ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

Enhancing Robustness of Encrypting Amazigh Alphabet based ECC using Scrambling Method

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

Abstract— ***With the fast development of cryptography research and computer technology, the cryptosystems such as RSA require large number of bits so they became inadequate. The cryptosystem based on Elliptic Curve Cryptography (ECC) is becoming the recent trend of public key cryptography. This paper proposes a new approach for encrypting Amazigh alphabet based ECC using Rubik's Cube Principle. As an alternative approach to handling ASCII characters in the cryptosystems, a Unicode implementation is deliberated of in this work. In fact, scrambling techniques are designed to make the content unintelligible. This approach will boost the security due to its complexity in encryption because it deals with Rubik's Cube. It attempts to augment the efficiency by providing add-on security to the elliptical cryptosystem. Our algorithm provides maximum security, so it is fast enough for most applications.***

***Index Terms*—Elliptic curve Cryptography, Scrambling technique, Rubik's Cube, Amazigh alphabet.**

I. INTRODUCTION

In the today's world, security is required to transmit confidential information over insecure channel. It is important to send data securely. Cryptographic algorithms play a vital role in providing the data security against malicious attacks[1]. In fact, cryptography is the science of using mathematics to encrypt and decrypt data. Encryption of data is an important topic for research, as secure and efficient algorithms are needed that allow optimized encryption and decryption of data. The efficiency of a cryptographic algorithm is based on its execution time taken for encryption /decryption and the way it produces diverse cipher text from a clear text. The RSA [2], the extensively used public key algorithm and other public key algorithms may not guarantee that the cipher text is copiously secured. As an alternative approach to RSA, a cryptosystem based on Elliptic Curve Cryptography is becoming the recent trend of public key cryptography.

In the last decade the application of the elliptic curves in cryptography has been attracting increased attention of many scientists, because they have opened wealth possibilities in terms of security. In recent past some encryption schemes have also been developed [3-5]. But the disadvantage is that one character is encrypted into fixed number of data values. So they can be vulnerable to the attackers.

The mechanism of scrambling method given by Suli Wu and al. [6], has given the idea of matrix scrambling based on two way circular queue. In our previous works [7, 8], our idea is based on matrix scrambling technique on elliptic curve. In this paper, we attempt to provide more secure encryption scheme by using the concept of Rubik's Cube. More precisely, we discuss a new technique of encrypting Amazigh alphabet based on scrambling method which is based on Rubik's Cube Principle. In fact, the original message is encrypted using elliptic curve cryptography and stored into data matrices. Then, the concept of Rubik's cube is applied to rows and columns of the encrypted matrix using scrambling method. In this paper, the security goals were enhanced using the concept of Rubik's Cube, which maintains the security on the communication channels by making it difficult for attacker.
The rest of this paper is organized as follows: the theoretical background, including elliptic curve cryptography and Rubik's Cube Principle is described in Section 2. Section 3 presents the proposed encryption scheme based on Rubik's cube, followed by simulation and results in section 4. Finally, the conclusion is presented in Section 5.

II. PRELIMINARY

A. *Elliptic Curve Cryptography*

ECC which was originally proposed by Victor Miller and Neal Koblitz [9] in 1985, is seen as a serious alternative to RSA with much shorter key size. The popularity of elliptic curve cryptography is due to the determination that is based on a harder mathematical problem than other cryptosystems such as RSA and ElGamal [10].

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 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the base point in the curve.

