International Journal Of Core Engineering & Management
Volume-3, Issue-9, December-2016, ISSN No: 2348-9510

FASTER ECC ALGORITHM FOR ENHANCING THE SECURITY OF AMAZIGH TEXT BASED ON MATRIX SCRAMBLING

Fatima Amounas
R.O.I Group, Computer Sciences Department,
Moulay Ismaïl University, Faculty of Sciences and Technics,
Errachidia, Morocco.
E-mail: f_amounas@yahoo.fr

Abstract
Cryptography is the art of using mathematical models to encrypt and decrypt data. Modern cryptography is suggesting a variety of encryption schemes for protecting and securing the data. In this paper we introduced novel method to encrypt text and enhance the security based on matrix scrambling. In this algorithm the input string is first converted into code points and then it imbedded into points on elliptic curve. Then, we divide the sequence into square matrices and encrypt them using key matrix. After this, we perform transposing data matrix and shifting technique to scramble the data. We illustrate the performance of our implementation using Netbeans 7.1. Our results strongly indicate that elliptic curves are the most efficient method for encryption of Amazigh characters. The use of scrambling matrix will provide better performance in this regard.

Index Terms – Elliptic Curve Cryptography, Matrix scrambling, Encryption, Decryption, Circular shift technique, Amazigh character, Tifinagh.

I. INTRODUCTION

Rapid growth of information technology in present era, secure communication, strong data encryption technique and trusted third party are considered to be major topics. Cryptosystems are commonly used for protecting the integrity, confidentiality, and authenticity of information resources. In addition to meeting standard specifications relating to encryption and decryption, such systems must meet increasingly stringent specifications concerning information security. This is mostly due to the steady demand to protect data and resources from disclosure, to guarantee the authenticity of data, and to protect systems from web based attacks. For these reasons, the development of cryptographic algorithms is a challenging task. Robust encryption algorithm development to secure sensitive data is of great significance among researchers at present. Elliptic Curve Cryptography has been a recent research area in the field of Cryptography. It provides higher level of security with lesser key size compared to other Cryptographic techniques. ECC is considered as a good alternative to RSA and other public key encryption algorithms as it offers high level of security with smaller key sizes [1]. Due to properties and characteristic of elliptic curve cryptography increased attention of the many scientists as a result of it have opened wealth potentialities in terms of security [2, 3, 4]. The security of elliptic curve cryptographic schemes is based on the hardness of the elliptic curve discrete logarithm problem (ECDLP).

The rest of the paper is organized as follows: section 2 discusses background in the field of elliptic curve cryptography and gives a brief review of Amazigh language. Section 3 is devoted to the

International Journal Of Core Engineering & Management
Volume-3, Issue-9, December-2016, ISSN No: 2348-9510

main results. Section 4 describes the implementation with an example. Section 5 discusses experimental report and test result. Finally section 6 ended with the conclusion.

II. BACKGROUND INFORMATION

a. Elliptic Curve

Elliptic Curve Cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. Elliptic curves over two finite fields are mostly used, prime field F_p, where p is a prime and binary field F_{2^m}, where m is a positive integer [5]. There are several standard domain parameters defined. Generally the protocols implementing the ECC specify the domain parameters to be used [6].

- Domain parameters over field F_p

The domain parameters for Elliptic curve over F_p are (p, a, b, G and n). p is the prime number defined for finite field F_p. a and b are the parameters defining the curve $y^2 = x^3 + ax + b \bmod p$. G is the base point on the elliptic curve chosen for cryptographic operations. n is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between 0 and n-1. E(F_p) is the number of points on an elliptic curve.

- Domain parameters over field F_{2^m}

The domain parameters for elliptic curve over F_{2^m} are (m, f(x), a, b, G and n). m is an integer defined for finite field F_{2^m}. The elements of the finite field F_{2^m} are integers of length at most m bits. f(x) is the irreducible polynomial of degree m used for elliptic curve operations. a and b are the parameters defining the curve $y^2 + xy = x^3 + ax^2 + b$. G is the base on the elliptic curve chosen for cryptographic operations. n is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between 0 and n-1. E(F_{2^m}) is the number of points on an elliptic curve.

