International Journal of Computer Applications Technology and Research
Volume 5– Issue 9, 578 - 583, 2016, ISSN:- 2319–8656

An Efficient Approach for Enhancing the Security of Amazigh Text using Binary Tree

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

Abstract: Now a day's Cryptography is one of the broad areas for researchers. Due to its importance, several cryptography techniques are adopted by many authors to secure the data, but still there is a scope to improve the previous approaches. The main of our research is to develop a novel Approach for enhancing the security of Amazigh Text using binary tree. The plaintext considered is the combination of Unicode characters. This paper contributes in the area of elliptic curve cryptography by encrypting data using matrix approach and using the concept of tree traversal method for enhancing the security of the encrypted points. The security goals were enhanced by making it difficult for attacker to predicate a pattern as well as speed of the encryption/decryption scheme. The results show strength of the algorithm.

Keywords: Elliptic Curve Cryptography, Binary Tree, In-order, Pre-order, Post-order, Unicode, Amazigh Alphabet.

1. INTRODUCTION

Cryptography is the science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. Security is a big concern and securing crucial data is very essential, so that the data cannot be change or misused for any illegal purposes. For ensuring the security, the plain text is converted to cipher text by the sender. This process is called encryption. Decryption is exactly reverse process of encryption by which intended user can decode the message to its original form.

Elliptic Curve Cryptography (ECC) is one of the most efficient techniques that are used for ensuring the security, because it is difficult for the adversary to solve the elliptic curve discrete logarithm problem to know the secret key that is used in encryption and decryption processes.

Now a day's Different mathematical schemes and algorithms are there to scuttle the content of the message using ECC technique. Many scientists were doing research on the existing methods to make more strong and unbreakable ciphers by enhancing them [1, 2, 3]. In this paper, an enhanced approach to secure Amazigh text is introduced which is based on binary structure, so that it will more secure and protect the confidentiality and integrity of the information being transmitted. From the literature, the tree is considered as a non linear data structure mainly used to represent the hierarchical relationship between data [4]. Recently, it play a vital role in compiler constructions, operating systems and others system software's.

There are two types of trees: General trees and Binary trees. A general tree is a finite non empty set of nodes and can contain any number of nodes. A binary tree is a finite set of elements that is either empty or is partitioned into three disjoint subsets. The first one contains a single element called the root of the tree. The other two subsets themselves are binary trees called the left sub tree and right sub tree. A binary tree is very useful data structure when two way decisions must be made at each point in a process. This structure is used in our proposed encryption algorithm for enhancing the security and the detailed explanation is presented in section 3.

2. BACKGROUND INFORMATION

In this section we provide some basic details required in the proposed method.

2.1 Binary Trees

A binary tree is a hierarchal data structure and it is a common tree that is used for various practical applications and computational processes. Binary trees are a type of data structures that contain nodes with information attached to these nodes.

The information can be processed in any way such that the nodes in the tree can be traversed from top to bottom or from left to right or right to left or bottom to top or any other possible ways. The nodes in the binary tree can be navigated in many different ways. One such possible way is taken and an encryption and decryption algorithm is proposed using the nodes of these binary trees. A binary tree is a tree where every node has at most degree as 2 and levels are labeled along with the name of the nodes such as leaf nodes and child nodes. Elements can be inserted in the nodes of a binary tree and they can be traversed from one node to another node.

Binary search trees are used for searching elements in binary tree through traversing in different possible ways possible. The root node is distinguished from every other node in a binary tree and all the nodes can be reached from the root node by traversing from the root node. Tree is a restricted form of graph and it does not contain cycles and it comes under the category of acyclic graphs in graph theory and applications.

Tree traversal (also known as tree search) is a form of graph traversal and refers to the process of visiting (checking and/or updating) each node in a tree data structure, exactly once [5, 6]. Trees can be traversed in pre-order, in-order, or post-order.

- *Pre Order Traversal*

In pre-order traversal:

1. Display the data part of the root (or current node).
2. Traverse the left sub tree by recursively calling the pre-order function.
3. Traverse the right sub tree by recursively calling the pre-order function.

Pre-Order Algorithm:

```
preorder(node)
{
if (node = null)
    return;
else
    visit (node)
    preorder (node.left)
    preorder (node.right)
}
```

- *InOrder Traversal*

In In-order traversal:

1. Traverse the left sub tree by recursively calling the In-order function
2. Display the data part of the root (or current node).
3. Traverse the right sub tree by recursively calling the In-order function.

