International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 3 502 - 506

Efficient methodology for Encrypting Amazigh Alphabet using Modified Knapsack Algorithm based ECC

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

***Abstract*—**With the development of computers there has been strong demand for means to protect information and to provide security. Recently, security of Amazigh characters has become a growing field in which several research efforts have been made. In this context this paper provides a novel methodology for encrypting Amazigh characters which is the combination of ECC cryptosystem and Knapsack Algorithm through which each character of the message will be strongly encrypted. This paper demonstrates how to strengthen the encrypted message being sent by use of Knapsack algorithm so that only the intended recipient of the message is able to decipher the message. Encryption and decryption process are given in details with an example. A comparison of the proposed technique with existing algorithms has been done in encryption and decryption time.

Keywords- *Elliptic curve, Encryption, Decryption, Knapsack, Unicode, Amazigh character, Data Matrix.*

*****

I. INTRODUCTION

In recent years information security has become an important issue in data transmission. Encryption has come up as a solution, and plays an important role in information security system. Encryption is the process of encoding messages or information in such a way that only authorized users can read it. In an encryption algorithm the original message or information called plaintext is given as input to form cipher text. Decryption is the process of transforming cipher text into plaintext.

Elliptic curve cryptography (ECC) is an effective approach to protect privacy and security of information. Elliptic curve cryptography transforms a mathematical problem in to an applicable computer algorithm. Intractable problems are the center of public key cryptography and bring computationally demanding operations into a cryptosystem. Elliptic curve cryptography (ECC) is based upon the algebraic structure of elliptic curves over finite field. Elliptic curve cryptography is the most efficient public key encryption scheme based on elliptic curve concepts that can be used to create faster, smaller, and efficient cryptographic keys [1, 2]. In ECC, the operations such as 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 operations. As a result, researchers are engaged to develop different cryptographic techniques based ECC to enhance data security. In the paper [3], Static and dynamic mapping methods are explained. In static, the same alphanumeric characters from the different words are mapped onto the same x-y coordinates of the elliptic curve points. So, an intruder can easily interpret data with trial and error method. Hence the secrecy of data transmission by using this methodology is very low. In dynamic mapping, the alphanumeric characters are mapped dynamically on to the points of elliptic curve. Thus it is difficult for an intruder to guess which particular character is mapped to which point on elliptic curve. Further this approach was modified and instead of using matrix method in our previous paper [4]. This method is more complex and guarantees the security for the data and no intruder can hack it. Since this method avoids the regularity in the resultant encrypted text. Thus strengthens the crypto systems and provides better performance. Recently, the cryptographic methods for enhancing the security of Amazigh contents have gained high significance in the current era [5, 6]. This paper presents an efficient methodology of ECC encryption based on matrix approach along with Knapsack algorithm, which gives high security for the Unicode. The new innovation idea discusses enhancement of ECC technique using Modified Knapsack Algorithm. The rest of the paper is structured as follows. Section 2 gives detailed description of commonly employed security concepts and terminology. In Section 3 we present basic idea of elliptic curve cryptography and Knapsack Algorithm. Section 4 is devoted to proposed method. A detailed example is presented that outlines the working procedure of the proposed method in section 5. The performance and the security analysis of the proposed method are studied in section 6 and section 7. The paper is concluded in section 8.

II. CRYPTOGRAPHIC TERMINOLOGY

In this section, we introduce some basics security terminologies and concepts connected with cryptography. A message present in a clear form, which can be understood by any casual observer, is known as the plaintext. The encryption process converts the plaintext to a form that hides the meaning of the message from everyone except the valid communicating parties, and the result is known as the cipher text. Decryption is the inverse of encryption. The processes of encryption and decryption are controlled on a quantity known as the key, which is ideally known only to the valid users. Strength of a security scheme depends on the secrecy of the keys used.

