International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 1 217 - 222

A New Encryption Algorithm to Increase Security of Amazigh Text through Tree Traversal Technique

Fatima Amounas
ROI Group, Computer Science Department,
Moulay Ismaïl University, Faculty of Sciences and
Technics, Errachidia, Morocco.
f_amounas@yahoo.fr

***Abstract*—** In recent years network security has become an important issue. Cryptography is one of the mathematical techniques that ensure secure communications within a non-secure channel. It basically deals with encryption and decryption of a given data. Recently, Elliptic Curve Cryptography (ECC) gained a lot of attention in the field of Cryptography. This paper deals with a new approach to enhance the security of Amazigh text using ECC and tree traversal technique. The Amazigh text is the composition of some character. Every character of the message can be represented as a Unicode value. Depending on the chosen key, the codes point is encrypted and scrambled using tree traversal method. The enhanced approach improved the efficiency of the ECC algorithm. Moreover, the use of tree traversing will provide better performance in this regard.

Keywords- *Elliptic Curve, Encryption, Decryption, tree traversing, Unicode, Tifinagh, Data Matrix.*

*****

I. INTRODUCTION

Elliptic Curve Cryptography (ECC) has been a recent research area in the field of Cryptography. For performing encryption or decryption a series of steps called procedure is required. In encryption, a message is converted into the codes point which is not easy to understand. The key attraction of ECC over RSA is that it offers equal security even for smaller bit size, thus reducing the band width, processing complexity. In ECC, the operations such as point inverse, point addition, point subtraction, scalar multiplication are performed on the points obtained from an elliptic curve. These point operations are useful in performing encryption and decryption operation.

A lot of research has been done in the field of cryptography. There are various encryption algorithms used for secure data transmission[1, 2, 3]. But still new algorithms are emerging because still we require a better technique for data encryption and decryption. ECC has some advantages that make it widely used these days such as small storage capacity, faster computations and reduction of the power consumption[4]. These advantages make ECC is a more suitable to be used in smart cards, wireless communications, portable devices and e-commerce applications. In [5], the author used decimal ASCII value to represent the characters. These characters are transformed into points on the elliptic curve through multiplying their values by a random point on the elliptic curve. An implementation of ElGamal ECC for encryption and decryption a message is also proposed by Debabrat Boruah in [6]. Recently, Graph theory is widely explored, implemented and used to study various applications in the field of cryptography. In [7], the author develops an enhanced version of elliptic curve encryption method using graph theory. In this work, we attempt to enhance the efficiency by providing add-on security to the ECC cryptosystem using tree traversal technique. Here, we attempt to increase the security of Amazigh text using the concept of tree traversing.

The rest of the paper is organized as follows. Section 2 briefly outlines the basic concepts of the binary tree and the elliptic curves cryptosystem. Section 3 describes our contribution and gives our detailed report to this algorithm by utilizing an example. Section 4 deals with the experimental results. Section 5 gives conclusion.

II. BACKGROUND INFORMATION

In this section, we give an overview of certain topics. This will serve as a background and introduction of the concepts which are used in the proposed method.

A. Trees

A tree is an undirected graph in which any two vertices are connected by exactly one path. In fact, a graph is an ordered pair G = (V, E) compromising a set V of vertices or nodes together with a set E of edges or links, which are 2 elements subset of V(that is an edge is related with two vertices, and the relation is represented as an unordered pair of the vertices with respect to the particular edge). Tree is a kind of graph with nodes. A normal tree can contain any number of nodes that are connected in no specific format. A binary tree is a hierarchal data structure and it is a common tree that is used for various practical applications and computational processes. In recent past, Udaya and al [8] have proven that the complete binary tree traversal methods are very useful in converting plain text in to cipher texts. Binary tree is a very important data structure in computer science. In this structure, each node has at most two children, which are referred to as the left child and the right child. In graph we have graph traversal i.e. BFS (Breadth First Search) or DFS

(Depth First Search). Tree traversal method of depth first search is used which is having three methods: In-order, Preorder and Post-order.

1) Tree Traversal

Tree traversal is a form of graph traversal and refers to the process of visiting each node in a tree data structure, exactly once, in a systematic way. Such traversals are classified by the order in which the nodes are visited [9]. Post-order, pre-order and in-order tree traversals are defined in [10]. While post-order and pre-order traversals are defined for all types of trees, in-order traversal is defined only for binary trees. In each of these traversals, the first node visited is assigned 1 as its visit count. For every sub-sequent vertex visited, the visit count is incremented by 1 and is assigned to the vertex. Breadth first search and depth first search are very easy to program either iteratively or recursively. Figure 1 shows graphical representation of traversing methods (BFS, DFS).

