An Enhanced Approach of Elliptic Curve Cryptosystem based Unicode Representation

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

Lahcen El Bermi
ROI Group, Computer Science Department,
Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco.
elbermi.lahcen@gmail.com

***Abstract*—**Data encryption is an important issue and widely used in recent times to ensure security. Elliptic Curve Cryptography (ECC) is one of the most efficient techniques that are used in public key cryptography, 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. ECC is more complex and thus it provides greater security and more efficient performance. This paper aims to propose an enhanced approach of elliptic curve cryptosystem based Unicode representation. The proposed technique transforms the text message into an affine point called P_m on the elliptic curve, over the finite field GF(p). Each character in the text message is represented by its Unicode value denoted by two digits and separated into two values. Then, the addition and doubling operations are performed on each value to obtain an affine point on elliptic curve. This transformation makes cryptosystem more secure and complicated to resist the adversaries. Further, the use of Unicode representation will provide better performance in this regard.

Keywords- *Elliptic Curve Cryptography, Unicode Encoding, Encryption, Decryption, Amazigh character.*

*****

I. INTRODUCTION

Cryptography is one of the mathematical techniques that ensure secure communications within a non-secure channel. Cryptography is divided into two types, Symmetric key and Asymmetric key cryptography. In Symmetric key cryptography a single key is shared between sender and receiver. The sender uses the shared key and encryption algorithm to encrypt the message. The receiver uses the shared key and decryption algorithm to decrypt the message. In Asymmetric key cryptography each user is assigned a pair of keys, a public key and a private key. The public key is announced to all members while the private key is kept secret by the user. The sender uses the public key which was announced by the receiver to encrypt the message. The receiver uses his own private key to decrypt the message.

Elliptic curve cryptography is one of the famous techniques used recently in public key cryptography. ECC is a better alternative for public key encryption. It depends on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which cannot be solved by the adversary.

The level of difficulty in solving the DLP can be increased by selecting a base point G whose order is very large [1, 2, 3]. Several studies have been presented by many researchers. Maria Celestin Vigila S. and al [4] discusses the implementation of text based Elliptic Curve Cryptosystem. Each character in the message is represented by its ASCII value. Each of these ASCII value is transformed into an affine point on the EC. This transformed character of the message is encrypted by the ECC technique. Meltem Kurt and al. [5] presented a modified cryptosystem using hexadecimal to encrypt data. Their study depended on Menezes Vanstone ECC algorithm by adding additional features. They made the system more security and more confusion than the original algorithm. An implementation of ElGamal ECC for encryption and decryption a message is also proposed by Debabrat Boruah in [6].

A number of research papers have been published showing the utilization of ECC for enhancing the security of applications [7, 8]. In this context, this research work aims to develop a secure encoding method which can enhance the security of elliptic curve cryptosystem by using Unicode representation. This paper is organized as follows. Section 2 presents a mathematical introduction to elliptic curve function over prime field and the Unicode representation. Section 3 explains the proposed approach. Section 4 gives a brief illustration with an example. The implementation result is presented in section 5. Finally, Section 6 presents the discussion and conclusion of the proposed method.

II. BACKGROUND DETAIL

A. *Mathematical Basics of elliptic curve*

In elliptic curve cryptography, a restricted form of elliptic curve defined over a finite field F_p is considered. One particular interest for cryptography is referred to elliptic group mod p, where p is prime number [9]. Eq.1 refers to the general form of elliptic curve:

$$y^2=x^3+ax+b \mod p \quad (1)$$

Where 'a' and 'b' are two nonnegative integers less than p, satisfying the following condition:

$$4a^3+27b^2 \pmod p \neq 0.$$

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.

