**International Journal of Electrical and Computer Engineering (IJECE)**
Vol. 13, No. 2, April 2023, pp. 1734~1743
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i2.pp1734-1743

# Design a cryptosystem using elliptic curves cryptography and Vigenère symmetry key

**Mai Manh Trung[1,2], Le Phe Do[2], Do Trung Tuan[3], Nguyen Van Tanh[4], Ngo Quang Tri[5]**

[1]Department of Information System, Faculty of Information Technology, University of Economics Technology for Industries, Hanoi City, Vietnam
[2]Department of Computer Science, Faculty of Information Technology, University of Engineering and Technology, Vietnam National University, Hanoi City, Vietnam
[3]Department of Computational Science, Faculty of Information Technology, University of Science, Vietnam National University, Hanoi City, Vietnam
[4]Faculty of Applied Sciences, International School, Vietnam National University, Hanoi City, Vietnam
[5]Department of Computer Network and Multimedia Technology, Faculty of Information Technology, University of Economics Technology for Industries, Hanoi City, Vietnam

**Article Info**

***Article history:***

Received Dec 5, 2021
Revised Oct 1, 2022
Accepted Oct 29, 2022

***Keywords:***

Decryption
Elliptic curves cryptography
Generating point
Symmetry key
Vigenère cryptography

## ABSTRACT

In this paper describes the basic idea of elliptic curve cryptography (ECC) as well as Vigenère symmetry key. Elliptic curve arithmetic can be used to develop elliptic curve coding schemes, including key exchange, encryption, and digital signature. The main attraction of elliptic curve cryptography compared to Rivest, Shamir, Adleman (RSA) is that it provides equivalent security for a smaller key size, which reduces processing costs. From the theorical basic, we proposed a cryptosystem using elliptic curves and Vigenère cryptography. We proposed and implemented our encryption algorithm in an integrated development environment named visual studio 2019 to design a safe, secure, and effective cryptosystem.

***Corresponding Author:***

Mai Manh Trung
Department of Computer Science, Faculty of Information Technology, University of Engineering and Technology, Vietnam National University
Hanoi, 144 Xuan Thuy Street, Cau Giay District, Hanoi City, Vietnam
Email: mmtrung@uneti.edu.vn

## 1. INTRODUCTION

In lightweight primitive cipher there are four main directions which are i) lightweight block cipher, ii) lightweight stream cipher, iii) hash function, iv) elliptic curve cryptography in addition there are v) message authentication. Elliptic curve cryptography (ECC) is one of the most well-known cryptographies with wide use in human life. Many companies in the America United States such as CloudFlare applied the ECC widely to secure the hypertext transfer protocol secure (HTTPS) connections between them and customers as well as the data converting channels in their data centers.

In Vietnam, the ECC has taken an important role in many security solutions which implemented in companies, banks and governmental agencies in recent year. In 15th December 2017, the Vietnam Ministry of Information and Communication introduced Circular No 39/2017/TTBTTTT contained the list of technical standards of information technology applied in governmental agencies. In this article, the ECC was a security standard which was encouraged to be applied.

Lenstra [1], proposed a cryptographic algorithm using elliptic curve for dividing composite number into prime numbers. This algorithm had rapid calculate speed which run-time complexity is below exponential big O function. This algorithm was the third fastest in set of integer factorization algorithms whom speed was lower than polynomial sieve algorithm and general number field sieve algorithm.

Elliptic curve cryptography system is used in dynamic secure routing link detection [2], in an effective and secure radio frequency identification (RFID) authentication [3], in wireless sensor networks using the number theoretic to transform [4], with [5] used elliptic curve cipher to encode the image. The image is represented by points on the curve. according to the research team [6], [7], they have researched enhancing security in text messages using matrix based mapping and El Gamal method in ECC. With the research group Tawalbeh *et al.* [8] and Abusukhon *et al.* [9] use of elliptic curve cryptography for multimedia encryption, they have split the video into frames and use points on the curve to encode for good results. According to [10], [11] gave mapping methods and blind digital image watermarking using Hénon chaotic map on ECC. ECC also applies parallel encryption, multi-point encryption at the same time [12], with researching [13] is using fuzzy set to evaluate the security on ECC. According to [8] based on elliptic curve cryptography to analysis of a secure communication for healthcare system using wearable devices. A new study of the curve is low-area point multiplication architecture and secured data storage using deduplication in cloud computing for ECC [14], [15]. ECC are also used in big data analysis [16]. In this researching [17], they define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing. In which, with the researching [18], a new cryptographic system is built by using the elliptic curve cryptography based on square matrices to achieve a secure communication between two parties.