In-Order Algorithm:

```
Inorder(node)
{
if (node = null)
    return;
else
    Inorder (node.left)
    visit (node)
    Inorder (node.right)
}
```

- *Post Order Traversal*

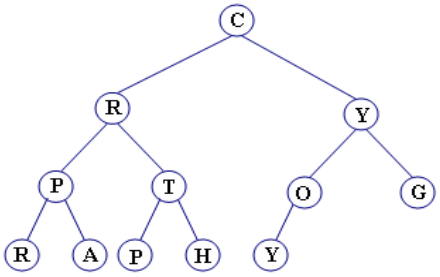
In post order traversal:

1. Traverse the left sub tree by recursively calling the post-order function.
2. Traverse the right sub tree by recursively calling the post-order function.
3. Display the data part of the root (or current node).

Post-Order Algorithm:

```
postorder(node)
{
if (node = null)
    return;
else
    postorder (node.left)
    postorder (node.right)
    visit (node)
}
```

Example: By applying the tree traversal techniques the result is as shown below:



Plaintext: CRYPTOGRAPHY

Inorder: RPARPTHCYOYG

Preorder: CRPRATPHYOYG

Postorder: RAPPHTRYOGYC

2.2 Elliptic Curve

An Elliptic Curve E consists of the set of points (X , Y , Z) that satisfy the following homogeneous Weierstrass equation:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Where a_i (i=1, 2, 3, 4, 5, 6) are elements of a finite field [7] and with the exception that the triple (0, 0, 0) is not a point on E.

If we set Z= 0 and substitute $x = X / Z$, $y = Y / Z$ then we get the equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 .$$

The above equation is called the affine Weierstrass equation. If a point P satisfy the homogeneous Weierstrass equation and the equation:

$$\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = \frac{\partial F}{\partial Z} = 0$$

Then we call that point singular and we call the Weierstrass equation also singular, note that singular Weierstrass equations are not of interest in the cryptography [8].

We need now criteria that can help us to determine if a given affine Weierstrass equation singular is or not. The discriminate Δ (field element) is such a tool, which can be defined as follow:

$$d_2 = a_1^2 + 4a_2$$

$$d_4 = 2a_4 + a_1 a_3$$

$$d_6 = a_3^2$$

$$d_8 = a_1^2 a_5 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

$$c_4 = d_2^2 - 24\, d_4$$

$$\Delta = -d_2^2 - 8d_4^3 - 27\, d_6^2 + 9 d_2 d_4 d_6$$

$$j(E) = c_4^3 / \Delta$$

If Δ =0, then affine Weierstrass equation is singular, otherwise not singular [9]. We call j(E) the j-invariant of the elliptic curve E. Note that only elliptic curves E over finite fields are of interest in cryptography [10].

The definition of group of points over elliptic curve E:

1. There is a point $\Omega \in E$, such that for all $P \in E$, $P + \Omega = \Omega + P = P$, (the identity of the group).
2. If $P \neq \Omega$ and $P=(x_1, y_1)$ then -P is $(x_1, -y_1 - a_1 x_1 - a_3)$.
3. If two points on E have same x-coordinate then either P=Q or P=-Q.
4. If Q = -P, then P + Q = Ω.
5. For two points $P \neq \Omega$ and $Q \neq \Omega$ on E, the addition is defined as follows. Draw the line through P and Q to intersect the curve in a third point; then reflect that point in the x-axis.
6. For two points $P \neq \Omega$ and $Q \neq \Omega$ on E, if P = Q, use the tangent line at P. The identity of the group is Ω, the "point at infinity", which conceptually lies at the top and bottom of every vertical line.

The following figure shows the addition of two points over the elliptic curve E:

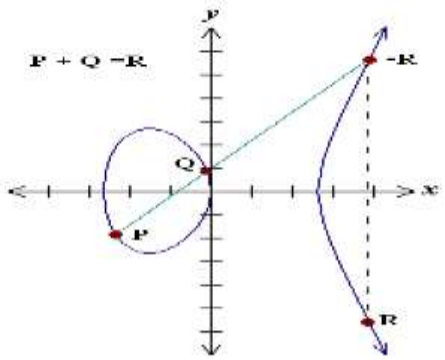


Figure 1. Addition of two points over elliptic curve E.

The discrete logarithm problem over the elliptic curve E is the following: given two points P and Q in a group that satisfy E, find a number α such that $\alpha P = Q$, α is called the discrete logarithm of Q to the base P.