ECC Point Operations

- Point Addition

Suppose M(x_M , y_M) and N(x_M , y_M) are two points lie on an elliptic curve E defined in Equation (1). The sum M+N results a third point R (x_R , y_R) which is also lies on E. The coordinates of the result point is given as follows:

- If M≠N ($x_M \neq x_N$), then the sum is defined by

R(x_R , y_R) =M+N such that:

$$x_R = (s^2 - x_M - x_N) \mod p$$

$$y_R = s(x_M - x_R) - y_M \mod p$$

Where

$$s = \frac{y_N - y_M}{x_N - x_M}$$

- If ($x_M = x_N$) but $y_M \neq y_N$ then M+N=Ω.

- Point Doubling

Let M(x_M , y_M) be a point lies on E. Adding he point M to itself is called doubling point on elliptic curve. The coordinates of the result point is given as follows:

R(x_R , y_R) = 2M such that:

$$x_R = (s^2 - 2x_M) \mod p$$

$$y_R = s(x_M - x_R) - y_M \mod p$$

Where

$$s = \frac{3x_M^2 + a}{2y_M}$$

- Scalar Multiplication

Suppose α is an integer and P(x_M , y_M) is a point lies on E. The scalar multiplication can be defined by:

αP= P+ P+ …+ P (α times).

A scalar multiplication αP can be computed by a combination of the point addition and point doubling operations on elliptic curve [10].

The security of ECC rests on the hardness of discrete logarithm problem over the points on the elliptic curve. Elliptic Curve Discrete Logarithm Problem (ECDLP) states that given a base point P and a point Q=αP lying on the curve, it is hard to determine α.

B. *Unicode Representation*

The characters of any language are encoded using UNICODE representation. The objective of UNICODE is to unify all the different encoding schemes so that confusion between computers can be limited as much as possible. UNICODE standard defines values for different characters and can be seen at the UNICODE Consortium [11]. It has several character encoding forms, UTF standing for UNICODE Transformation Unit. UTF-8 only uses one byte to encode the characters. UTF-16 uses two bytes (16 bits) to encode the most commonly used characters. UTF-32 uses four bytes (32 bits) to encode the characters.

The Amazigh alphabet which is called "Tifinagh-IRCAM", adopted by the Royal Institute of the Amazigh Culture (IRCAM), was officially recognized by the International Organization of Standardization (ISO) as the basic multilingual plan [12]. Each Amazigh character has a code point. It 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 of "U+". The set of Amazigh characters and their corresponding Unicode assigned by ISO is illustrated in [13].

III. PROPOSED APPROACH

Different methods are suggested in the literature for encoding message to an elliptic curve [14, 15]. The simplest method is to use the ASCII value of characters in the message to find the points on the curve. Each point can be directly mapped to the ASCII value of character. This method is suitable for encrypting short messages. But this method is inefficient in terms of security. In this paper, we suggest a novel method based ECC using Unicode representation which is structurally and functionally divided into two basic parts. The first part of the algorithm is based on elliptic curve based matrix approach [16, 17]. The second part deals with the traversing process (Figure 1). The main idea of our contribution depends on using the Unicode value to enhance the security of ECC technique. Now, we discuss the algorithms in greater details to explain its working and features.

 ISSN: 2321-8169
126 – 131

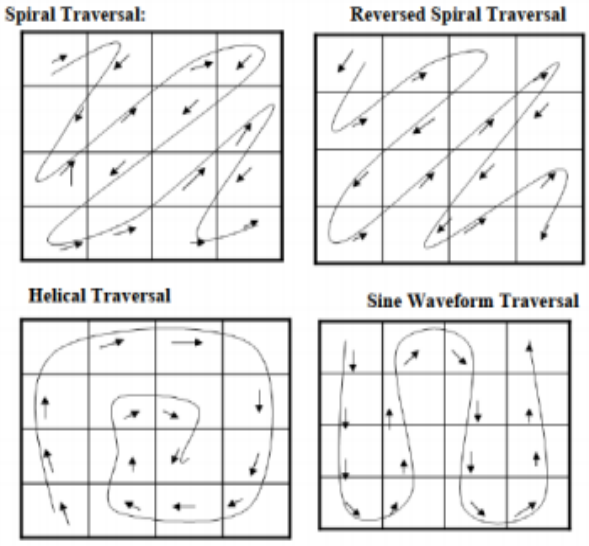

Figure 1. The traversing process.