In set of cryptographic studies, in 1985, the elliptic curve cryptography were first introduced in the paper “use of elliptic curves in cryptography” by Miller [19]. Koblitz [20] proposed some technical properties of the elliptic curve in the paper “elliptic curve cryptosystem”. After that, the EC were continued to be improved about theoretical base and applied in real security solutions. The EC was also standardized and became a crucial part of many security standards.

Cryptographies can be classified into 2 types by distribution of key. One type is symmetric key and the other is asymmetric key. The ECC uses asymmetric key [21] which might have public keys. In addition, an image cryptographic mechanism by public key of the EEC was proposed [22]. In this mechanism, image is mapped by matrix of pixels. In the other hand, the cryptosystem using symmetric keys allow a symmetric key to be used in both encrypt and decrypt process [23], [24]. Thus, a cryptographic solution to encrypt passages using Vietnamese language. This solution uses the ECC and a symmetric key which consist of a value [25]. In this paper, we also propose a cryptosystem using the EEC and a symmetric key. However, this symmetric key consists of more than one value because it helps the cryptosystem to enhance security and prevent the sniffing attacks effectively.

## 2. MATHEMATICAL THEOREM OF THE ELLIPTIC CURVE

The Formula (1) shows the model of almost elliptic curves equation in many researches:

$$y^2 = x^3 + Ax + B\ (mod\ p) \tag{1}$$

In (1), character *A* and character *B* are two constants, character *x*, character *y*, character *A* and character *B* are values which belong to a specific field such as field of real number (R), rational number (Q) and complex number (C). The specific field might be a finite set $Fq$ with $q=p^n$. Character *p* is a prime number and character *n* is a number with $n\geq1$. If $a, b \in$ field *K*, there is declaration that an elliptic curve is defined in field *K*. If a point in Cartesian coordinate system with numerical coordinates $(x, y) \in K$, this point would lie on an elliptic curve and be defined as point *K* – Finite. The (2) shows the elliptic curve is defined by model of general Weierstrass equation.

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

In (2), $a_1, ..., a_6$ are constants. Formula (2) can be defined if characteristic *chap(K)* of field *K* is equal to 2 or 3. If *chap(K)* is not equal to 2, formula (2) can be redefined by:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{{a_1}^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{{a_3}^2}{4} + a_6\right)$$

Also, formula (2) can be redefined by:

$${y_1}^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

In this above equation, $y_1=y+a_1x/2+a_3/2$ which $a_2'$, $a_4'$, $a_6'$ are constants. If *chap(K)* of field *K* is not equal to 3, we can replace $x_1=x+a_2'/3$ and the result is shown in:

$$y_1{}^2 = x_1{}^3 + Ax + B,$$

In this equation, character $A$ and character $B$ are specific constants. Curve (1) has determinant: $\Delta = 4A^3 + 27B^2$. We default all elliptic curves in our paper has $\Delta \neq 0$.

### 2.1. The addition of points in the Curve

$P_1(x_1, y_1)$ *và* $P_2(x_2, y_2)$ are 2 points lie on an elliptic curve E. The addition of these points is defined in (3):

$$P_3(x_3, y_3) = P_1(x_1, y_1) + P_2(x_2, y_2) \tag{3}$$

In (3), $P_3(x_3, y_3)$=-$P'_3(x_3, y'_3)$, point $P'_3(x_3, y'_3)$ is intersection of E and line which contains both two points $P_1$ and $P_2$ as in the Figure 1. Because 2 points $P_3(x_3, y_3)$ and -$P'_3(x_3, y'_3)$ lie on the curve E, $(x_3, y_3)$ and $(x_3, y'_3)$ must be compatible to (2):

If $x_1$=$x_2$ and $y_1$=- $y_2$, we define $P_1$+$P_2$=∞ (∞ is infinite point). In opposite condition, $P_1$+$P_2$=($x_3$, $y_3$) ∈ E which $x_3$=$\beta^2$-$x_1$–$x_2$, $y_3$=$\beta(x_1$–$x_3)$–$y_1$, and the value of $\beta$ is calculated in:

$$\beta = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + a}{2y_1}, \text{if } P_1 = P_2 \end{cases}$$

If $P_1 \neq P_2$ , $x_1 \neq x_2$, the value of $x_3$ and $y_3$ is calculated in (4):