A security protocol formally specifies a set of steps to be followed by communicating parties, so that the mutually desired security objectives are satisfied. The four main security objectives include:

- *Confidentiality*: This means that the secrecy of the data being exchanged by the communicating parties is maintained, i.e., no one other than the legitimate parties should know the content of the data being exchanged.
- Authentication: It should be possible for the receiver to ensure that the sender of the message is who he claims to be, and the message was sent by him.
- *Integrity*: It provides a means for the receiver of a message to verify that the message was not altered in transit. It checks originality of message.
- *Non-repudiation*: The sender of a message should not be able to falsely deny later that he sent the message, and this fact should be verifiable independently by an independent third-party without knowing too much about the content of the disputed message.

Security protocols realize the security objectives through the use of appropriate cryptographic algorithms. Security objectives thus provide trust on the Web. They are realized through the use of cryptographic algorithms which are divided into two categories depending on their characteristics: Symmetric algorithms and Asymmetric algorithms.

III. BACKGROUND DETAIL

A. *Elliptic Curve Cryptography*

Elliptic Curve Cryptography (ECC) was first introduced by Victor Miller and Neil Koblitz in 1985. The principal attraction of ECC compared to RSA is that it offers equal security for a far smaller key size, thereby reducing processing overhead [7]. The advantage of ECC over other public key cryptography techniques such as RSA is that the best known algorithm for solving ECDLP the underlying hard mathematical problem in ECC takes the fully exponential time and so far there is a lack of sub exponential attack on ECC. In fact, ECC bases its security on the hardness of computing discrete logarithms [8]. More precisely, the elliptic curve discrete logarithm problem (ECDLP) consists in recovering the value of multiplier α, given points P and Q= αP on an elliptic curve.

The dominant operation in ECC cryptographic schemes is scalar point multiplication. This is the operation which is the key to the use of elliptic curves for asymmetric cryptography the critical operation which is itself fairly simple, but whose inverse is very difficult. ECC arranges itself so that when you wish to perform operation, the cryptosystem should make easy encrypting a message with the public key, decrypting it with the private key, the operation you are performing is point multiplication [9].

Point multiplication is simply calculating αP, where α an integer and P is a point on the elliptic curve defined in the prime field. In point multiplication a point P on the elliptic curve is multiplied with a scalar α using elliptic curve equation to obtain another point Q on the same elliptic curve. i.e. αP=Q. Point multiplication is achieved by two basic elliptic curve operations [10].

- Point addition, adding two points M and N to obtain another point R: R = M + N.
- Point doubling, adding a point M to itself to obtain another point R: R = 2M.

This is shown in Figure 1 and Figure 2. Ω is the additive identity of the elliptic curve group. A negative of a point is the reflection of that point with respect to x-axis.

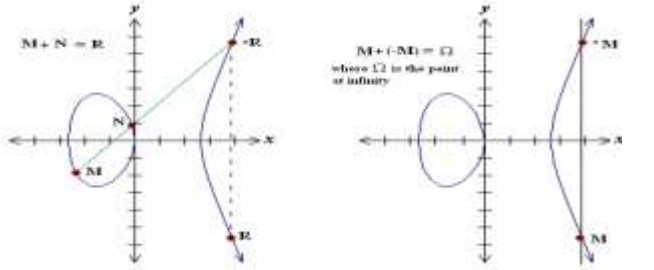

Figure 1. Point addition.

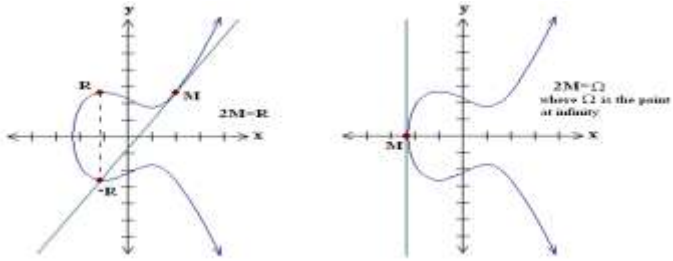

Figure 2. Point doubling.

B. *Knapsack Algorithm*

Knapsack problems are widely used to model solutions industrial problems such as public-key cryptography [11]. The knapsack problem selects the most useful items from a number of items given that the knapsack has a certain capacity. The 0-1 knapsack problem states that if there is a knapsack with a given capacity and a certain number of items that need to be put in the knapsack. Each item has a value and a weight associated with it. The knapsack problem selects the items that can be put in the knapsack so that the value of all the items is maximized and the weight does not increase the total capacity of the knapsack.