A. Encryption/ Decryption Algorithms

Suppose that A and B are two users wishing to communicate over insecure channel. Let us choose the user A as the sender who wants to encrypt and send a message to the user B (the receiver). Every entity needs to choose a private key. The private keys, n_A and n_B are positive integers chosen randomly from the interval [1, p-1]. Te public keys for the users A and B can be generated respectively as follows:

$$P_A = n_A P$$

$$P_B = n_B P$$

1) Encryption process

Step 1. Choose an elliptic curve Ep (a,b) with a base point P.

Step 2. Choose a random number k and compute a secure key $K = kP_B = (k_1, k_2)$.

Step 3. Input any sentence Amazigh as plain text message.

Step 4. Imbed the character into code point using Unicode form. Then, Substitute it with the corresponding value of two digits $(h_1 h_2)_{16}$.

Step 5. Convert each value of h_1 and h_2 to decimal values d_1 and d_2 respectively. Then, compute $P_1 = d_1 P$ and $P_2 = d_2 P$ where P_1 and P_2 are two points lie on E. two parameters:

Step 6. Perform ECC operations to compute the mapping points $Q_1 = P_1 + k_1 P$ and $Q_2 = P_2 + k_2 P$.

Step 7. Repeat the step 4 to 6 for the remaining characers.

Step 8. Arrange the mapping points into data matrix of r×2 with entries as points on EC.

$$PM = \begin{pmatrix} Q_{11} & Q_{12} \\ Q_{21} & Q_{22} \\ \dots & \dots \\ Q_{r1} & Q_{r2} \end{pmatrix}$$

Step 9. Choose a non-singular matrix A of 2×2 and compute the product PM*A. The result matrix is denoted B.

Step 10. Create a Square matrix of order m×m with entries as the encrypted points. Then, Apply traversing process to get data matrix C. Let b= $(b_i b_j)$, where j is bit position (LSB→MSB), which decides which transformation has to be performed.

If $b_i b_j$ =00 ➔ Spiral Traversal.

If $b_i b_j$ =01 ➔Helical Traversal.

If $b_i b_j$ =10 ➔ Reversed Spiral Traversal.

If $b_i b_j$ =11 ➔ Reversed Sine waveform Traversal.

Step 11. The set of points (kP, C_i) is sent to the user B.

2) Decryption process

Upon receiving the cipher text (kP, C_i) by user B, the decryption process will be started. The steps in decryption algorithm are as follows:

Step 1. Input the encrypted Text.

Step 2. Extract the first block and multiply his private key n_B by kP to get the secret key $K = (k_1, k_2)$.

Step 3. Arrange the remaining points into data matrix of m×m. Then, Reverse the operations done in the traversing process to get back data matrix C.

Step 4. Create a data matrix B of r×2 with entries as encrypted points. Then, perform ECC operations to compute the product B*A $^{-1}$ =PM.

Step 5. Apply subtraction operation for each row of data matrix to get the mapping points:

$$P_{i1} = Q_{i1} - k_1 P \text{ and } P_{i2} = Q_{i2} - k_2 P.$$

Step 6. Extract d_1 and d_2 from P_{i1} and P_{i2} respectively by solving the discrete logarithm problem.

Step 7. Convert each value into equivalent hexadecimal value. Then, transform the result values into code point.

Step 8. Find the equivalent Unicode value from the code point. Then, accumulate characters to form the plaintext message.