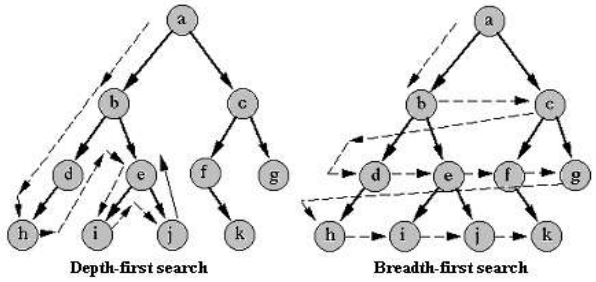

Figure 1. Tree Traversing methods (DFS, BFS).

B. Elliptic Curve Cryptosystem

Elliptic Curve Cryptography(ECC) was introduced by Victor Miller [11] and Neil Koblitz [12] as an alternative to other established public key cryptosystem such as RSA, Elgamal Cryptosystems, etc. The mathematical background of ECC is more complex and thus it provides greater security and more efficient performance than other first generation public key cryptosystems. With elliptic curves one of the main advantage is that the similar level of security can be achieved with considerably shorter keys than in methods based on the difficulties of solving discrete logarithms over integers or integer factorizations.

1) Mathematical operation

An elliptic curve over a finite field is defined by the following equation:

$$E: x^3+ax+b=0 \bmod p \quad (1)$$

By substituting different values for x and y in equation (1), the ECC points are generated. The set of all elliptic curve points is denoted by $E_p(a, b)$ and defined as

$$E_p(a, b)=\{(x,y): y^2=x^3+ax+b \bmod p \}$$

together with the point at infinity. The point at infinity denoted by 'Ω' is the additive identity for the abelian group.

All the entities in the elliptic curve cryptosystem agree upon a, b, p, P, n which are called Domain parameters of ECC. Here P is the base point of the elliptic curve and n is the order of P.

Crypto systems based on elliptic curves over F_p largely utilize the scalar multiplication operation. It is implemented by the repeated addition and doubling strategy of ECC technique [13,14]. Point addition and point doubling are two basic operations performed in scalar multiplication in ECC to implement the points on Elliptic curve.

a) Point addition

To perform addition of two distinct points $P(x_P, y_P)$ and $Q(x_Q, y_Q)$, the following calculation is used. Figure 2 shows graphical representation of point addition.

$$P(x_P, y_P) + Q(x_Q, y_Q)= R(x_R, y_R)$$

$$x_R = (s^2 - x_P - x_Q) \bmod p$$

$$y_R = (s(x_P - x_R) - y_P) \bmod p$$

$$s = \frac{y_Q - y_P}{x_Q - x_P} \bmod p$$

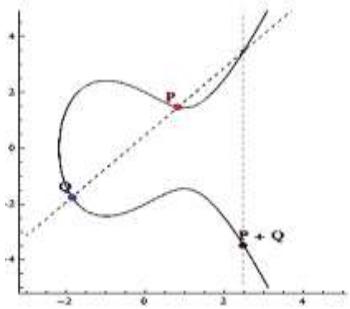

Figure 2. Point addition.

b) Point doubling

Point doubling is performed to add up two points which are same i.e. they have same coordinate value. Figure 3 shows graphical representation of point doubling.

$$P(x_P, y_P) + Q(x_Q, y_Q)= R(x_R, y_R)$$

$$x_R = (s^2 - 2x_P) \bmod p$$

$$y_R = (s(x_P - x_R) - y_P) \bmod p$$

$$s = \frac{2x_1^2 + a}{2y_P} \bmod p$$

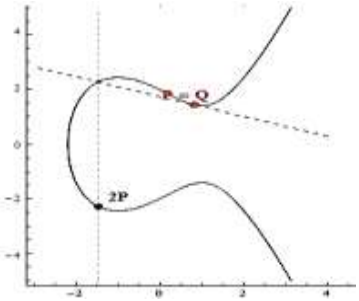

Figure 3. Point doubling.

2) Discrete Logarithm Problem

The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem. Let P and Q be two points on an elliptic curve such that $\lambda P = Q$, where λ is a scalar. Given P and Q, it is computationally infeasible to obtain λ, if λ is sufficiently large. λ is the discrete logarithm of Q to the base P. Hence the main operation involved in ECC is point multiplication. i.e. multiplication of a scalar λ with any point P on the curve to obtain another point Q on the curve.