This can be denoted as

Maximize $\sum a_i x_i$

Subject to $\sum w_i x_i \leq W$

$$x_i = \begin{cases} 1 & \text{if the item is included in the knapsack.} \\ 0 & \text{if the item is not included in the knapsack.} \end{cases}$$

w_i is the weight associated with each item i.

W is the maximum capacity of the knapsack.

r is the number of items.

The subset sum problem is a special case of the knapsack problem. This problem finds a group of integers from a list vector V, where V = (a_1, a_2, a_3, … a_r), the subset of elements in the vector V which have a given sum S. It also determines if a vector X = (x_1, x_2, x_3, … x_r) exists where x_i element of {0, 1} so that V*X = S.

Here, n may be assumed as some random integer less than 10. Therefore, the knapsack representation of x_1 can be denoted as: $S(x_1) = \sum a_i x_i$ i=1.. r

Recently, most of encryption cryptosystems based Knapsack algorithm are proposed [12, 13]. Only one parameter, namely

the Knapsack vector alone needs to be kept secret. This paper extends this algorithm and attempts to generate a new vector with entries are points on elliptic curve.

C. Unicode

Unicode is most popular encoding scheme that has led to internationalization and localization of computer software. It implemented successfully in most recent technologies like xml, java programming language and Microsoft .net framework. Unicode has several character encoding forms represented as:
- UTF-8: Uses one byte to encode the characters. It is widely used in HTML and similar protocols over Internet.
- UTF-16: Uses two bytes to encode the most commonly used characters.
- UTF-32: It is the simplest encoding form, which is capable of representing every character as one number. It is a preferred encoding form for Unix Platforms.

In general, each Amazigh character is encoded with particular integer called code point [14]. The standard understanding of code points in the Unicode Standard is to refer code point as their numeric value assigned in hexadecimal, with a "U+" prefix.
With the encoding system, Unicode characters can be used on computer. Amazigh characters are encoded in the Unicode range U+2D30 to U+2D7F. In general, there are 55 defined characters [15, 16].

IV. PROPOSED METHODOLOGY

A. Modified Knapsack Algorithm

Knapsack requires that we generate a series of vectors called a_i. There are several ways of generating these vectors [17, 18, 19]. This paper sets out to contribute to knapsack algorithm by developing a new way to generate the vector with elements on elliptic curve. In our case, we shall take the first value as n, and subsequent values as multiples of n Say

$$a_i = n, n^2, n^3, \ldots, n^r \qquad 1 \le i \le r.$$

Therefore, we generate the knapsack vectors as follows:

$$R_i = R_1, R_2, R_3, \ldots, R_r \qquad 1 \le i \le r.$$

Where $R_i \in EC$.

Here, the corresponding points on elliptic curve which falls below the vectors will be taken. This stage makes the proposed method efficient.

B. Encryption Algorithm

The encryption is done through the following steps:

1. Input any sentence in Amazigh as a plain text.
2. Imbed the alphabetic characters into points on elliptic curve.
3. Create a data matrix of 3×m with entries as points on EC:

$$M = \begin{pmatrix} M_{11} & M_{12} & \ldots & M_{1m} \\ M_{21} & M_{22} & \ldots & M_{2m} \\ M_{31} & M_{32} & \ldots & M_{3m} \end{pmatrix}$$

4. Choose a random number k and compute a secure key $K=kP_B$.
5. Choose a non-singular matrix A of 3×3 and compute the product A*M. The result matrix is denoted Q.
6. Apply Modified Knapsack algorithm to each row of data matrix. Let b= (b_j), where j is bit position (LSB→MSB), which decides which operation has to be performed.
   If $b_j = 1$ then $D_i = Q_i + R_i$,
   If $b_j = 0$ then $D_i = Q_i - R_i$, with $R_i = a_i K$.
7. Convert each point into equivalent Unicode value. Then, transform the result blocks into binary form.
8. Arrange the first bit of all the blocks in the first row and second bits of all block in the second row and continuing this process arrange the remaining bit of all the blocks in the corresponding row of matrix.