ISSN: 2321-8169
126 – 131

IV. ILLUSTRATION WITH AN EXAMPLE

Assume that Alice and Bob are agreed to use the elliptic curve:

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

Let the point (1, 46) be chosen as the base point P.
The points of the elliptic curve $E_{241}(-1, 188)$ are shown below:

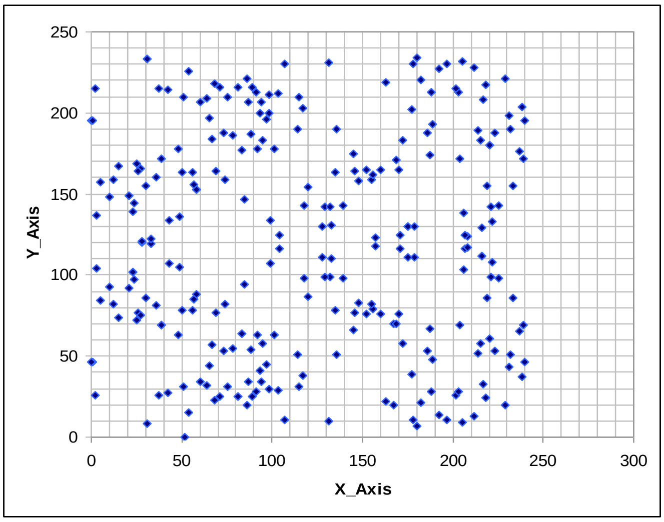

Figure 2. The set of points on elliptic curve $E_{241}(-1, 188)$.

Each user chooses his secure key and computes his public key: $n_A = 61$, $n_B = 13$, $P_A = (107, 11)$, $P_B = (222,133)$.

Let the plaintext to be encrypted is: "ɑLIX≡HΦɑI".
First, convert each character to the hexadecimal value as shown below:

ɑ	LI	X	≡	H	Φ	ɑ	I
30	61	33	3B	4D	40	30	4F

Next, separate each value into two values and converts them to decimal values. Then, compute the mapping points using addition and doubling operations on EC:

(Q_{ij}) = {(238,204), (91,28), (197,230), (43,107), (238,204), (25,72), (238,204), (28,120), (56,78), (240,195), (56,78), (91,28), (238,204), (91,28), (56,78), (186,53)}

Let A be a chosen non-singular matrix:

$$A=\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$$

Now, apply ECC technique based matrices to get the encrypted points stored into square matrix as shown below:

(179,111)	(26,164)	(146,77)	(182,220)
(97, 45)	(239,69)	(74,159)	(30, 86)
(231,43)	(189,193)	(30,155)	(65,197)
(152,165)	(12,159)	(21,149)	(156,79)

Let K be a chosen secure key: K=(48, 63).
Now, select the bits position to perform traversing transformation. The result data matrix C is given as below:

(179,111)	(26,164)	(146,77)	(182,220)
(97, 45)	(239,69)	(74,159)	(30, 86)
(231,43)	(189,193)	(30,155)	(65,197)
(152,165)	(12,159)	(21,149)	(156,79)

⇩

(179,111)	(30, 86)	(231,43)	(156,79)
(26,164)	(74,159)	(189,193)	(21,149)
(146,77)	(239,69)	(30,155)	(12,159)
(182,220)	(97, 45)	(65,197)	(152,165)

⇩

(156,79)	(26,164)	(74,159)	(189,193)
(231,43)	(97, 45)	(65,197)	(21,149)
(30, 86)	(182,220)	(152,165)	(146,77)
(179,111)	(12,159)	(30,155)	(239,69)

⇩

(156,79)	(26,164)	(97, 45)	(65,197)
(74,159)	(231,43)	(21,149)	(179,111)
(189,193)	(30, 86)	(146,77)	(12,159)
(182,220)	(152,165)	(30,155)	(239,69)

⇩

(156,79)	(179,111)	(189,193)	(239,69)
(26,164)	(21,149)	(30, 86)	(30,155)
(97, 45)	(231,43)	(146,77)	(152,165)
(65,197)	(74,159)	(12,159)	(182,220)

Then, the result points are given as follows:
(156,79) (179,111) (189,193) (239,69) (26,164) (21,149) (30, 86) (30,155) (97, 45) (231,43) (146,77) (152,165) (65,197) (74,159) (12,159) (182,220)
Therefore, the cipher text to be sent is:

"[illegible]"

 ISSN: 2321-8169
126 – 131

Decryption process is just the reverse of the encryption and we get back to the plaintext easily.