For more information about elliptic curves in cryptography see [11, 12, 13].

2.3 Amazigh Language

In Morocco, Amazigh language is used by tens of millions of people mainly for oral communication, and has been introduced in mass media and in the educational system. Due to its complex morphology as well as to the use of the different dialects: Tarifit in the North, Tamazight in the center and Tashlhit in the southern parts of the country in its standardization, the Amazigh language presents interesting challenges for many researchers [14, 15, 16].

The official graphic system for writing Amazigh is Tifinagh. It does not have capitalization in its script and it is written from left to right. IRCAM uses 33 characters (consisting of: 27 consonants, 2 semi-consonants and 4 vowels). The Figure 2 represents the repertoire of Tifinagh which is recognized and used in Morocco. The total numbers of Tifinagh letters are occupying 2D30-2D7F plage in Unicode. There are 55 defined characters [17].

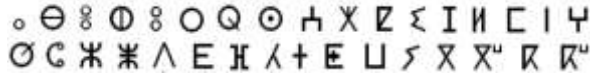


Figure 2. Tifinagh characters adopted by IRCAM.

3. Proposed Approach

The proposed algorithm is an attempt to present a new approach for enhancing the security of Amazigh text based on binary tree in such a way that the new approach can make use of tree traversal method to achieve higher level of security. Let $E_p(a,b)$ be the set of all elliptic curve points over finite field GF(p) corresponding to the defined curve, here $E_p(a,b)$ and the base point P are publicly known [18]. Suppose Alice wants to send a plaintext message to Bob aver an insecure channel, the procedure is as follows:

3.1 Encryption Process

1. Take any sentence Amazigh as input of the algorithm and imbed the given string into respective mapping points on elliptic curve.

2. Convert the given sequence into a data matrix with entries in elliptic curve, called M.

$$\{P_1(x_1,y_1), P_2(x_2,y_2), P_3(x_3,y_3), \ldots, P_n(x_n,y_n)\}$$

$$\Downarrow$$

$$M = \begin{pmatrix} P_1 & P_2 & P_3 & \ldots & P_r \\ P_{r+1} & P_{r+2} & P_{r+3} & \ldots & P_s \\ P_{s+1} & P_{s+2} & P_{s+3} & \ldots & P_t \\ P_{s+1} & P_{s+2} & P_{s+3} & \ldots & P_n \end{pmatrix}$$

Here r=n/4 and s=n/2 and t=3n/4.

If n isn't divided by 4, the points have padded with $\propto$ in order to fill the entries of the matrix M.

3. Construct a key matrix of the same order as the order of the matrix M. The key matrix is denoted K.

4. Multiply the key matrix with the data matrix Q= K×M and insert the resultant values in the binary tree as proposed.

5. Construct a random complete binary tree with total number of nodes n=length (string). Label the nodes starting from the root node in that order as seen in Figure 3.

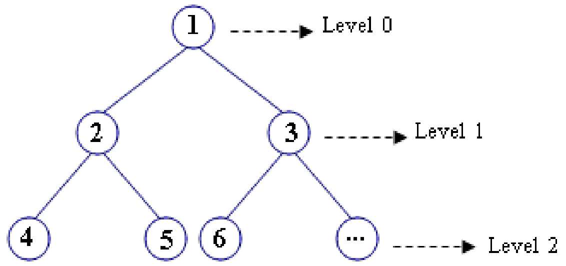


Figure 3. A Complete Binary Tree with two levels

6. Choose a random number integer k and compute a secure key $k_1=kP_B$.

7. Let b= $(b_jb_{j+1}b_{j+2})$, where j is bit position (LSB→MSB), which decides which traversal method, has to be performed on binary tree.

8. Select the tree traversal method based on the selected digit in the key. Divide the decimal number by 3 and keeps track of the remainder.

If the number is 0 ➔ Pre-order, 1 ➔ In-order and

2 ➔ Post -order.

9. Determine the result of the selected traversal method of the complete binary tree.

10. Insert the resultant values in the binary tree as proposed. Repeat steps 7 to 9 for m times.

11. Send the result cipher text (kP, C_j) to the receiver.

3.2 Decryption Process

Decryption is done by reversing the procedure.

