ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A MULTI-LEVEL APPROACH OF ELLIPTIC CURVE CRYPTOSYSTEM FOR ENHANCED SECURITY OF AMAZIGH ALPHABET USING CELLULAR AUTOMATA

Fatima Amounas

R.O.I Group, Computer Sciences Department, Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco.

ABSTRACT

Securing data is a challenging issue in today's era. Encryption is one of the popular methods to achieve secret communication between sender and receiver. Many different encryption techniques have been proposed to save the security of information. Encryption provides only one level of security during transmission over the channel. Hence there is a need for a stronger encryption which is very hard to break. So, to achieve better results and improve security, information has to pass through several levels of encryption. The aim of this paper would be to provide new approach of elliptic curve cryptosystem using Cellular Automata (CA). The fundamental idea behind this encryption technique is to enhance security using the concept of cellular automata. The results show that the proposed algorithm has a high security feature and it is efficient for encrypting Amazigh alphabet. Practical implementation proved that the proposed encryption algorithm is robust and provides high level of security as compared to existing algorithms.

KEYWORDS: Elliptic curve, Encryption, Compression, Cellular automata, Unicode, Data Matrix.

INTRODUCTION

With the development of computers there has been strong demand for means to protect information and to provide security. Cryptography plays an important role in this field [1]. For ensuring the security, the plain text is converted to cipher text and the process is called encryption. Although this conversion idea is old, the way of encryption should not be vulnerable to attacks. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized users for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security. These methods are also easy to implement but can be cracked easily with the high end technologies. In fact, as security level is increased, the time and complexity of algorithm is also increased and speed and performance of these system is low. This is the major cause of decreasing the speed and efficiency of the encryption system.

Elliptic curve cryptography (ECC) is an effective approach to protect privacy and security of information. ECC was introduced by Victor Miller and Neal Koblitz [2] in 1985.The popularity of elliptic curve cryptography is due to the determination that is based on a harder mathematical problem than other cryptosystems [3]. It is an alternative to the conventional public key cryptosystem such as RSA [4]. ECC offers the same level of security with smaller key size.

In recent years, researchers have given more attention to develop the proposed ECC algorithms and improve their efficiency. In our previous works [5-7], we have proposed cryptographic algorithm for text encryption using elliptic curve. In this paper we attempt to provide an enhanced ECC encryption algorithm based on compression technique with cellular automata. The aim of this work is to develop multi-level encryption system based ECC that can be used to encrypt Unicode characters. Recently, the cryptography with elliptic curve by using the Unicode characters is a newer approach. The Amazigh language is considered as an official language In Morocco only in 2003. With the UTF-8 encoding, Unicode characters can be used. The

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

Amazigh characters are encoded in the Unicode range U+2D30 to U+2D7F. There are 55 defined characters [8]. A code point is the value that a character is given in the Unicode standard. The values according to Unicode are written as hexadecimal numbers and have a prefix "U+". In this paper, a multilevel encryption system has been proposed with the help of cellular automata to encrypt Amazigh characters.

The remaining parts of this paper are developed as follows: Section II gives an overview of the elliptic curve cryptography. The next Section III presents a detailed description of Cellular automata. Section IV is devoted to the proposed approach. Section V presents the simulation and results comparison of the proposed method with existing algorithms. Finally, Section VI concludes the paper.

REVIEW OF ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curves are used for several kinds of cryptosystems, including key exchange protocols and digital signature algorithms. The mathematical background of ECC is more complex and thus it provides greater security and more efficient performance than other public key cryptosystems [9].

An elliptic curve over the field F_p is given by an equation of the form:

$$E: y^2=x^3+ax+b \qquad (1)$$

with a, b in F_p and $4a^3+27b^2 \neq 0$.

The group used for cryptosystem is the group of points on a curve over F_p. With affine coordinates, the points obtain the form (x, y), where x and y are in F_p, and they satisfy the equation of the curve as well as a distinguished point Ω, called the point at infinity[10].

