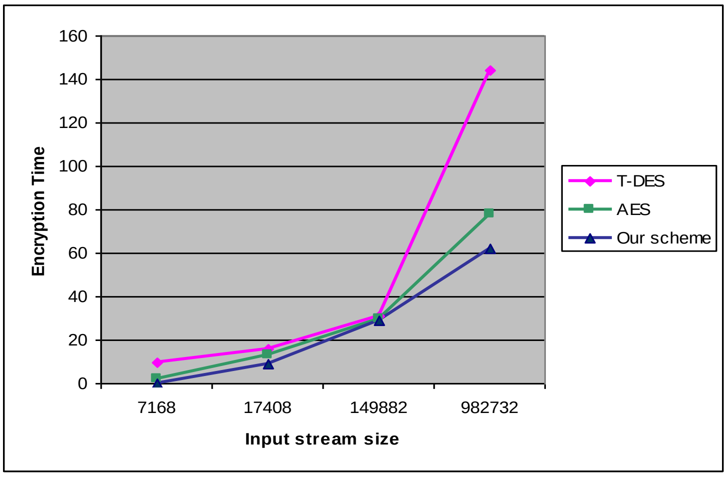

Figure 6. Encryption time for T-DES, AES and our scheme

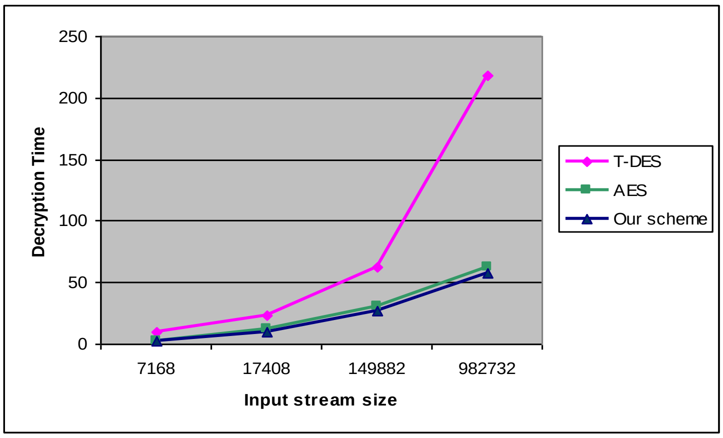

Figure 7. Decryption time for T-DES, AES and our scheme

5. CONCLUSION

In this paper, a novel encryption scheme is introduced by using Catalan numbers. The security of the proposed method is obtained by utilizing the elliptic curve discrete logarithm problem. The algorithm uses the concept of splitting the plaintext and key equally and applies the encryption process. Further, the rule of spiral matrix is applied to the result data matrix to randomize the cipher text. This approach strengthens the cryptosystem. Therefore, the main advantage of this method is higher level of security at relatively low computational overhead. The comparative study realized on the algorithm showed their robustness and their efficiency. Finally, we like to point out that the use of randomization technique will scrambled the cipertext and provide better performance in this regard.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

[1] M. Aydos, T. Yanik, and C. K. Kog, "High-speed implementation of an ECC based wireless authentication protocol on an ARM microprocessor", *IEE Proceeding Communications*, vol. 148, no. 5, pp. 273-279, 2001.

[2] C. J. McIvor, M. McLoone, and J. V. McCanny, "Hardware elliptic curve cryptographic processor over GF (p)", *IEEE Transactions on Circuits and Systems*, vol. 53, no. 9, pp. 1946-1957, 2006.

[3] S. M. C. Vigila and K. Muneeswaran, "Implementation of text based cryptosystem using elliptic curve cryptography", *IEEE International Conference on Advanced Computing*, pp. 82-85, 2009.

[4] J. Lee, H. Kim, Y. Lee, S. M. Hong, and H. Yoon, "Parallelized scalar multiplication on elliptic curves defined over optimal extension field", *International Journal of Network Security*, vol. 4, no. 1, pp.99-106, 2007.

[5] Alter.R, "Some Remarks and Results on Catalan Numbers", *proceedings of Louisiana Conference on Combinatorics*, Graph Theory and computing, 1971.

[6] F.Amounas and E.H. El Kinani, "Fast mapping method based on matrix approach for elliptic curve cryptography", *International Journal of Information & Network Security*, vol.1, No.2, pp. 54-59, 2012.

[7] F.Amounas and E.H. El Kinani, "Elliptic Curve Digital Signature Algorithm Using Boolean Permutation based ECC", *International Journal of Information & Network Security*, vol.1, No.3, pp. 216-222, 2012.

[8] F.Amounas and E.H. El Kinani, "An Efficient Elliptic Curve Cryptography protocol Based on Matrices", *International Journal of Engineering Inventions*, vol 1, Issue 9, pp. 49-54, 2012.

[9] F.Amounas and E.H. El Kinani, "Construction Efficiency of the Elliptic Curve Cryptosystem using Code Computing for Amazigh Alphabet", *International Journal of Information & Network Security*, vol 2, No 1, pp. 43-53, 2013.

[10] F.Amounas and E.H. El Kinani, "A Novel Encryption Scheme of Amazigh Alphabet Based Elliptic Curve using Pauli Spin 1/2 Matrices", *International Journal of Information & Network Security*, vol 2, No 2, pp. 190-196, 2013.

[11] F.Amounas, E.H. El Kinani and H.Sadki, "An Efficient Signcryption Scheme based on the Elliptic Curve Discrete Logarithm Problem", *International Journal of Information & Network Security*, vol 2, No 3, pp. 253-259, 2013.

[12] F.Amounas and E.H. El Kinani, "Proposed Developments of Blind Signature Scheme based on The Elliptic Curve Discrete Logarithm Problem", *Computer Engineering and Applications Journal*, vol 2, No 1, 2013.

[13] "Triple Data Encryption Standard" FIPS PUB 46-3 Federal Information Processing Standards Publication, Reaffirmed, National Institute of Standards and Technology, 1999.

[14] "Advanced Encryption Standard", Federal Information Processing Standards Publication 197, 2001.

[15] N. Koblitz. "Elliptic Curve Cryptosystems". *Mathematics of Computation*, vol. 48, No. 177, pp. 203-209, 1987.

[16] V. S. Miller. "Use of Elliptic Curves in Cryptography", *Advances in Cryptology CRYPTO'85*, pp. 417-426, 1986.

[17] Darrel R. Hankerson, Scott A. Vanstone, and Alfred J. Menezes. "Guide to Elliptic Curve Cryptography". *Springer*, 2004.

BIOGRAPHIES OF AUTHORS

EL HASSAN EL KINANI received the Ph.D in mathematical physics in 1999 from Mohamed V University Rabat Morocco. He is full professor at department of mathematics in Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco. He is interested in classical and quantum cryptography.

E-mail: elkinani_67@yahoo.com

MOHA HAJAR received the Ph.D in mathematical in 1988 from Aix-Marseille II University French. He is full professor at department of mathematics in Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco. He is interested in Mathematics and Computer Sciences.

E-mail: Moha_hajjar@yahoo.fr

FATIMA AMOUNAS received the Ph.D degree in Mathematics, Computer Sciences and their applications in 2013 from Moulay Ismaïl University, Morocco. She is currently an assistance Professor at Computer Sciences department at Faculty of Sciences and Technics, Errachidia, Morocco. Her research interests include elliptic curve and cryptography.

E-mail: F_amounas@yahoo.fr