1. Determine the alphabetical representation of the received message and extract kP.
2. Compute $k_1= n_B(kP)$ with n_B is his own private key.
3. Processing the reverse process the various steps and constructs the complete binary tree.
4. Convert each node into point on elliptic curve and insert them in the data matrix, called Q.
5. Compute M = $K^{-1}Q$ to obtain the mapping points.
6. Reverse the embedding to recover the plaintext.

4. RESULTS AND DISCUSSION

4.1 Illustration with an example

Let the message to be encrypted be:

"[illegible]"

That means:

"The teacher distributed books to students at the school."

Consider a non-singular elliptic curve defined as follows:

$$y^2=x^3-x+19 \bmod 71.$$

The points on the elliptic curve over $E_{71}(-1, 19)$ are shown below in Figure 4.

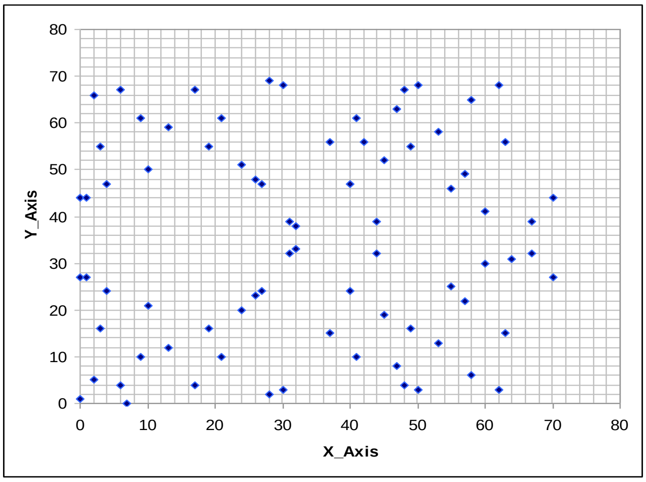


Figure 4. The elliptic curve E_{71} (-1, 19)

The base point P is chosen as (1, 27). Assume that Alice wants to send the above message to Bob. The initial mapped points are given as:

P_i={(17,4) (21,10) (47,8) (63,15) (24,20) (41,10) (3,16) (13,12) (55,25) (63,15) (47,8) (24,20) (17,4) (47,8) (13,12) (17,4) (3,16) (9,10) (24,20) (58,6) (9,61) (24,20) (17,4) (9,10) (13,12) (55,25) (63,15) (47,8) (9,10) (24,20) (26,23) (24,20) (44,32) (17,4) (9,10) (55,25) (13,12)}

These points can be written as a 4×9 matrix denoted M.

The random nonsingular matrix K is chosen as:

$$K=\begin{pmatrix} 2 & 0 & 4 & 3 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 0 & 2 & 2 \end{pmatrix}$$

The above set of points is converted into the following Cipher-text through the data matrix approach:

Q_i={(6,67) (10,50) (57,22) (37,15) (60,30) (17,67) (42,15) (67,32) (21,10) (19,55) (41,10) (62,3) (3,55) (13,59) (26,23) (58,6) (70,44) (67,39) (48,67) (44,32) (53,58) (49,16) (17,67) (24,51) (3,16) (1,44) (67,32) (45,52) (49,16) (47,8) (21,10) (53,13) (27,24) (3,55) (42,15) (30,68) (60,30) (37,15) (26,48) (41,10) (17,67) (31,32)}

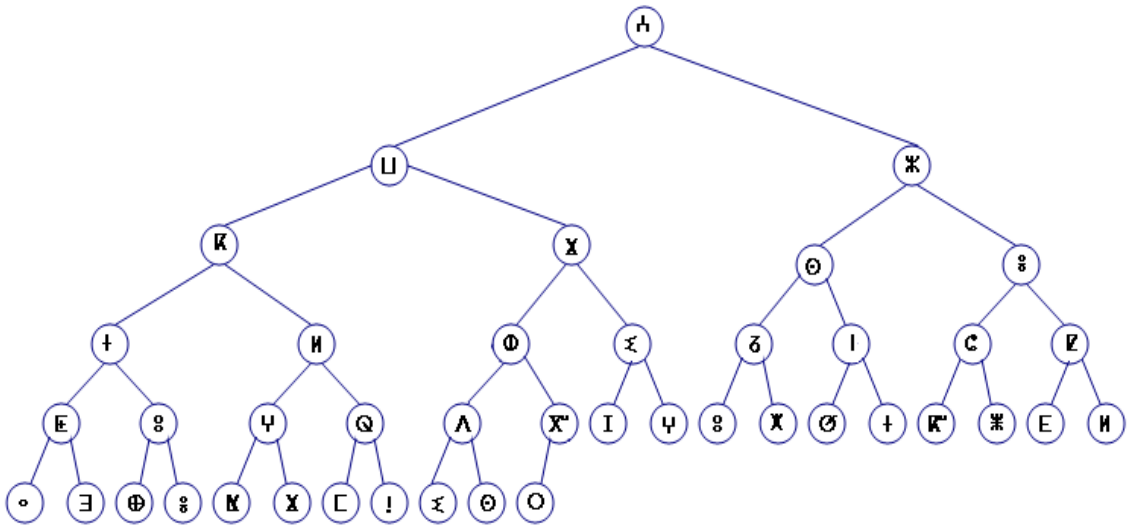
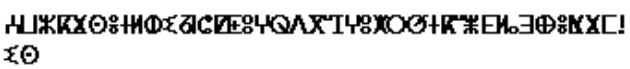