Then the cipher text is (kP, C_i).

C. Decryption Algorithm

The decryption process involves converting the encrypted data back to its original form for the receiver's understanding. The steps in decryption algorithm are as follows:

1. Input the encrypted Text.
2. Extract the first block and compute the secure key.
3. Arrange de remaining bits into data matrix.
4. Convert each column into hex code. Then, transform the result Unicode value into point on elliptic curve. The obtained points are denoted D_i.
5. Apply the reverse process of Modified Knapsack algorithm. If $b_j = 1$ then $Q_i = D_i - R_i$, else $Q_i = D_i + R_i$ with $R_i = a_i K$.
6. Arrange these points into data matrix Q.
7. Apply the reversal matrix A^{-1} to recover the encrypted points.
8. Find the equivalent characters by decrypting each point.
9. Accumulate characters to form the secret message.

V. IMPLEMENTATION OF THE PROPOSED ALGORITHM

The following example will help understand the above mentioned encryption technique in a better manner.
In our case, the chosen elliptic curve is represented by the Weierstrass equation: $y^2 = x^3 + ax + b \bmod p$, with a=1, b=13 and p=53. The points on the elliptic curve over $E_{53}(1, 13)$ are shown below in Figure 3.

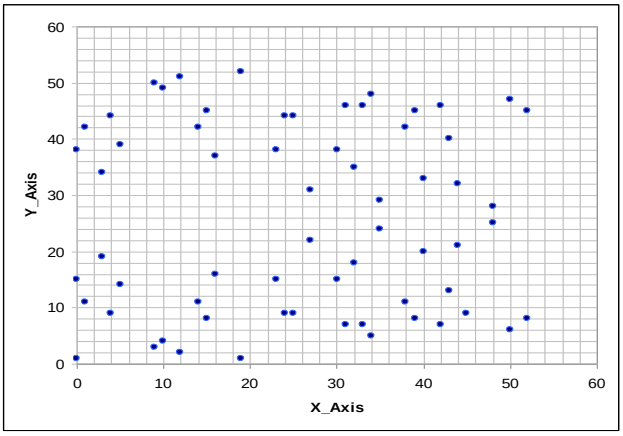

Figure 3. Set of points on EC

The non-singular matrix A is selected as

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

Consider the following plaintext:

That means

"Thank you IJRITCC"

After converting the alphabetic characters into points on elliptic curve, we get

(19, 52) (4, 9) (35, 24) (3, 34) (32, 35) (33, 7) (19,52) (0, 1) (23, 15) (33, 42) (33, 7) (23, 15) (23, 15) (19, 52) (33, 7)

Arranging this into 3*m matrix, we get

$$M=\begin{pmatrix}(19,52) & (4,9) & (35,24) & (3,34) & (32,35)\\ (33,7) & (19,52) & (0,1) & (23,15) & (33,42)\\ (33,7) & (23,15) & (23,15) & (19,52) & (33,7)\end{pmatrix}$$

After applying the non-singular matrix A, we get

$$Q=\begin{pmatrix}(24,9) & (27,22) & (12,2) & (9,50) & (31,7)\\ (16,37) & (5,39) & (40,33) & (15,45) & (48,28)\\ (15,8) & (27,31) & (16,37) & (12,51) & (35,29)\end{pmatrix}$$

Now, consider a random number k=23 and generate the knapsack vectors on elliptic curve as follows:

(15, 45) (19, 52) (45, 9) (42, 7) (12, 2) (3, 19) (35, 29) (24, 44), …

After applying the Modified Knapsack algorithm, we get

(14, 42) (31, 7) (50, 47) (25, 9) (48, 28) (10, 49) (3,19) (24, 44) (33, 7) (30, 15) (25, 44) (23, 15) (27, 22) (52, 8) (14, 11)

Converting the points into equivalent Unicode values as follows:

2D49 2D46 2D54 2D36 2D5A 2D4F 2D5F 2D3D 2D48 2D4B 2D26 2D3E 2D63 2D 3B 2D62

After converting hex code into binary form, we get data matrix C as

$$C=\begin{pmatrix}0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 1&1&1&0&1&1&1&0&1&1&0&0&1&0&1\\ 0&0&0&1&0&0&0&1&0&0&1&1&1&1&1\\ 0&0&1&1&1&0&1&1&0&0&0&1&0&1&0\\ 1&0&0&0&1&1&1&1&1&1&0&1&0&1&0\\ 0&1&1&1&0&1&1&1&0&0&1&1&0&0&0\\ 0&1&0&1&1&1&1&0&0&1&1&1&1&1&1\\ 1&0&0&0&0&1&1&1&0&1&0&0&1&1&1\end{pmatrix}$$

Therefore, the final cipher is shown as:

1101111111000000000000000111011101100101000100010011111001110110001010100011111101010011101110011000010111100111111100001110100111

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

VI. PERFORMANCE COMPARISON

This section is mainly focused on comparative analysis of our approach and existing methods [12, 20] at encryption and decryption time. The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from plaintext. It indicates the speed of encryption. The decryption time is considered the time that decryption algorithm takes to produce a plaintext from cipher text. Also, it indicates the speed of decryption. The simulation is performed using Maple software. The results for this comparison are shown in table 1.

TABLE 1. EXECUTION TIME (IN MILLISECOND) COMPARISON BETWEEN EXISTING ALGORITHMS WITH PROPOSED METHOD.

	Alg [12]	**Alg[20]**	**Our method**
Encryption time	27.3	25.4	13.03
Decryption time	33.6	30.11	19.3

Graphical representation of the above described table is shown in Figure 4 as follows:

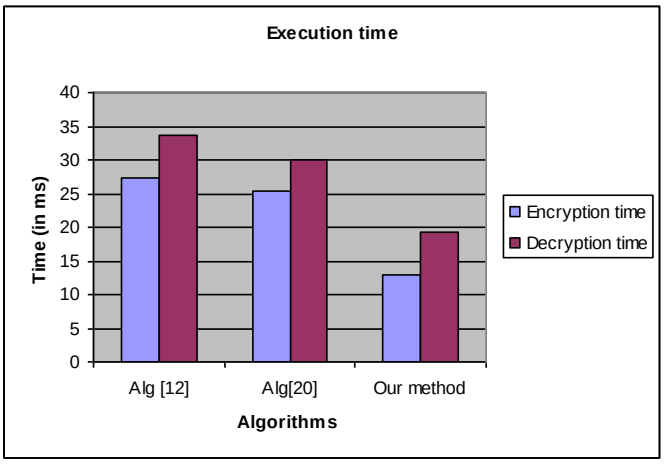

Figure 4. Comparison performance of various algorithms in term of time execution.

The results shows that time needed for the encryption/decryption process by proposed method is lesser than encryption/decryption time of compared algorithms. Encryption and decryption operation is performed very swiftly. So, we can say that our approach work faster than others methods.

VII. SECURITY ANALYSIS

This section provides the security analysis of the proposed method. In the proposed method, two kinds of attacks are considered.

Attack 1: an adversary attempts to derive the user's private key k from known public information: E, p, n, P, K, R and P_B (public key). This attack is not possible in the proposed scheme.

Proof: An adversary can not derive secure key from known public information: R and K, because ECDLP to obtain private key is difficult.

Attack 2: Suppose an adversary attempts to decrypt the message M from the cipher text without knowing the sender's private key.

Proof: In attack 2, suppose an adversary attempts to decrypt the original message M then he has to know two things for applying the reverse knapsack, 1) the knapsack vector generation series using points on elliptic curve and 2) n value for generating the knapsack values. These two things are unique for every user. So, the adversary's attempt of applying the reverse knapsack will not work. So, attack 2 is not possible in the proposed method.