In our case, we introduce new encryption method based on algebraic description for addition operation over finite field F_p. The mathematical operations of ECC is defined over the elliptic curve $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$. Each value of the parameters a, b gives a different elliptic curve. All points (x, y) which satisfies the above equation lie on the elliptic Curve. The public key is a point on the curve and the private key is also a point on the elliptic curve [7, 8]. The public key is obtained by multiplying the private key with a point which is a generator of the cyclic group. This generator point G, the curve parameters a and b, together with few more constants constitutes the domain parameter of ECC [9, 10,11].

- ***Addition operation***

Suppose that P= (x_1, y_1) and Q= (x_2, y_2) are two distinct points on an elliptic curve E, and the P ≠-Q. To add the points P and Q, a line is drawn through the two points. This line will intersect the elliptic curve E in exactly one more point, called -R.

The image of the point R such that P+Q= R is as follows.

Let P+Q=R where R = (x_3, y_3),

$$x_3 = \lambda^2 - x_1 - x_2$$

International Journal Of Core Engineering & Management
Volume-3, Issue-9, December-2016, ISSN No: 2348-9510

$y_3 = -y_1 + \lambda (x_1 - x_3)$

$\lambda = (y_2 - y_1) / (x_2 - x_1)$ where λ is the slope of the line through P and Q.

- Doubling operation

To add a point P to itself, a tangent line to the curve is drawn at the point P. If y_1 is not 0, then the tangent line intersects the elliptic curve at exactly one other point R. -R is reflected in the x-axis to R. This operation is called doubling the point P; the law for doubling a point on an elliptic curve group is defined by:

P+P=2P=R. when $y_1 \neq 0$, 2P=R where consider a point P such that P = (x_1, y_1), where $y_1 \neq 0$.
Let R = 2P where R = (x_3, y_3), Then

$x_3 = \lambda^2 - 2x_1$

$y_3 = (x_1 - x_3) - y_1$

$\lambda = \frac{3x_1^2 + a}{2y_1} \bmod p$, λ is the tangent at point P.

b. Amazigh Characters

The Amazigh language is a branch of the Afro-Asiatic (Hamito-Semitic) languages. Nowadays, it covers the Northern part of Africa which extends from the Red Sea to the Canary Isles, and from the Niger in the Sahara to the Mediterranean Sea. In Morocco, this language is divided, due to historical, geographical and sociolinguistic factors, into three main regional varieties, depending on the area and the communities: Tarifite in North, Tamazight in Central Morocco and South-East, and Tachelhite in the South-West and the High Atlas [12]. The Amazigh language is spoken today by about 14 million people, mainly in the Morocco.

Since the ancient time, the Amazigh language has its own writing system that has been undergoing many slight modifications. In 2003, it has also been changed, adapted, and computerized by IRCAM, in order to provide the Amazigh language an adequate and usable standard writing system. This system is called Tifinaghe-IRCAM. With the UTF-8 encoding, Unicode characters can be used. The Table 1 below presents the Amazigh characters and the associated Unicode allocated by ISO. It is encoded in the Unicode range U+2D30 to U+2D7F. There are 55 defined characters [13, 14].

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																

International Journal Of Core Engineering & Management
Volume-3, Issue-9, December-2016, ISSN No: 2348-9510

III. MAIN RESULT

In this section we offer the new methodology for encrypting of a Unicode message (plain text) and decrypting back once more to the original message. The proposed scheme is based on Elliptic Curve Cryptography (ECC) approach. Performing the process of encryption several times enhance the security by changing secure key in every phase. It enhances security because of performing the ECC operation with different encryption key at every step. This mechanism is more secure and fast than existing systems. So we have tried to implement this mechanism with matrix approach to achieve better results.

Suppose that we have some elliptic curve E defined over a finite field F_p and that E and a point $P \in E$ are publicly known, as is the embedding system M→ P_m which imbed plain text on an elliptic curve E [15, 16, 17]. The overall encryption methodology is as shown in the Figure 1.

a. Key Exchange between Alice and Bob

Elliptic curve cryptographic key exchange can be done in the following way. First, choose the parameters (a, b, p) of the elliptic curve equation. Then, define the elliptic group of points. Next, pick a base point $P \in E_p(a, b)$ whose order is very large order value n.
A key exchange between the intended users can be accomplished as shown below:

1. Alice selects an integer n_A less than n. This is Alice's private key. Alice then generates a public key $P_A = n_A P$ where the public key is a point in $E_p(a, b)$.
2. Bob similarly selects a private key n_B and computes a public key $P_B = n_B P$.
3. Alice generates the secret key. Bob generates the secret key.