Figure 5. Complete binary tree of the mapping points.

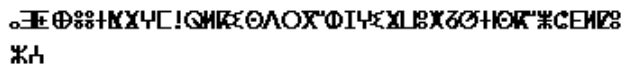
The alphabetical representation of the result sequence is given as:



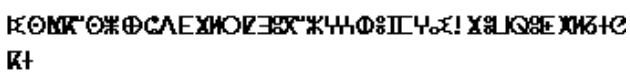
Next, insert the resultant characters in the complete binary tree as seen in Figure 5.

After applying the traversal methods based on the secure key: k_1= (21,10), we get

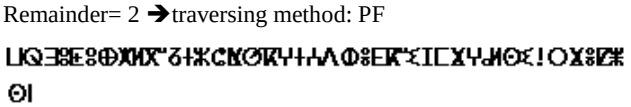
Remainder= 2 ➔traversing method: PF



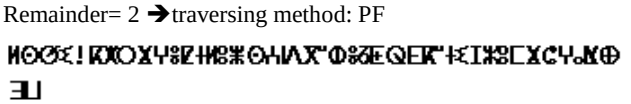
Remainder= 1 ➔traversing method: IF



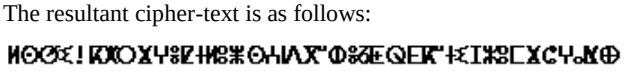
Remainder= 2 ➔traversing method: PF



Remainder= 2 ➔traversing method: PF



The resultant cipher-text is as follows:



At the receiving side, decryption is done by reversing the procedure.

5. RESULTS & DISCUSSIONS

Data Security is a very important aspect. Security of an algorithm is measured by computing number of decryption steps. Higher the number of decryption steps to decrypt the cipher text to get original message shows higher level of security. It is shown that the security can be enhanced by applying the proposed method. For different data sets, results of existing algorithms [19] and [20] are compared with the proposed algorithm. To enhance security, tree traversal method is performed on encrypted data.

The table 1 illustrates the number of decryption steps for input text data of different lengths. As shown below, number of decryption steps varies according to different data values.

Table 1. Number of decryption steps of different algorithms.

Input data size	10	30	50	70
Alg. [19]	27	78	122	195
Alg. [20]	44	95	143	214
Proposed Alg.	63	113	168	231

Graphical representation of the above described table is shown in Figure 6 for computing security in terms of number of decryption steps.

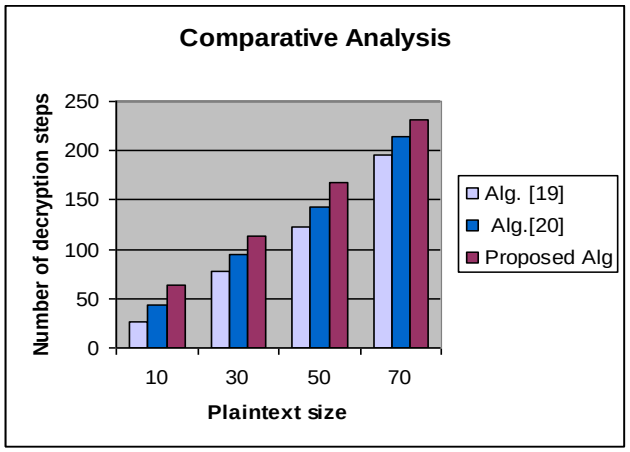


Figure 6. Comparison performances with the existing algorithms.