The addition of any two distinct points on the elliptic curve can be conducted using some formulas as shown below:

When $M=(x_1,y_1)$ and $N=(x_2,y_2)$ are not negative of each other, then $M+N=R(x_3, y_3)$.

First step is to find s as the slope of the line through M and N:

$$s=\frac{y_1-y_2}{x_1-x_2}$$

Then

$$\begin{cases} x_3=s^2-x_1-x_2 \\ y_3=-y_1+s(x_1-x_2) \end{cases}$$

The doubling operation for any point in the elliptic curve group requires some steps. For each doubling of the point P, we need the above procedure to obtain 2P,2(2P),2(2(2P)), and so on. It should be noted that to compute kP for any integer k, we need to perform a series of doublings and additions operations.

Assuming we want to double the point $M(x_1,y_1)$ when y_1 is not 0,

2M=R, where

$$s=\frac{3x_1^2+a}{2y_1}$$

$$\begin{cases} x_3=s^2-2x_1 \\ y_3=-y_1+s(x_1-x_3) \end{cases}$$

Point multiplication is achieved by two basic elliptic curve operations as shown in Figure 1. A negative of a point is the reflection of that point with respect to x-axis.

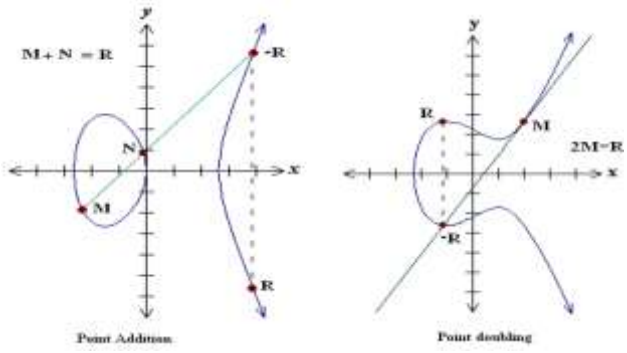


Fig 1. Point multiplication

CELLULAR AUTOMATA

Cellular Automata were originally proposed by John von Neumann as computing model of complex system using simple rule. The structure studied was most on one and two-dimensional infinite grids, through higher dimensions were considered. Cellular Automata are widely of applications like in cryptography, computer graphics, neural network etc. A class of cellular automata (CA) based encryption

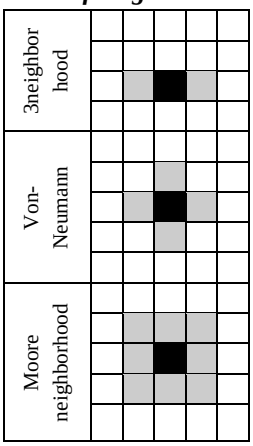
algorithms presents a particular promising approach to cryptography.

Cellular Automata can be represented by the quadruple as, {D, K, N, F} where:

- D defines the dimension of CA may be 1D, 2D, 3D…
- K holds set of possible states of all cells in a Cellular Automata.
- N defines the set of neighborhood states.
- F is Transition Rule.

Cellular Automata (CA) is a collection of cells and each cell change in states by following a local rule that depends on the environment of the cell [11]. The environment of a cell is usually taken to be a small number of neighboring cells. Various neighborhood techniques are exists [12], in that more popularly are shown in Table 1. By applying the transition rule the current state of CA moves to new state by considering the neighborhood states, for more details, see [13].

Table 1. Set of neighborhood states



For example, consider Rule 90, which is given by:

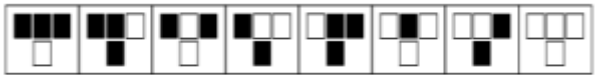


Fig 2. Representation of rule '90'

PROPOSED APPROACH

In this paper, we have imported some innovative advancement to elliptical encryption scheme which is more secure and fast. So we have tried to implement this mechanism with compression technique based on cellular automata to achieve better level of security. The proposed approach combines the advantage of Automata theory and asymmetric encryption based ECC into a total scheme. The overall module design shows the different levels of security used (Figure 3). Encryption and decryption algorithms are described in this section.