C. Amazigh Language

Amazigh language is a branch of the Afro-Asiatic (Hamito-Semitic) languages [15]. It is spoken over the Northern part of Africa which extends from the Red Sea to the Canary Isles and from Niger in the Sahara to the Mediterranean Sea. In Morocco, according to the geographic area, there are three main varieties of Amazigh: Tarifit in the North, Tamazight in the Center, and Tashelhit in the South. The Amazigh language has its own writing that was adapted by IRCAM in 2003, to provide an adequate and usable standard alphabetic system, called Tifinaghe-IRCAM. With the UTF-8 encoding, Unicode characters can be used [16, 17]. The table 1 presents the Amazigh characters and the associated Unicode allocated by ISO.

Table 1. Encoding of Amazigh characters.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
U+2D3x	ⴰ	ⴱ	ⴲ	ⴳ	ⴴ	ⴵ	ⴶ	ⴷ	ⴸ	ⴹ	ⴺ	ⴻ	ⴼ	ⴽ	ⴾ	ⴿ
U+2D4x	ⵀ	ⵁ	ⵂ	ⵃ	ⵄ	ⵅ	ⵆ	ⵇ	ⵈ	ⵉ	ⵊ	ⵋ	ⵌ	ⵍ	ⵎ	ⵏ
U+2D5x	ⵐ	ⵑ	ⵒ	ⵓ	ⵔ	ⵕ	ⵖ	ⵗ	ⵘ	ⵙ	ⵚ	ⵛ	ⵜ	ⵝ	ⵞ	ⵟ
U+2D6x	ⵠ	ⵡ	ⵢ	ⵣ	ⵤ	ⵥ										ⵯ
U+2D7x																

III. MAIN RESULT

Structural approach is the most recently used approach for protecting text documents [18, 19]. In this the structure is extended to enhance the security of Amazigh text. The basic idea behind this is that all nodes are represented by points on elliptic curve. In this technique, the root is always associated with the point on EC. For achieving efficiency in the elliptic cryptosystem, we have involved the tree traversal methods to generate the cipher text. This mechanism is more secure, robust and fast than ECC mechanism. So we have tried to implement this mechanism with the concept of tree-traversal to achieve better security enhancement.

A. Key generation

If two communicating parties Alice and Bob want to communicate the messages then they agree upon to use an elliptic curve $E_p(a,b)$ where p is a prime number and a random point P on the elliptic curve[20].

Alice's (or Bob's) public and private keys are associated with a particular set of elliptic key domain parameters [21, 22].

Alice and bob generate the public and private keys as follows:

Alice: - Select a random number n_A , $n_A \in [1, n-1]$
- Compute $P_A = n_A P$.

Bob: - Select a random number n_B , $n_B \in [1, n-1]$
- Compute $P_B = n_B P$.

Alice's public key is P_A and private key is n_A.

Bob's public key is P_B and private key is n_B.

B. Development of Algorithm

The algorithm for the proposed encryption and decryption architecture in figure 4 can be used for various applications.

- *Encryption process*

The encryption algorithm is given below:

Step 1. Input any sentence Amazigh as plain text message.
Step 2. Split the input message into number of block of data with specified size and convert it into codes points.
Step 3. Imbed each value into points on elliptic curve and store the mapping points into data matrix PM.
Step 4. Choose a random number k and compute the point kP_B. Then, construct the key matrix KP with the specified size.
Step 5. Perform the encryption using ECC technique based matrices approach. The result matrix is denoted PC.
Step 6. Insert the resultant values in the binary tree as proposed and apply tree traversal technique to scramble the encrypted data.
Step 7. Pack out two pair of bit stream of data sequence ($b_i b_j$) one by one to decide which traversing method has to be performed:

'00'	'10'	'01'	'11'
↓	↓	↓	↓
BFS	DFS1	DFS2	DFS3

Step 8. Perform the respective operations as proposed to the remaining blocks.
Step 9. Send the result message to the receiver.

- *Decryption process*

To decrypt the cipher text, Bob does the following:

Step 1. Get the Encrypted message.
Step 2. Split the message into number of block of data with specified size.
Step 3. Imbed each block into points on elliptic curve and extract the first point kP.
Step 4. Compute the secure key $K=n_BP_1$ and generate the key matrix KP with the specified size.
Step 5. Insert the encrypted points in the binary tree as proposed.
Step 6. Apply the reversible process of tree traversal technique and store the mapping points into data matrix.
Step 7. Perform the respective operations as proposed to the remaining blocks.
Step 8. Perform the decryption using ECC technique based key matrix.
Step 9. Reverse the embedding to get back the original message.