According to the graph, there is tendency that number of decryption steps of the proposed algorithm, and compared algorithms increases with text data size. According to the proposed algorithm, number of decryption steps taken by decryption algorithm to decrypt the cipher text is high than number of decryption steps of existing algorithms.

6. CONCLUSION

Information security is one of the most important issues in the recent times. ECC is one of the most efficient public key cryptosystems that is secured against adversaries because it is difficult for them to solve the elliptic curve discrete logarithm problem to find the secret key. In this paper, a new efficient approach has been proposed to improve the ECC cryptosystem based matrix. The main contribution is to enhance the security of the proposed method using binary tree. To enhance security, tree traversal method is performed on encrypted data. In this paper the possibility of arranging text into binary tree, and the chose of traversing method provide better performance in this regard. As results, this proposed algorithm can be applied to various Character encoding systems. In near future, it can be applied to various software packages like banking, Educational system etc.

7. REFERENCES

[1] Tanusree Saha, 2015. "An Enhanced Approach to Secure Message Using Combination of Symmetric and Asymmetric Cryptography and Triangulation Method", International Journal of Latest Trends in Engineering and Technology, Vol. 5 Issue 1.

[2] S. Thiraviya Regina Rajam and S. Britto Ramesh Kumar, 2015. "Enhanced Elliptic Curve Cryptography", Indian Journal of Science and Technology, Vol 8 (26).

[3] G.Prabu kanna and V.Vasudevan, "Enhancing the Security of User Data Using the Keyword Encryption and Hybrid Cryptographic Algorithm in Cloud", International Conference on Electrical, Electronics, and Optimization Techniques, IEEE, 2016.

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

[5] T. H. Corment, C. Leiserson, R. Rivest and C. Stein, "Introduction to Algorithms", 2nd Edition, MIT Press, September 2001.

[6] Sumit Sharma and Shobha bhatt, 2015. "Encryption of Message Block using Binary Tree in Block Cipher System: An Approach", International Journal of Science Technology & Engineering, Vol. 2, Issue 01.

[7] Nils Gura , Sheueling Chang Shantz , Hans Eberle , Sumit Gupta , Vipul Gupta , Daniel Finchelstein Edouard Goupy, 2002. "An End-to End Systems Approach to Elliptic Curve Cryptography", In Cryptographic Hardware and Embedded Systems, pp. 349-365.

[8] Darrel Hankerson, Alfred Menezes and Scott Vanstone, Guide to elliptic curve cryptography, Springer-Verlag, 2004.

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

[10] C. Doche G. Frey T. lange K. Nguyen R. Avanzi, H. Cohen and F. Vercateren. "Handbook of elliptic and hyperelliptic curve cryptography". Chapman and Hall, 2006.

[11] William Stalling, "Cryptography and network security"4th edition, Prentice Hall, 2006.

[12] Vishwa gupta, 2012. "Advance cryptography algorithm for improving data security" Int. J of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 1.

[13] Sonali Nimbhorkar1 and Dr. L.G.Malik, 2013. "Prospective Utilization of Elliptic Curve Cryptography for Security Enhancement", International Journal of Application or Innovation in Engineering & Management, Vol. 2, Issue 1.

[14] M. Ameur., A. Bouhjar, F. Boukhris, A. Boukouss, A. Boumalk, M. Elmedlaoui, E. Iazzi, and H. Souifi, "Initiation à la langue Amazighe", Publications de l'IRCAM, 2004.

[15] Fatima Amounas, 2015. "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.

[16] M. Ameur, A. Bouhjar, F. Boukhris, A. Boukouss, A. Boumalk, M. Elmedlaoui, and E. Iazzi, "Graphie et orthographe de l'Amazighe", Publications de l'IRCAM, 2006.

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

[18] F. Amounas and E.H. El Kinani, 2012. "Fast Mapping Method based on Matrix approach For Elliptic Curve Cryptography", International Journal of Information & Network Security, Vol.1, No.2, pp. 54-59.

[19] Geetha G and Padmaja Jain, 2014. "Implementation of Matrix based Mapping Method Using Elliptic Curve Cryptography", International Journal of Computer Applications Technology and Research, Vol. 3, Issue 5, pp. 312-317.

[20] Priti V. Bhagat, Kaustubh S. Satpute and Vikas R. Palekar, 2013. "Reverse Encryption Algorithm: A Technique for Encryption & Decryption", International Journal of Latest Trends in Engineering and Technology, Vol. 2 Issue 1.