V. RESULTS

It is observed that the proposed algorithm is successfully is working, it could able to encrypt and decrypt the Amazigh characters. To prove that it is working well, we have implemented in JAVA programming language [18], for a chosen curve. Results are presented to show the security level by using the Enhanced ECC Algorithm as shown in Figure 3, Figure 4 and Figure 5.

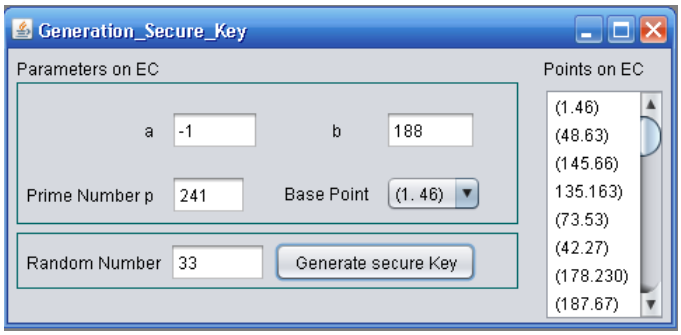

Figure 3. Generation of the secure key.

In this implementation, the plaintext is first given in Amazigh language then the secret key is used to perform the encryption process. This encrypted text will be given as input for the decryption process. Then, decryption is performed to generate the original text.

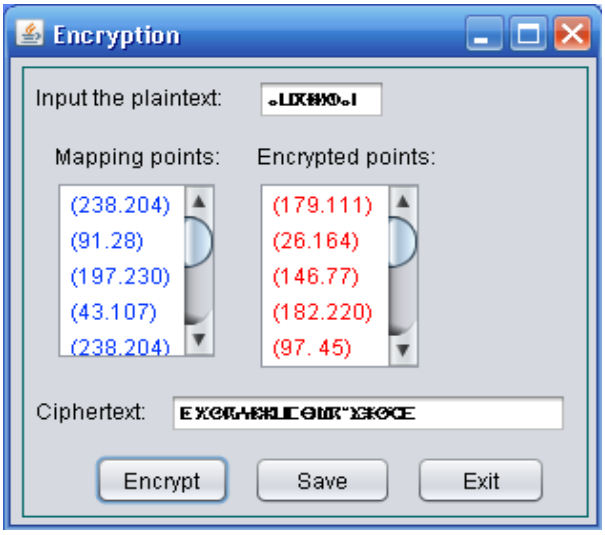

Figure 4. A screen shot of the encryption process.

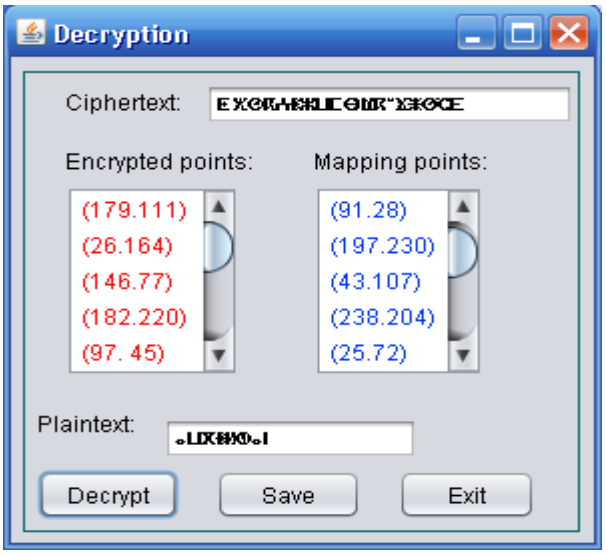

Figure 5. A screen shot of the decryption process.