These two calculations in step 3 produce the same result: $n_A \times P_B = n_A(n_B P) = n_B(n_A P) = n_B P_A$

b. Encryption process

Let us assume that the plaintext containing Amazigh characters has to be encrypted, a user can perform encryption on the code point of each character. The various steps of the proposed approach are shown in Figure 1.

Steps of an algorithm to perform encryption:
1. Input the original text as a sentence Amazigh and store it.
2. Get the code points for each characters of the input string. Let the set of code points based number conversion is (x_1, x_2, …, x_n).
3. Split the sequence into blocks and arrange the equivalent points into square matrix of 3×3 as follows:

P_1	P_2	P_3
P_4	P_5	P_6
P_7	P_8	P_9

4. Choose a random number k and compute the secure key.

5. Create a square matrix of 3×3 with the next characters.

International Journal Of Core Engineering & Management
Volume-3, Issue-9, December-2016, ISSN No: 2348-9510

K_1	K_2	K_3
K_4	K_5	K_6
K_7	K_8	K_9

6. Apply the ECC operations to encrypt the mapping point P_m.
7. Apply transposing process of the matrix followed by row shift and column shift.
8. Repeat scrambling process m times.
9. Convert the result points into characters. Then, send (kP, C_i), i=1, 2, …

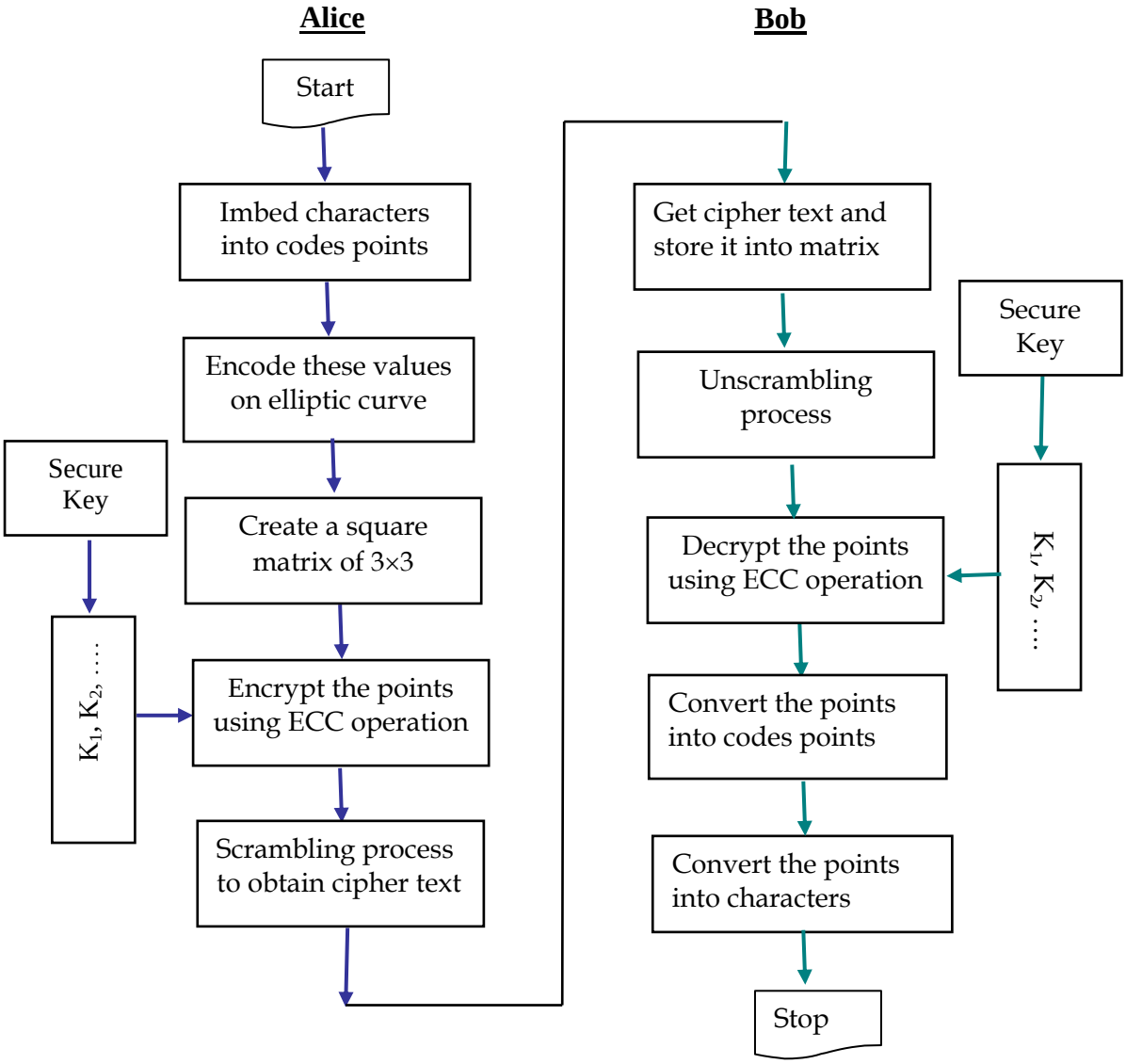


Fig. 1. Flow Chart of the proposed method.

International Journal Of Core Engineering & Management
Volume-3, Issue-9, December-2016, ISSN No: 2348-9510

c. Decryption process

To recover the plain text from the cipher text, Bob should do following steps:

1. Get the cipher text and convert it to points on elliptic curve.
2. Extract the first block and compute the secure key K= $n_B P_1$.
3. Arrange the obtained points into data matrix.
4. Apply unscrambling process to get back the encrypted data matrix.
5. Repeat step 3-4 for the remaining blocks.
6. Generate the key matrix with entries in elliptic curve.
7. Decrypt the data matrix by performing addition and doubling operations on EC.
8. Convert the result points into code points.
9. Reverse the embedding to get the original message.

IV. IMPLEMENTATION DETAILS OF THE PROPOSED METHOD

In this section, we have a tendency to take into account the elliptic curve given by the Weierstrass equation $y^2=x^3 -x + 188$ mod 241 and detailed our method by an example.