VIII. CONCLUSION

In this methodology, the usage of random number selection firstly for generating secure key and, secondly for generating Knapsack vectors for scrambling the mapping points, avoids the regularity in the resultant cipher text which is transformed from plain text matrix, and hence improves the difficulty for decrypting. As result, I find that the proposed method is a very strong and it cannot be broken by any cryptanalytic attack. Further, the results in the performance comparison table showed that the proposed method has a very good performance compared to other algorithms in term of execution time.

The work done is a first step for several perspectives. We try to improve our method by changing the chosen number by another random number like Fibonacci numbers or Armstrong numbers for a better representation of knapsack vectors. Furthermore, the modified cryptosystem can be made till better by enhancing ECC algorithm.

REFERENCES

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

[2] 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, 2014, pp. 103-106.

[3] O. Srinivasa Rao and S. Pallam Setty, "Efficient Mapping methods for Elliptic Curve Cryptosystems" , International Journal of Engineering Science and Technology, Vol. 2, No. 8, 2010, pp. 3651-3656.

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

[5] Fatima Amounas, "Enhancing Robustness of Encrypting Amazigh Alphabet based ECC using Scrambling Method', International Journal of Engineering and Innovative Technology, Vol 5, Issue 3, 2015, pp. 138-142.

[6] Ali Rachidi and Mustapha Eddahibi, "An Amazigh Geo-cultural Information System", International Journal of Emerging Technology and Advanced Engineering, Vol 4, Issue 8, 2014, pp.10-14.

[7] Rahat Afreen and S.C. Mehrotra, "A Review on Elliptic curve Cryptography for Embedded Systems", International Journal of Computer Science and Information Technology, Vol. 3, No. 3, 2011, pp.84-103.

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

[9] Andrej Dujella, "Applications of elliptic curves in public key cryptography", Basque Center for Applied Mathematics and Universidad del Pais Vasco / Euskal HerrikoUnibertsitatea, Bilbao, 2011.

[10] Shabnoor Qureshi and Somesh Dewangan, "Prospective Utilization of Elliptic Curve Cryptography for Security: Authentication, Encryption and Decryption", OSR Journal of Computer Engineering, Vol. 16, Issue 3, 2014, pp.31-35.

[11] Jitendra Sharma and Prashant Shukla, "ECC Cipher Processor Based On Knapsack Algorithm", National Conference on Emerging Trends in Electrical, Instrumentation & Communication Engineering, Control Theory and Informatics, Vol.3, No.2, 2013, pp. 53-57.

[12] R. Rajaram, M. Amutha Prabakar, M. Indra Devi, and M. Suguna, "Knapsack Based ECC Encryption and Decryption", International Journal of Network Security, Vol. 9, No. 3, 2009, pp. 218-226.

[13] Ashish Agarwal, "Encrypting Messages using the Merkle-Hellman Knapsack Cryptosystem", International Journal of Computer Science and Network Security, Vol.11, No.5, 2011, pp.12-14.

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

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

[16] Hassain Sadki, Fatima Amounas and El Hassan El Kinani, "A Novel Approach of Amazigh Text Steganography based Elliptic Curve", International Journal of Information & Network Security, Vol.3, No.2, 2014, pp. 83-91.

[17] Khushboo Thakur, B. P. Tripathi and B. K. Sharma, "Companion Matrix Encryption Using the Knapsack Problem Based on Elgamal" , Journal of Computer and Mathematical Sciences, Vol.6, No 8, 2015, pp. 416-422.

[18] Mythrigowda Y.P1, Leelavathi G, "Implementation of ECC Using Knapsack Algorithm", International Journal for Research in Applied Science & Engineering, Vol.3, special Issue-II, 2015, pp. 7-11.

[19] Shinsuke Hamasho, Yasuyuki Murakami, Masao Kasahara, "A Systematic Encryption Algorithm for Knapsack Scheme Using Random Sequence", Journal of Communications and Information Sciences, Vol. 3, No. 3, 2013.

[20] Megha Kolhekar and Anita Jadhav, "Implementation of elliptic curve cryptography on text and image", International Journal of Enterprise Computing and Business Systems, Vol. 1, july 2011, Issue 2.