Encryption Algorithm

The steps in Encryption Algorithm are as follows:

1. Input a text file "Amazigh.txt" as a secret data into the encryption algorithm.
2. Read source file character by character.
3. Map the alphabetic characters into points on elliptic curve and store them into data matrix M.
4. Perform the scalar multiplication with non-singular matrix A. The result matrix is denoted B.
5. Create compressed block of each element of data matrix.
6. Generate randomly one number k. Then, compute secure key kP_B and take the corresponding code point. The compressed block is denoted C_1.
7. Perform XOR between each block and the secure key.
8. Generate the compressed form of secure key K_2=eP, where e is x-coordinate of K_1.
9. Perform XOR with the result block (step 7).
10. Repeat the step 9 until end of the plaintext.
11. Concatenate kP with the obtained blocks and store the result characters to "Encrypt.txt".

Decryption Algorithm

The steps in Decryption Algorithm are as follows:

1. Input the encrypted file "Encrypt.txt" to the decryption algorithm.
2. Split the data sequence into blocks of length m bits and map it to points on EC.
3. Extract the first block as a point P_1. Then, compute n_BP_1 using addition and doubling operations.
4. Perform XOR between the remaining blocks and the secure key K_2=eP, where e is x-coordinate of K_1.
5. Generate the compressed block of the secure key and perform XOR with the result blocks.
6. Convert the data sequence into points on EC and store them into data matrix B.
7. Compute $M = A^{-1}B$ to obtain a data matrix M with entries are points on EC.
8. Reverse the embedding process to get a plaintext.
9. Store the characters in the file "Decrypt.txt".

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

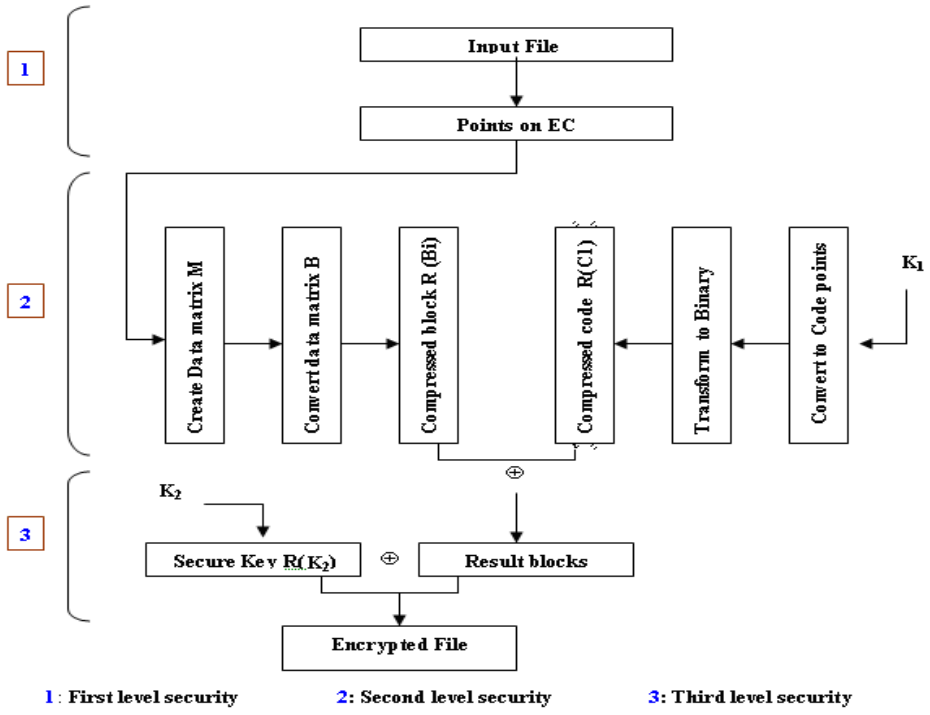


Fig 3. Flow chart of the proposed algorithm

SIMULATION AND RESULTS

In this section, we implement the proposed method using Java Development Kit, for its better GUI features, robustness and platform independent features. The following set of figures shows the encryption and decryption of text files.