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

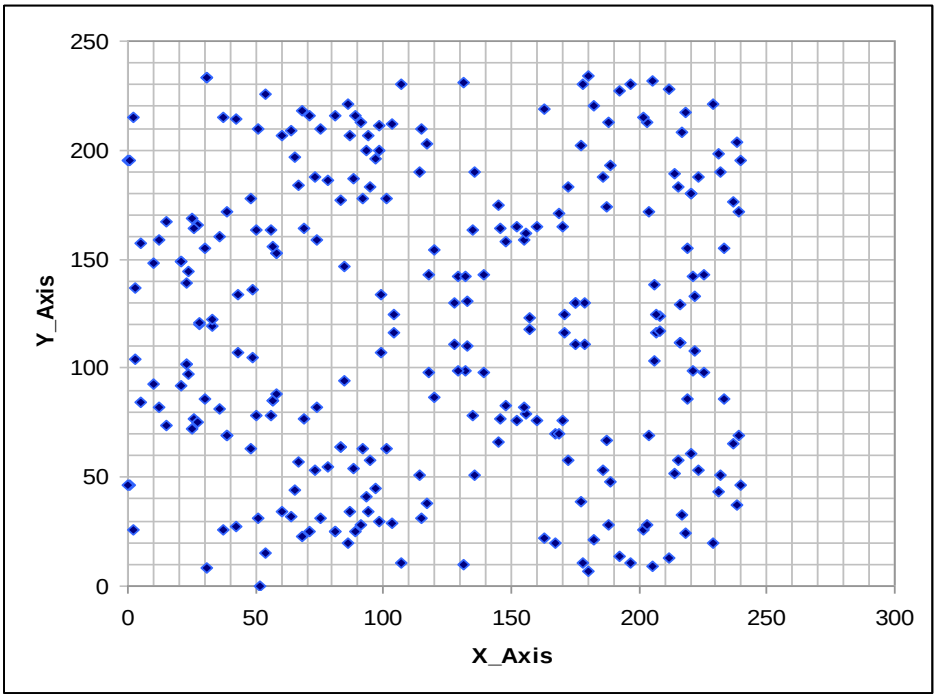


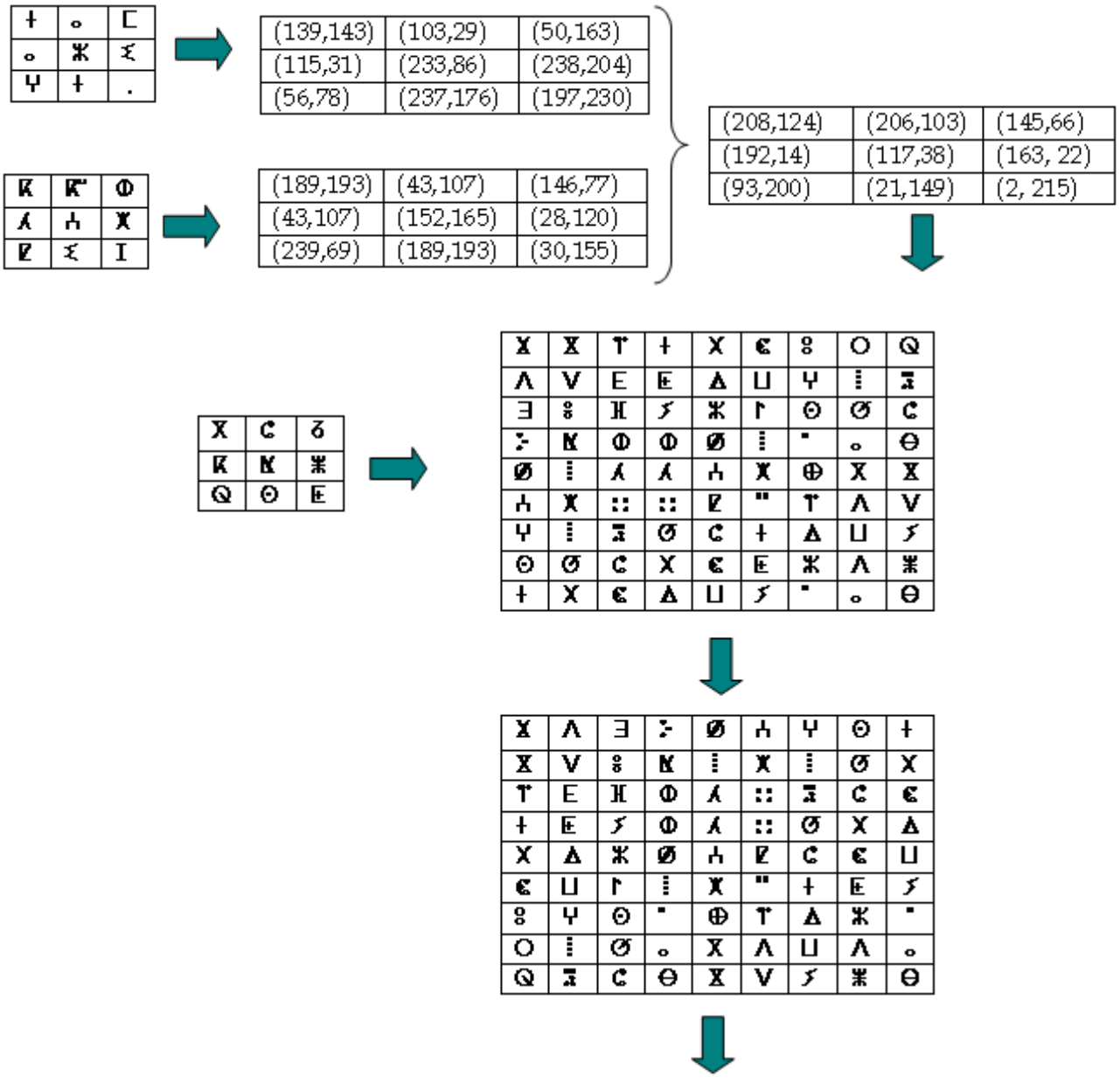
Fig. 2 The set of points on elliptic curve $E_{241}(-1 ,188)$.

International Journal Of Core Engineering & Management
Volume-3, Issue-9, December-2016, ISSN No: 2348-9510

Let P= (1, 46) be the base point chosen on the elliptic curve.
Alice's private key: $n_A = 19$, public key: (23, 102).
Bob's private key: $n_B = 31$, public key: (31, 233).
Let k be a random number: k=43 ➔ K=(208,124).