ECC consists of a few basic operations and rules that define how addition, subtraction, multiplication, and doubling are performed [11]. ECC point addition is described in Fig 1 and is defined as finding the line between two points, in this case P and Q. The result is a third point R. Point multiplication kP is accomplished by performing multiple additions. Thus, the elliptic curve discrete logarithm is the following given public key kP, find the private key k.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

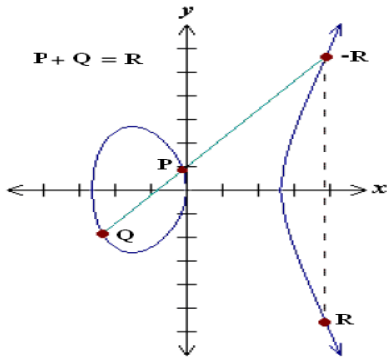

Fig 1. ECC Point Addition

- Point Addition

Consider two distinct points P and Q such that P = (x_1, y_1) and Q = (x_2, y_2)

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

$$x_3 = s^2 - x_1 - x_2 \bmod p$$

$$y_3 = -y_1 + s(x_1 - x_2) \bmod p$$

s is the slope of the line through P and Q.

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

- Point Subtraction

Consider two distinct points P and Q such that P = (x_1, y_1) and Q = (x_2, y_2)

Then P - Q = P + (-Q) where -Q = $(x_2, -y_2 \bmod p)$

- Point Doubling

Consider a point P such that P = (x_1, y_1), Where $y_1 \neq 0$.

Let Q = 2P where Q = (x_2, y_2) Then

$$x_2 = s^2 - 2x_1 \bmod p$$

$$y_2 = -y_1 + s(x_1 - x_2) \bmod p$$

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

B. Rubik's Cube

The Rubik's cube was created in 1974 for entertainment purposes. In 1992, the cube was used in cryptography by writing and jumbling the message on the cube. It was very new technique in cryptography and it has given rise to further new suggested techniques [12]. Many cryptography solutions have been implemented that use a cube [13, 14].

A Rubik's cube is built from 26 cubies, each able to make restricted rotations about a core of Rubik's cube. A face of Rubik's cube is a side as shown in Fig 2. Each face is divided into 9 facelets, where each of the 9 facelets is part of a distinct cubie.

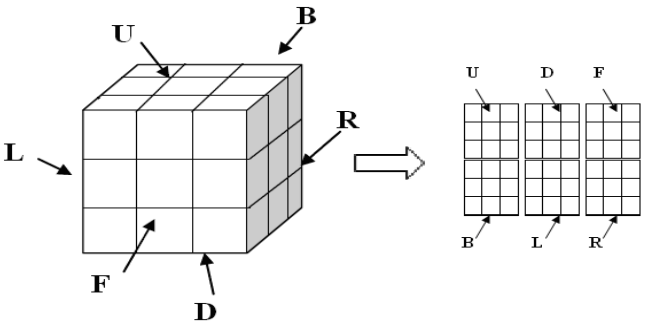

Fig 2. Representation of Rubik's Cube

F: Front face U: Up face D: Down face
B: Back face R: Right face L: Left face

The Rubik's cube has a strong mathematical structure: the set of its configurations is a subgroup of some finite permutation group. In this work, we extended this structure to boost the security of cryptosystem.

C. UTF-8 (Unicode Transformation Format-8)

UTF-8 is a variable-width encoding that may represent each character within the Unicode list. UTF-8 has become the dominant character secret writing for the WWW. UTF-8 is additionally more and more being used because the default character encoding in operative systems, programming languages, APIs, and software package applications. With the UTF-8 encoding, Unicode characters can be used. The Amazigh alphabet which is called "Tifinagh-IRCAM", adopted by the Royal Institute of the Amazigh Culture, was officially recognized by the International Organization of Standardization (ISO) as the basic multilingual plan [15]. The list of Amazigh characters and their corresponding Unicode assigned by ISO is shown in Table 1 and Table 2.