The use of Unicode representation makes the cryptanalysis based on letter frequency of plaintext can be defeated. To enhance the strength of the cipher we can have more numbers of rotations with different keys.

VI. CONCLUSION

ECC technique is a secure method and is widely used for encrypting text messages. It has the ability to provide adequate security with smaller key size. But the advancement in the areas of cryptanalysis demands the enhancement of existing scheme. In this context, we have proposed an enhanced approach for ECC cryptosystem using Unicode representation, which provides an additional level of security for elliptic curve cryptosystem. The method uses Unicode characters instead of ASCII, and then it is suitable to encrypt most of the written languages in the world.

REFERENCES

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

[2] Su, Pin-Chang, Erl-Huei Lu, and Henry Ker-Chang Chang. "A knapsack public - key cryptosystem based on elliptic curve discrete logarithm." Applied mathematics and computation 168 (1): pp.40-46, 2005.

[3] Garima Kaushik and, Shailendra Gaur, “Proposed Model for Network Security Issues Using Elliptical Curve Cryptography”, IOSR Journal of Electronics and Communication Engineering, Vol. 7, Issue 3, pp. 56-60, 2013.

[4] Maria Celestin Vigila S, Muneeswaran K, “Implementation of Text based Cryptosystem using Elliptic Curve Cryptography”, IEEE, Vol. 9, pp. 82-85, 2009.

[5] Kurt M, Yerlikaya Y. “A new modifed cryptosystem based on Menezes Vanstone elliptic curve cryptography algorithm that uses characters’ hexadecimal values”. International Conference on Technological Advances in Electrical, Electronics and

Computer Engineering (TAEECE), Konya: IEEE, 9-11 May, 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] Komal Agarwal,Anju Gera, "Elliptic Curve Cryptography with Hill Cipher Generation for secure Text Cryptosystem", International Journal Of Computer Applications, Vol 106, No.1, 2014.

[8] Santhoshi Pote, "Enhancing the Security of Koblitz's Method Using Transposition Techniques for Elliptic Curve Cryptography", International Journal of Research in Engineering & Advanced Technology", Vol. 2, Issue 6, 2015.

[9] D. R. Hankerson, S. A. Vanstone, and A. J. Menezes, "Guide to Elliptic Curve Cryptography", Springer, 2004.

[10] Geetha G, Padmaja Jain , " 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, 2014.

[11] Maram Balajee, "UNICODE and Colors Integration tool for Encryption and Decryption", published in International Journal on Computer Science and Engineering, Vol. 3 No. 3, 2011.

[12] L. Zenkouar, " L'écriture Amazighe Tifinaghe et Unicode", in Etudes et documents berbères. Paris (France). No 22, pp. 175-192, 2004.

[13] Fatima Amounas and El Hassan El Kinani, "Cryptography with Elliptic Curve using Tifinagh Characters", Journal of Mathematics and System Science 2, pp. 139-144, 2012.

[14] D.Sravana Kumar, CH Suneetha, A.Chadrasekhar, "Encryption of data using Elliptic Curve over finite fields", International Journal of Distributed and Parallel Systems, Vol 3, No1, January 2012.

[15] F.Amounas, E.H.EI Kinani, "Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography", International Journal of Information and Network Security,Vol-1,No 2, pp. 54-59, 2012.

[16] F.Amounas, "An Innovative Approach for Enhancing the Security of Amazigh Text Using Graph Theory Based ECC", International Journal of Scientific Research in Science, Engineering and Technology, Vol. 2, Issue 3, pp. 480-487, 2016.

[17] Balamurugan, R, Kamalakannan, V, Rahul G, D, Tamilselvan, S. "Enhancing security in text messages using matrix based mapping and ElGamal method in elliptic curve cryptography". In: Contemporary Computing and Informatics, 2014 International Conference on. IEEE, pp 103-106, 2014.

[18] Herbert Shildt, "Java complete reference", Tata McGraw-Hill, 2011