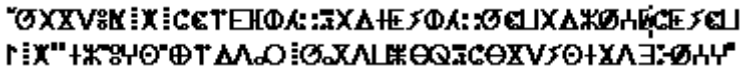
Encryption

Alice wants to send the plaintext: "" to Bob. She does the following steps:



International Journal Of Core Engineering & Management
Volume-3, Issue-9, December-2016, ISSN No: 2348-9510

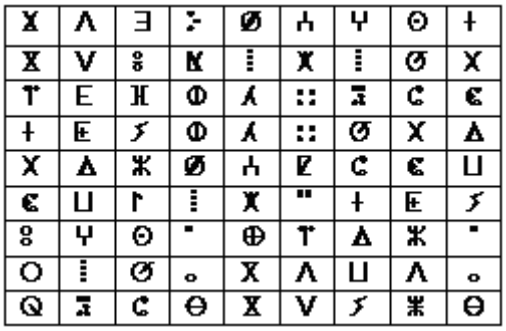
Therefore, the cipher text is:



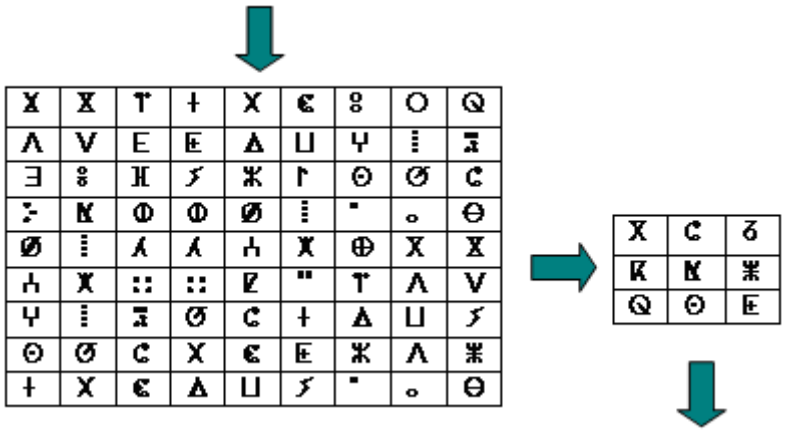
Decryption

When Bob received the cipher text, he does steps as following:

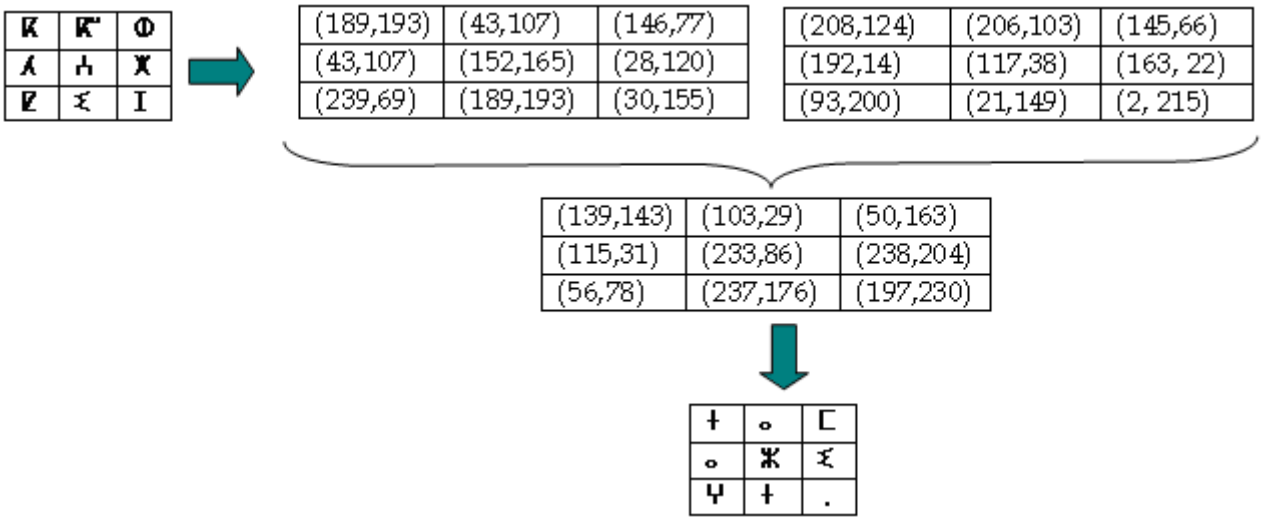
Extract the first block and arrange the remaining characters into square matrix as shown below. To unscramble the cipher text, perform row shift and column shift followed by transposing data matrix.