Table 1. Encoding of Amazigh alphabet (2Dx0-2Dx7)

	0	1	2	3	4	5	6	7
2D3x	ⴰ	ⴱ	ⴲ	ⴳ	ⴴ	ⴵ	ⴶ	ⴷ
2D4x	ⴸ	ⴹ	ⴺ	ⴻ	ⴼ	ⴽ	ⴾ	ⴿ
2D5x	ⵀ	ⵁ	ⵂ	ⵃ	ⵄ	ⵅ	ⵆ	ⵇ
2D6x	ⵈ	ⵉ	ⵊ	ⵋ	ⵌ	ⵍ		
2D7x								

Table 2. Encoding of Amazigh alphabet (2Dx8-2DxF)

	8	9	A	B	C	D	E	F
2D3x	ⵎ	ⵏ	ⵐ	ⵑ	ⵒ	ⵓ	ⵔ	ⵕ
2D4x	ⵖ	ⵗ	ⵘ	ⵙ	ⵚ	ⵛ	ⵜ	ⵝ
2D5x	ⵞ	ⵟ	ⵠ	ⵡ	ⵢ	ⵣ	ⵤ	ⵥ
2D6x								ⵯ
2D7x								

III. MAIN RESULT

The proposed algorithm is an attempt to present a new approach for encrypting and decrypting Amazigh characters based on ECC technique in such a way that the new approach can make use of Rubik's cube principle to achieve higher

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

speed with higher level of security.

The main idea is that the cipher text can be scrambled by rotating the rows and the columns of the magic cube faces.

1. Encryption Algorithm

The proposed encryption algorithm consists of the following steps:

Input: Source data file, say, tifinagh.txt

Output: Encrypted data file, say, Ciphertext.txt

Step 1. Read source file character by character. Then, transform all characters into points on elliptic curve.

Step 2. Choose a random number k and compute secure key $K=kP_B$. The obtained code is converted into binary form.

Step 3. Encrypt the sequence of points using ECC encryption formula to obtain the encrypted points. Then, arrange the result points into six sub-matrices.

Step 4. Mapping of the six sub-matrices on the faces of a magic cube.

Step 5. Mark the six faces as Up (U), Front (F), Right (R), Left (L), Down (D) and Back (B).

Step 6. Let b= (b_j), where j is bit position (LSB→MSB), which decides which transformation has to be performed on rows and columns of matrices. By rotating the rows and the columns of data matrix, the cipher text can be scrambled.

Step 7. The value of b is verified: If b=1, row transformation is applied on the sub-matrices that are attached to the faces of the magic cube F, U, B, D. If b=0, column transformation is to applied the sub-matrices that are attached to the faces of the magic cube F, R, B, L.

Step 8. Repeat step 7 for m of times. Then the final cipher text is created and encryption process is done.

Step 9. Convert the result points into corresponding characters and store them to Ciphertext.txt.

2. Decryption Algorithm

The decryption process follows the reverse process of encryption using secure key.

Input: Encrypted data file, say, Ciphertext.txt

Output: Decrypted data file, say, Decrypted.txt

Step 1. Read the encrypted file characters by character. Repeat 1.1 and 1.2

1.1. Transform each character into point on EC.

1.2. Repeat.

Step 2. Extract the first point P_1 and applies his secret key n_B to compute the secure key $K = n_BP_1$.

Step 3. Arrange the remaining points into six sub-matrices and Mapped on the faces of a magic cube.

Step 4. Let b= (b_j), where j is bit position (LSB→MSB), which decides which transformation has to be performed on rows and columns of matrices.

Step 5. Apply a reversal of rotation process to unscramble the encrypted points using Rubik's cube.

Step 6. By rotating the rows and the columns a number of times depending on the bit position selected, the encrypted sequence is created.

Step 7. Repeat step 5 for m of times. Then, decrypt the sequence of points using ECC technique.

Step 8. Convert all points into characters and store them to Decrypted.txt.

IV. IMPLEMENTATION AND RESULT

In this section, we present the results obtained from practical implementation of our algorithm in Java programming language [16]. A plaintext is represented as Text-document. The text file is taken as the input to the algorithm (Fig 3). A JAVA Swing application was developed using Netbeans 7.1 to implement this methodology. The user interface of the application is illustrated in Fig 4.

In our case, we consider the elliptic curve [1] given by the Weierstrass equation: $y^2= x^3 + 4x + 20 \bmod 29$.