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \end{cases} \tag{4}$$

If $P_1 = P_2$, $x_1 = x_2$, the value of $x_3$ and $y_3$ is calculated in (5):

$$\begin{cases} x_3 = \left(\frac{3x_1{}^2 + A}{2y_1}\right)^2 - 2x_1 \\ y_3 = \left(\frac{3x_1{}^2 + A}{2y_1}\right)(x_1 - x_3) - y_1 \end{cases} \tag{5}$$

It is noted that 2 points ($x_3$, $y_3$) and ($x_3$, -$y_3$) lie on the Curve E. In the Cartesian coordinate system, both 3 points ($x_1$, $y_1$), ($x_2$, $y_2$) and ($x_3$, -$y_3$) also lie on one line. In addition, we define: the result of the addition between a point and an infinite point is this point. The below equation shows our definition.

$$P_1 + \infty = \infty + P_1 = P_1.$$

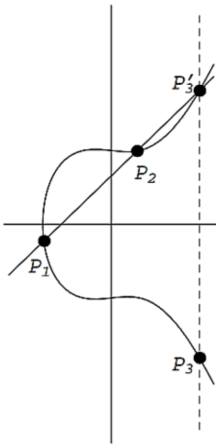


Figure 1. The addition in elliptic curve

### 2.2. The scalar multiplication of points in elliptic curve

The scalar multiplication of point $P$ in the curve $E$ is thought of as a k-times repeated addition as the below illustration. It is noted that $k \in N\backslash\{0\}$:

$$P \rightarrow kP = \underbrace{P + P + \cdots + P}_{k\ times} = Q$$

In elliptic curve, the multiplication between a point in the Cartesian coordinate system and a constant is not as simple as the normal imagine that it is the multiplication between each coordinate of this point and this constant. As above indication, the multiplication is the thought of as repeated addition. For example, to find result of the multiplication 3P, we calculate 2P by finding result of the addition between P and P. As indication in Part 2.1, we draw a segment line from P to P and this line becomes tangent of the curve. Meanwhile, the intersection point between this line and the curve is minus 2P (-2P). 2P is the point that is symmetric to minus 2P throughout coordinate horizontal axis. We continue to draw a segment line from 2P and P and find an intersection point minus 3P. We find the point, which is symmetric to -3P throughout coordinate horizontal axis. This point is 3P. Figure 2 describes the multiplication in the elliptic curve.

With this calculation as below mention, we can calculate easily the multiplication between k and P. However, when we have result of the multiplication k*P, it is impossible to define k and P by normal division. In term of security, this phenomenon can be applied to a cryptosystem using asymmetric key.

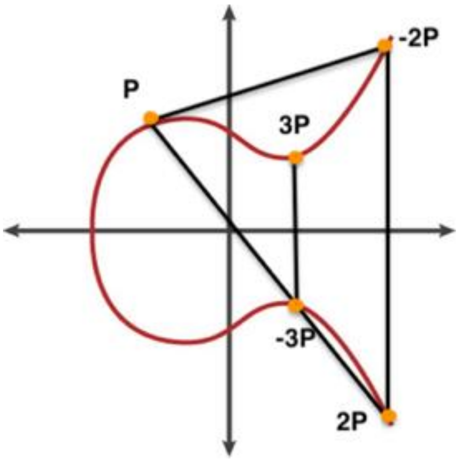


Figure 2. The multiplication in the elliptic curve

## 3. PROPOSAL OF CRYPTOSYSTEM USING ELLIPTIC CURVE AND VIGENERE KEY

We call our proposal Vigenère elliptic curve cryptosystem (VECC), all components of cryptosystem including $(\mathcal{P}, \mathcal{C}, \mathcal{E}, \mathcal{D}, \mathcal{K})$, where $\mathcal{P}$ is plain text; $\mathcal{C}$ is cipher text; $\mathcal{E}$ is encrypt function; $\mathcal{D}$ is decrypt function; $\mathcal{K}$ is key. It is noted that $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_m$, and $\mathcal{K}$ is a string.

### 3.1. Encryption process

Step 1: Input the elliptic curve parameter indicated in (1).
Step 2: Define the sum of points and the point generating value m of the elliptic curve.
Step 3: Find all points in the curve represent all characters in the Set $Z_m$. Find ordered list of points which each point represents each character in the plain text. We call these points: plain point.
Step 4: Select a random key is n characters in the set $Z_m$.
Step 5: Define encrypt function:

$$\mathcal{C}_i = \mathcal{E}(\mathcal{P}_i) = [(\mathcal{P}_i + \mathcal{K}_j)\ mod\ m]P \quad (6)$$

Here, $i = 0, \ldots, l-1$ ($l$ is the plaintext length), $j = 0, \ldots, h-1$ ($h$ is the key length).