International Journal Of Core Engineering & Management
Volume-3, Issue-9, December-2016, ISSN No: 2348-9510



Next, perform ECC operations to decrypt the encrypted points as follows:



(189,193)	(43,107)	(146,77)
(43,107)	(152,165)	(28,120)
(239,69)	(189,193)	(30,155)

(208,124)	(206,103)	(145,66)
(192,14)	(117,38)	(163, 22)
(93,200)	(21,149)	(2, 215)

(139,143)	(103,29)	(50,163)
(115,31)	(233,86)	(238,204)
(56,78)	(237,176)	(197,230)

Then, reverse the embedding to get back the original message: "ⵜⴰⵎⴰⵣⵉⵖⵜ."
It is clear from example that the amazigh text is encrypted and decrypted correctly and that the code point of Unicode is stronger as compared to decimal values of ASCII Code. The encryption and decryption process is successfully performed with the help of matrix approach.

V. RESULTS

In this section, we present the results obtained from practical implementation of our algorithm using Netbeans as tools. The key generation process can be seen in the Figure 3. It shows the selected EC parameters, and the secure key generated. A key matrix is generated with entries are points on elliptic curve. To demonstrate the potency of our method, we tested our system with some sentences Amazigh as input string. Below figures shows the results obtained by our proposed algorithm.

International Journal Of Core Engineering & Management
Volume-3, Issue-9, December-2016, ISSN No: 2348-9510

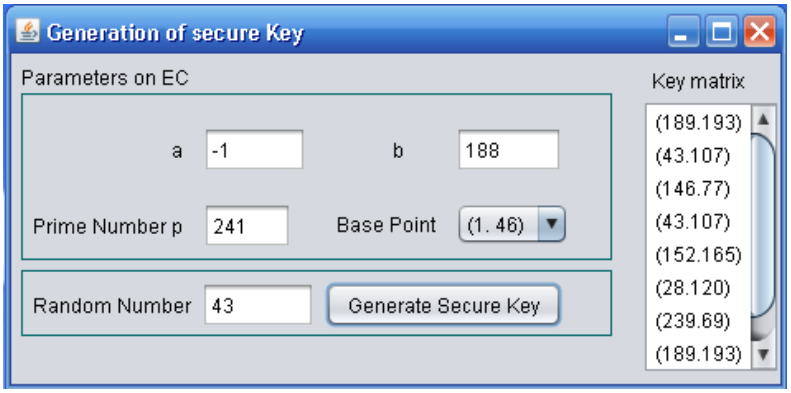


Fig.3 Generation of key matrix.