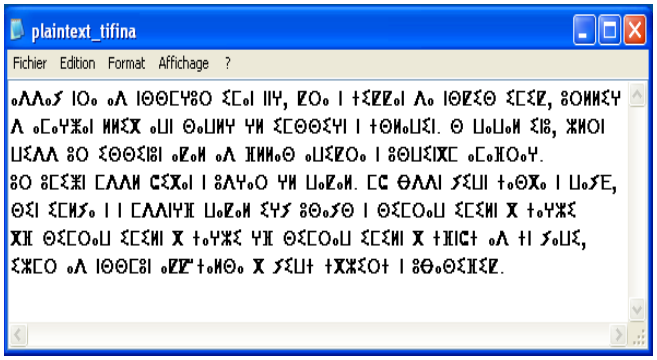

Fig 3. Text-File as Input of Algorithm

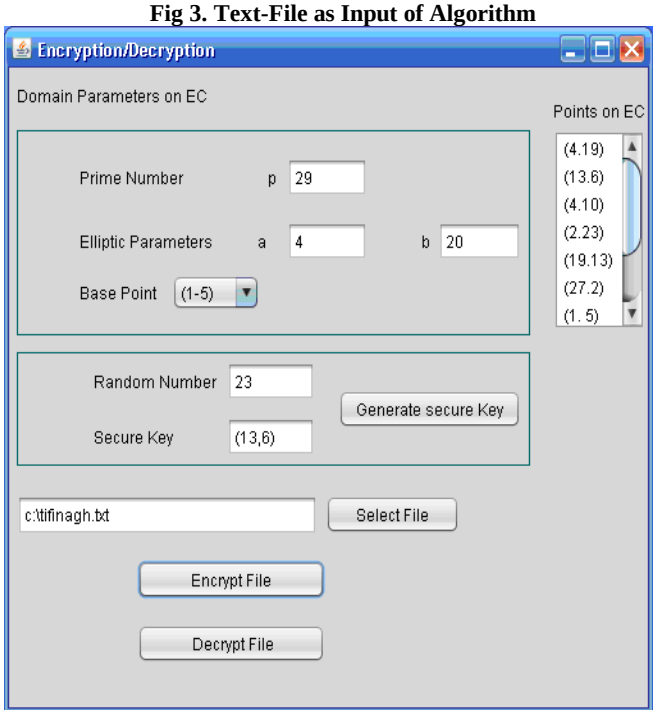

Fig 4. Encryption-Decryption Interface

The Encryption process is implemented on the loaded file and a new encrypted-file is generated. A file so generated is illustrated in Fig 5.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

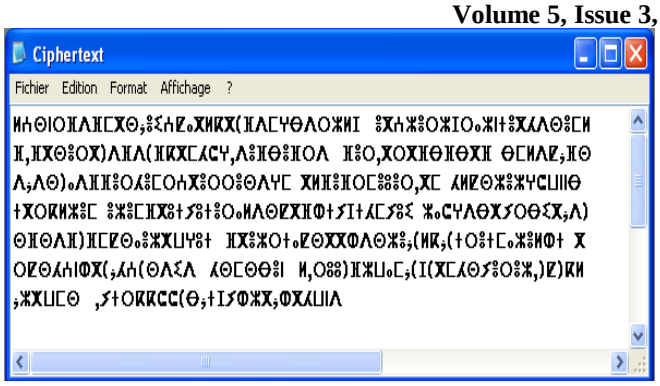

Fig 5. Ciphertext generated

The security offered by the proposed method, lies in the generation of secure key that is obtained by scalar point multiplication. Say, given a point P(x, y) on an EC, one needs to compute kP, where k is a random number chosen.

For attacking this cryptosystem, we should know the random number and we should know the private key that uses ECC. ECC's strength lies in solving the discrete logarithm problem for elliptic curves [17]. The random number to be sent to the receiver is encrypted using elliptic curve operation. In order to know the random number, we should to solve the discrete logarithm problem for elliptic curves. To enhance the security and robustness of data transfer, we have applied scrambling technique based on the concept of Rubik's Cube, which maintains the security on the communication channels by making it difficult for attacker. Hence, our proposed method provides the authenticity, integrity and non-repudiation to ensure better security.