The result of this process is ordered list of points which each point represents each character in the cipher text. We call these points: cipher point. Finally, we use the map between point and character defined in step 2 to find each character in cipher text from each cipher point. The final result is string of cipher text.

### 3.2. Decryption process

Step 1: Use parameter and generating point of the curve E as the encryption process.
Step 2: Convert each character of cipher text to cipher point.
Step 3: Input key. The value of key must be equal to this of inputted key in the encryption process.
Step 4: Define decryption process

$$P_i = D(C_i) = [(C_i - K_j) \ mod \ m]P \tag{7}$$

Here, $i = 0, \ldots, l - 1$ ($l$ is the ciphertext length), $j = 0, \ldots, h - 1$ ($h$ is the key length).

The result of this process is ordered list of plain points. We use the map between point and character defined in step 2 of encrypt process to find all characters in plain text and define string of plain text. Parameters in (6), (7): $P_i$ is position of character in plain text, $C_i$ is position of character in cipher text, $K_i$ is position of character in key. $M$ is sum of points in the curve (1), and P is generating point of the elliptic curve.

## 4. AN EXAMPLE OF OUR PROPOSAL

The proposal elliptic curve equation is: $y^2 = x^3 + x - 2$ (mod 19). A and B are two participants of transmission using our proposed cryptosystem. A sends a plain text: "MYCOMPUTER" to B, this text is considered as the input text. A uses the VECC to encrypt the text to secure data during transmission. The encrypt process is described below:

### 4.1. Encryption process

Step 1: Input parameters of the elliptic curve: $A = 1, B = -2,$ and $p = 19.$
Step 2: Define the sum of points in the elliptic curve: m=28 points. The generating point is P(0,6).
Step 3: Find all points in the curve represent all characters in the set $Z_{28}$. Table 1 presentations the point of the curve corresponding to the character in the English alphabet.
Step 4: We select the key: $K = UNETI.$

The key selection consists of n characters and is chosen at random. Here, the research team chooses the illustrated key as UNETI. Each key character corresponds to 1 point on the curve. They are presented as Table 2.

Table 1. Character is represented by point in the curve from point $P$

| Point, Character | Point, Character | Point, Character | Point, Character |
|---|---|---|---|
| (0, 6) | (7, 14) | (4, 3) | (12, 3) |
| A a | B b | C c | D d |
| (13, 2) | (17, 8) | (3, 16) | (6, 12) |
| E e | F f | G g | H h |
| (14, 18) | (10, 18) | (15, 14) | (8, 10) |
| I i | J j | K k | L l |
| (16, 5) | (1, 0) | (16, 14) | (8, 9) |
| M m | N n | O o | P p |
| (15, 5) | (10, 1) | (14, 1) | (6, 7) |
| Q q | R r | S s | T t |
| (3, 3) | (17, 11) | (13, 17) | (12, 16) |
| U u | V v | W w | X x |
| (4, 16) | (7, 5) | (0, 13) | |
| Y y | Z z | @ | ∞ |

Table 2. The points in the curve represent characters of key

| U | N | E | T | I |
|---|---|---|---|---|
| (3, 3) | (1, 0) | (13, 2) | (6, 7) | (14, 18) |

Step 5: Find all characters of cipher text by using (6).

We use Table 1 to find each plain point represents each character of plain text. Each point on this curve corresponds to a corresponding character. The result is shown in Table 3.

- Character "M": We calculate Pi of "M": 13P; The represented point is point (16, 5);
  We calculate $C_0 = [(13 + 21) \ mod \ 28]P = 6P = 6(0,6) = (17, 8)$ represent to character F.
- Character "Y": We calculate Pi of "Y" là 25P; The represented point is point (4, 16);
  We calculate $C_1 = [(25 + 14) \ mod \ 28]P = 11P = 11(0,6) = (15, 14)$ represent to character K.

- We do the same with the other characters which find the Plain cryptographic points and generate the characters of cipher text. The result is shown in Table 4.

The result of encrypt process is a cipher text: FKHGVIGYY@. A sends this cipher text to B in channel.