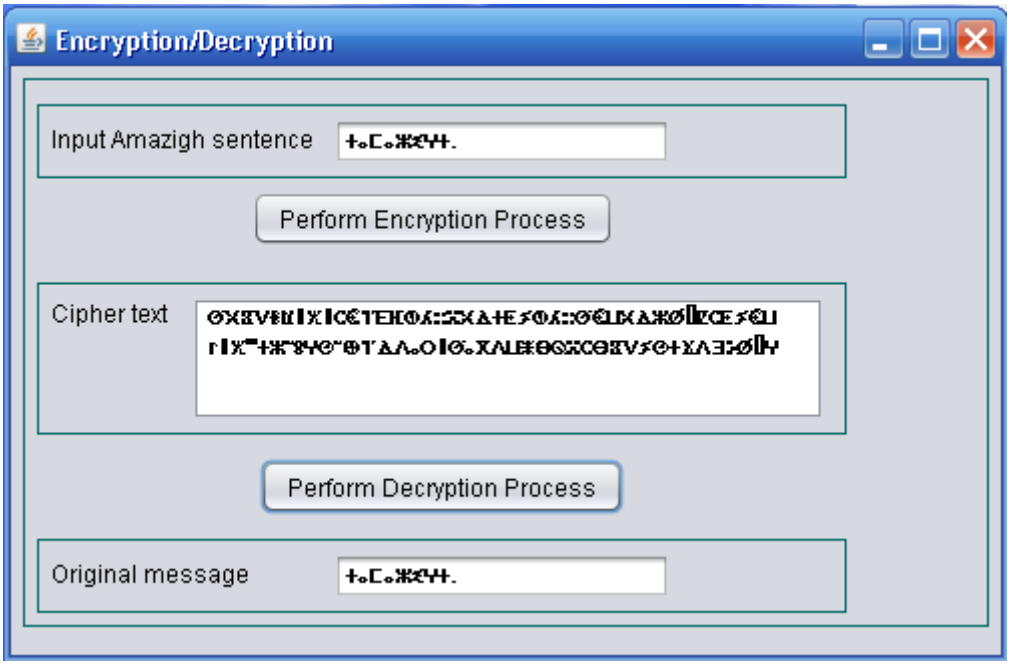


Fig. 4 Encryption and decryption interface.

From the implementation and testing results it is concluded that the proposed method is suitable to encrypt Amazigh text. Further, the main feature of this method is that it satisfies the properties of confusion and diffusion so without knowing keys it makes decryption nearly impossible.

VI. CONCLUSION

In this paper, we discussed the main challenges in enhancing the security of the Amazigh language, and we attempted to provide a novel encryption algorithm based ECC using scrambling technique. In this work, we have used basic matrix properties based on ECC for communicating Unicode message. So manipulations involved in sending any message is simple, but it is strong since until one knows the EC parameters, determining key matrix is not possible. The test conducted on the algorithm showed its robustness and efficiency. Finally, we would like to point out that the use of a matrix scrambling will provide better performance in this regard. Furthermore, the proposed method is suitable to encrypt most of the written languages in the world. In the future, experiments should be conducted to implement the algorithm on different applications related to Amazigh language, in order to ensure its feasibility and applicability.

REFERENCES

[1] Dindayal Mahto, Danish Ali Khan and Dilip Kumar Yadav, "Security Analysis of Elliptic Curve Cryptography and RSA", Proceedings of the World Congress on Engineering 2016 Vol I, WCE 2016, June 29 - July 1, 2016.

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

[3] Naresh S. Badve, "Cryptography using Elliptic Curve with Matrix Scrambling", Journal for Research, Vol. 01, Issue 01, March 2015.

[4] 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.

[5] D. Sravana Kumar, Ch. Suneetha and A. Chandrasekhar, "Encryption of Data Using Elliptic Curve Over Finite Fields", International Journal of Distributed and Parallel Systems, vol. 3, no. 1, 2012.

[6] William Stallings, "Cryptography and network security principles and practice", Prentice Hall, 5th Edition, 2011.

[7] Padma Bh, D.Chandravathi, P.Prapoorna Roja, "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method", International Journal on Computer Science and Engineering, Vol. 02, No. 05, pp. 1904-1907, 2010.

[8] O.Srinivasa Rao and S. Pallam Setty, "Efficient Mapping methods for Elliptic Curve Cryptosystems", International Journal of Engineering Science and Technology, Vol. 2(8), pp.3651-3656, 2010.

[9] B. Ravikumar, G. Naga Lakshmi, T. Surendra, A. Chandra Sekhar. "A Study on group theoretic Elliptic curves - An m implementation to Cryptography", International Journal of Science and Advanced Technology, Vol 1, No 6, 2011.

[10] 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.

[11] Vishal Kumar, Ratnesh, Mashud A. And Monjul Saika, "Multiple Encryption using ECC and

it's Time Complexity Analysis, International Journal of Computer Engineering In Research Trends, Vol. 3, Issue 11, pp. 568-572, 2016.
[12] Ameur M., Bouhjar A., Boukhris F., Boukous A., Boumalk A., Elmedlaoui M., Iazzi E., Souifi H. Initiation à la langue amazighe. IRCAM, Rabat, Maroc, 2004.
[13] Lazzi E., Outahajala M. Amazigh Data Base. In Proceedings of HLT & NLP Workshop within the Arabic world: Arabic language and local languages processing status updates and prospects, Marrakech, Morocco, pp. 36-39, 2008.
[14] Andries P. Unicode 5.0 en pratique, Codage des caractères et internationalisation des logiciels et des documents. Dunod, France, Collection InfoPro. 2008.
[15] Fatima Amounas and El Hassan 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.
[16] Geetha G, Padmaja Jain ,"Implementation of Matrix based Mapping Method Using Elliptic Curve Cryptography",International Journal of Computer Applications Technology and Research Volume 3– Issue 5, 312 - 317, 2014.
[17] 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, 2014.