Figure 4 shows the original input file to be encrypted with the data (plaintext: Thank you IJESRT…).

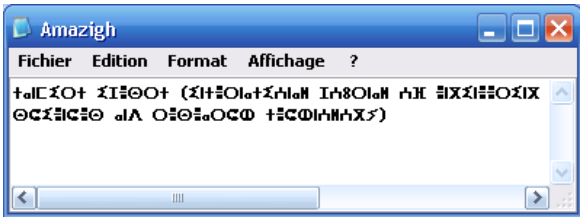


Fig 4: Input original file "Amazigh.txt"

The Figure 5 shows the parameters generated by our system. Parameters panel includes the values related to the elliptic curve that must be initialized in order to be able to perform the encryption/decryption procedure. Then, the following steps are used to generate the keys.

- Generate random number.
- Compute a secure key and create the compressed block using CAR.

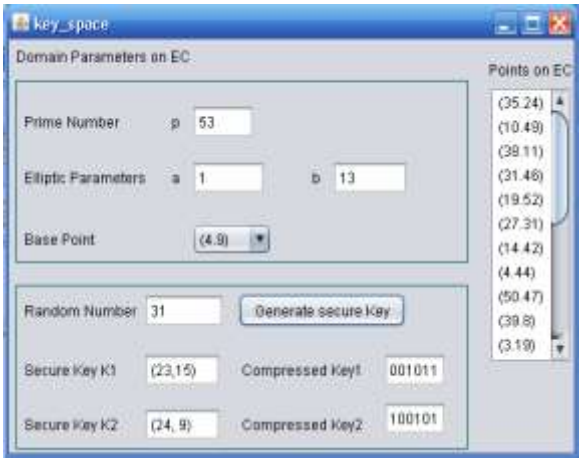


Fig 5: Generation of secure Keys

Figure 6 is a snapshot of the encryption process. The plaintext is encrypted using ECC technique based matrices. After this we reduce length of the obtained blocks using compression technique based on the concept of cellular automata.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

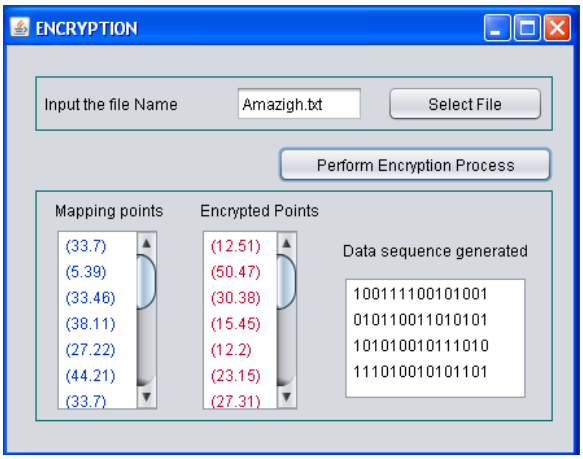


Fig 6: Encryption process

Therefore, the cipher text file generated is given as shown below:

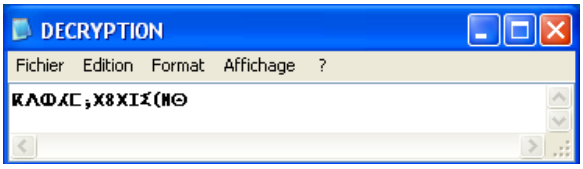


Fig 7: Cipher text "Encrypt.txt"

Figure 8 is a snapshot of the decryption process. The cipher text is decrypted using the reverse process of the encryption technique.