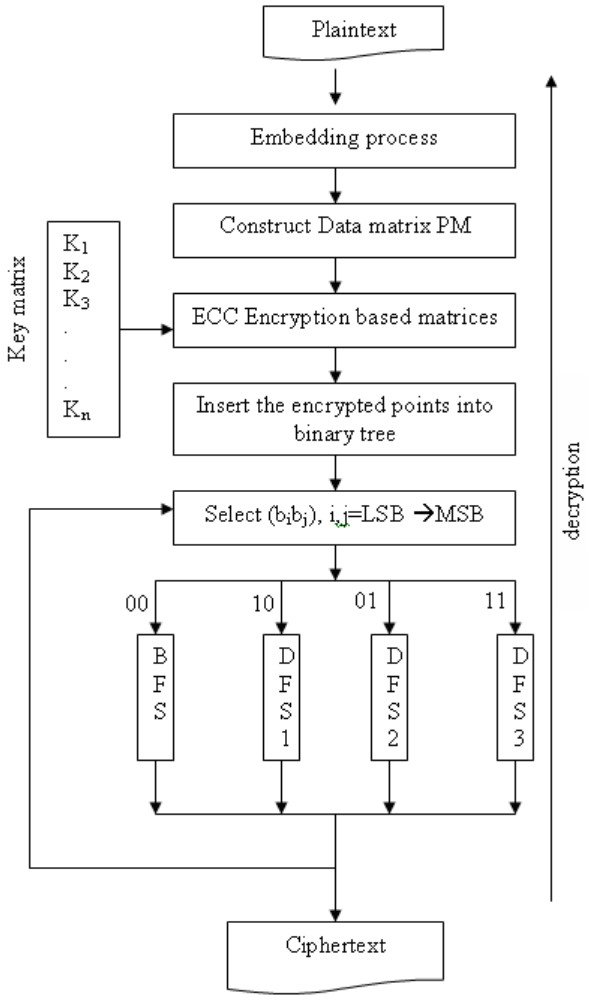

Figure 4. Flowchart of the proposed Algorithm.

C. *Illustration with Example*

In order to show the implementation steps clearly, both the sender and the receiver decide on a simple elliptic curve E_{241} (-1, 188) that is represented by:

$$y^2 = x^3 - x + 188 \bmod 241.$$

The points of the elliptic curve E_{241}(-1 ,188) are shown below:

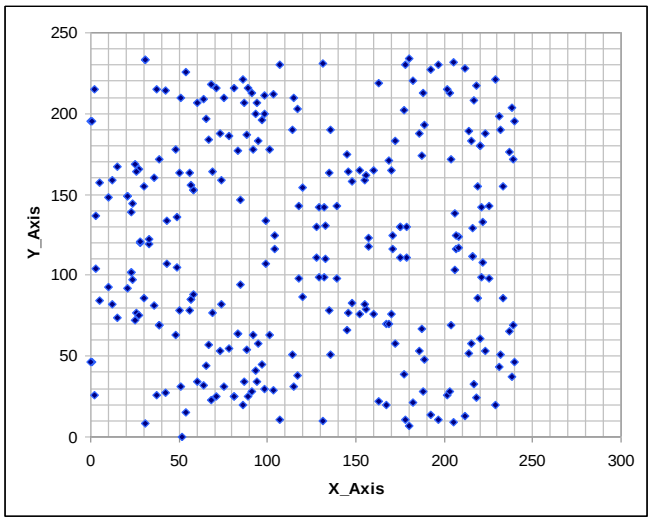

Figure 5. The set of points on elliptic curve E_{241}(-1 ,188).

Let the point (1, 46) be chosen as the base point P and K=(169,70) as a secure key.

If Alice wants to send the message '[illegible]" to Bob, he should first convert each character in the message into the points on elliptic curve. Let us discuss clearly about encryption mechanism.