V. CONCLUSION

This paper focuses on the encryption of Amazigh alphabet. After encrypting characters using ECC technique, we apply scrambling method to enhance security. In this approach the usage of random number selection firstly for generating secure key and, secondly the scrambling by selecting the operations on the cube to rotate it in appropriate direction, avoids the regularity in the resultant cipher text which is transformed from plaintext matrix; and hence improves the difficulty for decrypting.

Therefore, with all the above process implemented, we justify that the cipher is highly robust and secure. To date, we have modeled our technique for the encryption and decryption of text file as input. Further, it can be implemented for image and video encryption and decryption, and also in steganography applications involving encryption and decryption.

Future Enhancement: To achieve higher security proposed method will include more complicated process in matrix transformation as well as using traversing process.

ACKNOWLEDGMENT

The author would like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

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

[2] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communication ACM, 1978.

[3] S. Maria Celestin Vigila , K. Muneeswaran "Implementation of Text based Cryptosystem using Elliptic Curve Cryptography", IEEE, pp. 82-85, 2009.

[4] Sairam Natarajan, Manikandan Ganesan and Krishnan Ganesan , "A Novel Approach for Data Security Enhancement Using Multi Level Encryption scheme", International Journal of Computer Science and Information Technologies, Vol. 2 (1), 469-473, 2011.

[5] K.C.Shyamala Bai, Satyanarayana MV, Vijaya PA. "Variable Size Block Encryption using Dynamic-key Mechanism (VBEDM)", International Journal of Computer Applications, Vol 27, No.7, 2011.

[6] Suli Wu and Xiaofei Yi, Text Encryption Algorithm Based Cyclic Shift, the Smart Internet'2010. pp. 3483-3486, 2010.

[7] F.Amounas and E.H. El Kinani, An Elliptic Curve Cryptography Based on Matrix Scrambling Method, Proceedings of the JNS2, IEEE Xplore, pp 31-35, 2012.

[8] F.Amounas, E.H. El Kinani and M.Hajar, " A Matrix Approach for Information Security Based ECC using Mealy Machine and Fibonacci Q-Matrix ", International Journal of Engineering and Innovative Technology, vol 3, Issue 1, pp. 500-504, 2013.

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

[10] T. ElGamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, Advances in Cryptology, in: Proc. of CRYPTO 84, Springer Verlag, 1985.

[11] J. Lopez, R. Dahab, "An overview of elliptic curve cryptography", Technical report, IC-00-10, May 22, 2000.

[12] Alexander H.Frey, Jr. and David Sing master. "Handbook of Cubik Math", Enslow Publishers, 1982.

[13] Rajdeep Chowdhury and Saikat Ghosh,"Normalizer based encryption technique (NBET) using the proposed concept of rubicryption", International Journal of Information Technology and Knowledge Management , Volume 4, No. 1, pp. 77-80, 2011.

[14] Lini Abraham and Neenu Daniel, "Secure Image Encryption Algorithms: A Review", international journal of Scientific & Technology Research, Vol (2), Issue 4, 2013.

[15] L. Zenkouar, "L'écriture Amazighe Tifinaghe et Unicode", in Etudes et documents berbères. Paris (France). n° 22, pp. 175-192, 2004.

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

[17] Lawrence C.Washington. Elliptic Curves Number Theory and Cryptography. Discrete Mathematics and its Applications. Chapman and Hall/CRC, University of Maryland College Park, Maryland, U.S.A., 2 editions, 2008.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

AUTHOR BIOGRAPHY

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 at Faculty of Sciences and Technics, Errachidia, Morocco. Her research interests include elliptic curve and cryptography.

E-mail: F_amounas@yahoo.fr