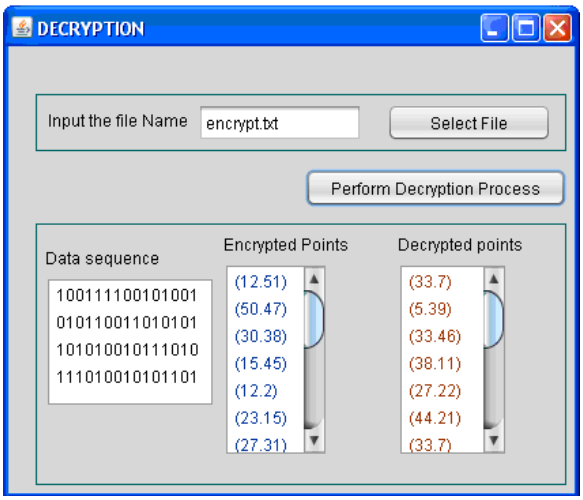


Fig 8: Decryption process

In order to test the performance analysis for any encryption and decryption algorithms, the speed play a major roles [14]. The speed of the algorithm can be characterized by measuring the time required for encryption and decryption. The execution time [15] is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext.

In our analysis, we computed that execution time that covers both encryption and decryption by our proposed algorithm is less as compared to existing encryption systems: AES [16] and "A Block Cipher having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side" [17]. The simulation results are shown in tabular and graphical form respectively.

Table 2. Comparison between proposed method with existing Algorithms in term of Time taken for encryption and decryption

Plaintext size	AES		Alg. [17]		Our scheme	
	Enc	Dec	Enc	Dec	Enc	Dec
20	2,23	2,29	1,98	2,02	1,12	1,72
50	2,56	2,61	2,38	2,37	1,34	1,93
130	3,08	2,98	2,76	2,84	1,85	2,13
240	3,78	3,72	3,62	3,58	2,84	2,86

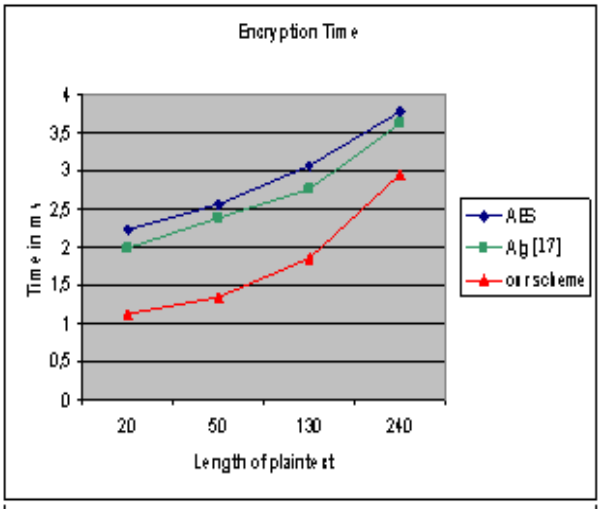


Fig 9: Encryption Time Comparison

According to the graph (Figure 9, Figure 10), it can be clearly seen that our proposed multilevel encryption system using cellular automata takes much less time for encryption and decryption process than the existing encryption algorithms. Hence, it can be used to encrypt any plain text.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