First, we imbed the plaintext into points on elliptic curve as shown below:

$$PM = \begin{pmatrix} (188,213) & (132, 99) & (139,143) & (156,79) \\ (120,87) & (37, 215) & (49, 136) & (65, 197) \\ (192,14) & (27,166) & (219, 86) & (95,58) \\ (155,82) & (212,13) & (12,159) & (58,153) \end{pmatrix}$$

Here, we construct the key matrix as follow:

$$KP = \begin{pmatrix} (21,149) & (216,112) & (39, 69) & (57, 85) \\ (189,193) & (232,190) & (225,143) & (206,103) \\ (212,228) & (128,130) & (202,26) & (219,86) \\ (74,159) & (157,118) & (203,213) & (172,58) \end{pmatrix}$$

Next, by applying ECC encryption algorithm we get:

$$
CP=\begin{pmatrix} (120,154) & (229,20) & (237,65) & (37,215) \\ (133,110) & (12, 82) & (15,167) & (73,188) \\ (172,183) & (27,166) & (197,11) & (89,216) \\ (91,216) & (156,162) & (115,210) & (139,98) \end{pmatrix}
$$

After applying traversing methods, we get:
(15,167),(120,154),(115,210),(197,11), (27,166), (156,162), (89,216), (139,98), (133,110), (91,216), (12, 82), (229,20), (73,188), (237,65), (37,215), (172,183)

Therefore, the cipher text to be sent is:

"ⵅⵍⵅⵅⴽⵉⵚⵍⴷⵜⵍⵍⵙⴷⴻⵛ"

At the receiver side, we reverse the process to retrieve the original message. Firstly reverse the traversing process and decrypt cipher points to original points using key matrix. Then it is converted to Unicode character to get back the original message.

IV. SIMULATION AND RESULTS

This section demonstrates the proposed algorithm in practical aspect using Netbeans 7.1. It is observed that the algorithm is successfully working, it could able to encrypt and decrypt the plaintext of any Unicode character. To prove that it is working well we have considered plaintext as a collection of Amazigh sentences from the book "Le Petit Prince". This book has been translated in Amazigh language by Lahbib Fouad, a researcher at the Royal Institute of Amazigh Culture (IRCAM). The user interface of the application is illustrated in Figure 6.

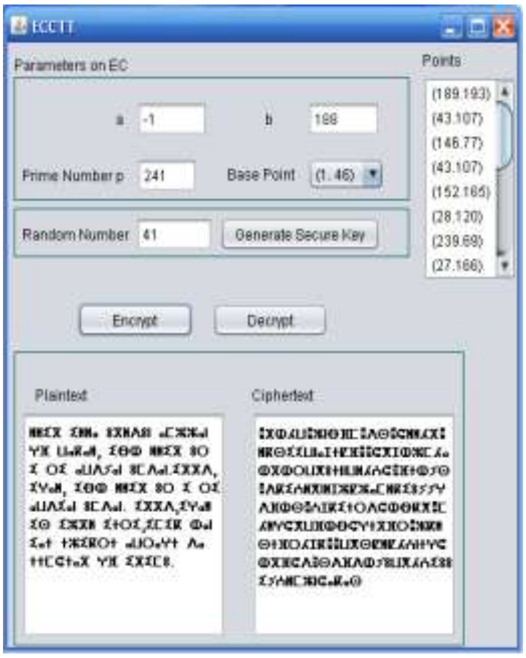

Figure 6. A Screen Shot of Encryption/Decryption process.

To encrypt a plaintext message, the user chooses EC parameters and generates the set of points on EC. Next, the user generates the code operations to be performed. After that, the user input the text to be encrypted and the "Encrypt" button is clicked to perform the encryption algorithm as shown in Figure 6. Subsequently the encryption algorithm is implemented on the original message and the cipher text is generated.

Similar is the procedure to decrypt the encrypted message. To decrypt the cipher text, the "Decrypt" button is clicked to perform the decryption algorithm. A result message so generated is similar to the original text.

Finally, the propose paper concepts shows efficient results and has been efficiently tested on text Amazigh. Further, the proposed algorithm is faster than the previously known results. Our approach reduces lower complexity which contributes to an efficient implementation of elliptic curve cryptosystems. The strength of the any algorithm depends on key rather then the algorithm, in this we generate a set of keys randomness to perform tree traversing and proven that it is far from crypt analysis attacks.

V. CONCLUSION

In this paper we have developed a novel approach to enhance the security of ECC cryptosystem with tree traversing technique. In this we have used two types of tree traversing methods to improve the complexity. We have proven that it can encrypt/decrypt Amazigh characters secretly and it can be extended to encrypt any Unicode characters. It should also be mentioned that the enhanced cryptosystem over elliptic curve is suitable to be implemented on many small devices (e.g. smart card). This enhanced version performs better enhancement to elliptic curve cryptosystems which are considered newly in cryptography and is one of the most researched topic in cryptography.

REFERENCES

[1] Kefa Rabah "Elliptic Curve Cryptography over Binary Finite Field GF(2^m)". Information Technology Journal 5(1) pp. 204-229, ISSN 1812-5638, 2006.

[2] Lv H, Li H, Yi J, Lu H. "Optimal implementation of elliptic curve cryptography". IEEE International Conference on Service Operations and Logistics and Informatics; Dongguan, Guangdong, China, pp. 28-30, 2013.

[3] V.Kamalakannana and S.Tamilselvan, " Security Enhancement of Text Message Based on Matrix Approach Using Elliptical Curve Cryptosystem", 2nd International Conference on Nanomaterials and Technologies, Procedia Materials Science 10, pp. 489-496, 2015.

[4] Sagheer AM. "Elliptic curves cryptographic techniques". Proceeding of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS'2012), Gold Coast, Australia: IEEE, 2012.

[5] Vigila SMC, Muneeswaran K. "A new elliptic curve cryptosystem for securing sensitive data applications". International Journal of Electronic Security and Digital Forensics, 5(1), pp. 11-24, 2013.

[6] Boruah D, Saikia M. "Implementation of ElGamal Elliptic Curve Cryptography over prime field using C". IEEE International Conference on Information Communication and Embedded Systems (ICICES); 2014.

[7] Fatima Amounas, "On enhancement of Elliptic Curve Encryption of Amazigh Text using Graph Theory", International journal of Computer Science & Network Solutions, Vol. 4, No.3, pp. 1-10, 2016.

[8] Ravindra Babu, Udaya Kumar and Vinaya Babu, "A Block Cipher Generation Using an Innovative Permutation Algorithm", Communicated to International Journal of Mathematical Archive, 3(4), pp. 1443-1447, 2012.

[9] Yedidyah Langsam, Moshe J. Augenstein, M.Tenebaum, "Data Structures using C and C++", 2nd Edition , 249-319, ISBN-81-203-1177-9, 2000.

[10] Fatima Amounas, "An Efficient Approach for Enhancing the Security of Amazigh Text using Binary Tree", International Journal of Computer Applications Technology and Research, Volume 5- Issue 9, pp. 578-583, 2016.

[11] N. Koblitz. "Elliptic curve cryptosystems". Mathematics of Computation, 48:203-209, 1987.

[12] Miller VS. "Use of elliptic curves in cryptography". Advances in Cryptology. Proceedings of Crypto85. Lecture note in Computer Science. Berlin, Heidelberg: Springer-Verlag. p. 417-26, 1986.

[13] Hitesh Kag and Ruchi Telang Gode, "Matrix based Efficient ECC Technique for Text Encryption", Proceedings of 7th IRF International Conference, 27th pp. 107-117, April-2014.

[14] Vigila S, Muneeswaran K. "Implementation of text based cryptosystem using elliptic curve cryptography". IEEE Proceedings of Advanced Computing Conference, 2009.

[15] Ouakrim, O. "Fonética y fonología del Bereber ". Survey at the University of Autonoma de Barcelona, 1995.

[16] F. Amounas and E.H. El Kinani, "Cryptography with Elliptic Curve using Tifinagh Characters", Journal of Mathematics and System Science 2, pp.1-6, 2012.

[17] Jaafar EL Bakkali, EL Mehdi Stouti and Tarek EL Bardouni, "Design and Implementation of an Android SMS Virtual Keyboard for the Berber Language", I.J. Education and Management Engineering, 1, pp. 1-7, 2015.

[18] Manmeet Kaur and Kamna Mahajan, "An Existential Review on Text Watermarking Techniques", International Journal of Computer Applications, Vol 120, No.18, pp. 29-32, 2015.

[19] G. Sherlin Shobitha and K. Kishore Kumar, "Implementation of CAVLD Architecture Using Binary Tree Structures and Data Hiding for H.264/AVC Using CAVLC & Exp-Golomb Codeword Substitution", International Journal of Computer Science and Mobile Computing, Vol.5, Issue.3, pp. 540-549, 2016.

[20] Hankerson D, Menezes A, Vanstone S. "Guide to elliptic curve cryptography". New York: Springer Science and Business Media, 2004.

[21] Hofstein J, Pipher JC and Silverman JH. "An Introduction to Mathematical Cryptography". New York: Springer pp. 299–371, 2014.

[22] Ali, M, Sagheer, "Enhancement of elliptic curves cryptography methods", MSc. Thesis, University of Technology, Baghdad, Iraq, 2004.