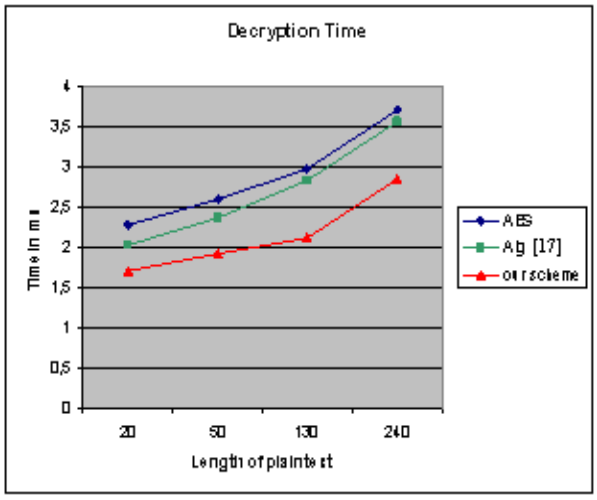


Fig 10: Decryption Time Comparison

CONCLUSION

This paper presented a new multilevel encryption scheme based the concept of cellular automata as a promising approach to elliptic curve cryptography. Although there have been many researchers on the elliptic curve cryptography, but most of the existing algorithms have several weaknesses either caused by low security level or increase the delay time due the design of the algorithm itself. The main scope of this paper is the new level of data security solution with encryption using elliptic curve and Cellular automata. The strength of the algorithm due to the difficulty level used in secure key generated. In fact, Cellular Automata is the strengthen method to generate strong keys. From the results, we analyzed that this enhanced approach can achieve better results as compared to existing encryption algorithms. Therefore, it can be consider as a good alternative to some applications because of the high level of security. In future, experiments should be conducted to implement the algorithm on different applications using Amazigh language to ensure its feasibility and applicability.

REFERENCES

[1] Manoj Kumar Pandey , Deepty Dubey, "Survey Paper: Cryptography The art of hiding Information", International Journal of Advanced Research in Computer Engineering & Technology, Vol. 2, Issue 12, December 2013.

[2] N. Koblitz, "Elliptic curve cryptosystem", Mathematics of Computation 48, pp. 203-209, 1987.

[3] L. C. Washington, "Elliptic Curves: Number Theory and Cryptography", Chapman & Hall/CRC, 2003.

[4] R.L. Rivest, A. Shamir, L.M. Adleman, "A Method for obtaining digital signatures and public key cryptosystem", Communications of the ACM 21, pp.120-126, 1978.

[5] 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.

[6] F.Amounas and E.H. El Kinani, "An efficient elliptic curve cryptography protocol based on matrices, "International Journal of Engineering Inventions, Vol. 1, no. 9, pp. 49-54, 2012.

[7] Fatima Amounas, "Enhanced Elliptic Curve Encryption Approach of Amazigh alphabet with Braille representation", International journal of Computer Science & Network Solutions, Vol. 3, no. 8, pp 1-9, Aug. 2015.

[8] F.Amounas and E.H. El Kinani, "Cryptography with elliptic curve using Tifinagh characters", Journal of Mathematics and System Science 2, pp. 139-144, 2012.

[9] Andrej Dujella "Applications of elliptic curves in public key cryptography" Basque Center for Applied Mathematics and Universidad del Pais Vasco/Euskal Herriko Unibertsitatea, Bilbao, 2011.

[10] D. Hankerson, A. J. Menezes, and S. A. Vanstone, "Guide to elliptic curve cryptography", Springer-Verlag, Berlin, 2003.

[11] P. Sarkar, "A Brief History of Cellular Automata", ACM Computing Surveys, 2000

[12] Petre Anghelescu, Silviu Ionita and Emil Sofron "Block Encryption Using Hybrid Additive Cellular Automata", Seventh International Conference on Hybrid Intelligent Systems, pp. 132- 137, 2007.

[13] Divyashree N P, Sowmya K S, "Design of Stream Cipher for Encryption of Data Using Cellular Automata", International Journal of Innovative Research in Science, Engineering and Technology , Vol. 3, Issue 5, May 2014.

[14] Yan Wang and Ming Hu, "Timing evaluation of the known cryptographic algorithms", International Conference on Computational Intelligence and Security, 2009.

[15] Majdi Al-qdah and Lin Yi Hui, "Simple Encryption/Decryption Application" International Journal of Computer Science and Security, Vol. 1, Issue 1, 2008.

[16] J. Nechvatal, Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000.

[17] V. U. K. Sastry, D. S. R. Murthy and S. Durga Bhavani, "A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side", International Journal of Computer Theory and Engineering, Vol. 2, no. 5, pp. 1793-8201, October 2010.

AUTHOR BIBLIOGRAPHY

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