Table 3. Plain cryptographic points in the curve

| Plain text | M | Y | C | O | M | P | U | T | E | R |
|---|---|---|---|---|---|---|---|---|---|---|
| Plain points | (16, 5) | (4, 16) | (4, 3) | (16, 14) | (16, 5) | (8, 9) | (3, 3) | (6, 7) | (13, 2) | (10, 1) |

Table 4. Table of characters after encryption process

| Plain text | Plain points | Cipher points | Cipher text |
|---|---|---|---|
| M | (16, 5) | (17, 8) | F |
| Y | (4, 16) | (15, 14) | K |
| C | (4, 3) | (6, 2) | H |
| O | (16, 14) | (3, 16) | G |
| M | (16, 5) | (17, 11) | V |
| P | (8, 9) | (14, 18) | I |
| U | (3, 3) | (3, 16) | G |
| T | (6, 7) | (4, 16) | Y |
| E | (13, 2) | (4, 16) | Y |
| R | (10, 1) | (0, 13) | @ |

### 4.2. Decryption process

Step 1: Use parameters of the curve $E$: $A = 1, B = -2$, and $p = 19$ and generating point (0, 6).
Step 2: Convert each character of cipher text to cipher point. The result is shown in Table 5.
Step 3: Input key: UNETI.
Step 4: Find all characters of plain text by using (7).

- Character “F” of cipher text is represented by point (17, 8) which is equal to 6P.
  We calculate $P_0 = D(C_i) = [(6 - 21)\ mod\ 28]P = 13P = 13(0,6) = (16,5)$ represented by character M.
- Character “K” of cipher text is represented by point (15, 14) which is equal to 6P.
  We calculate $P_1 = D(C_i) = [(11 - 14)\ mod\ 28]P = 25P = 25(0,6) = (4,16)$ represented by character Y.

To find the final ciphertext. We do the same step in the other characters of cipher text. The result is each character of plain text shown in Table 6. The final output is the plain text that A encrypts in encryption process: MYCOMPUTER.

Table 5. Characters of cipher text is represented by points in the curve

| Cipher text | F | K | H | G | V | I | G | Y | Y | @ |
|---|---|---|---|---|---|---|---|---|---|---|
| Cipher points | (17, 8) | (15, 14) | (6, 2) | (3, 16) | (17, 11) | (14, 18) | (3, 16) | (4, 16) | (4, 16) | (0, 13) |

Table 6. Result of decrypt process

| Cipher text | Cipher point | Plain point | Plain text |
|---|---|---|---|
| F | (17, 8) | (16, 5) | M |
| K | (15, 14) | (4, 16) | Y |
| H | (6, 2) | (4, 3) | C |
| G | (3, 16) | (16, 14) | O |
| V | (17, 11) | (16, 5) | M |
| I | (14, 18) | (8, 9) | P |
| G | (3, 16) | (3, 3) | U |
| Y | (4, 16) | (6, 7) | T |
| Y | (4, 16) | (13, 2) | E |
| @ | (0, 13) | (10, 1) | R |

## 5. EVALUATION OF THE ALGORITHM'S SECURITY

With the curve cipher algorithm presented above, the security is based on the parameters of the curve. With the input parameters of (1) are *A*, *B*, p. With these different parameters, the total score will be different, accompanied by a different score. In addition, among these found points, it is necessary to find the point generator to generate the remaining points. Particularly with this factor, it will be difficult for the cryptanalyst to break the code because it has to try n fields in m cases. Next, the security of the proposed cryptosystem depends on the key because the cryptanalyst does not know whether this is a single key or a compound key, a numeric key or a string. Finally, the level of encryption is also based on assigning points to characters, these characters can be arranged or randomly set up by the designer from scratch.

RSA cryptography is a widely used public-key algorithm, but cryptography based on ECC can replace RSA for a higher level of security and processing speed. The advantage of ECC is that it uses a key of smaller length than RSA as mentioned in Table 7 that increases the processing speed significantly, because the number of operations used to encode and decode is less. and lower computational capabilities are required. Therefore, they increase speed but decrease energy used in encoding and decoding. The comparison of the key sizes between conventional and public-key encryption at the same level of security is displayed in Table 8.

Table 7. Key length for public-key and symmetric-key cryptography [26]

| Symmetric-key | ECC | RSA/DLP |
|---|---|---|
| 64 bit | 128 bit | 700 bit |
| 80 bit | 160 bit | 1024 bit |
| 128 bit | 256 bit | 2048-3072 bit |

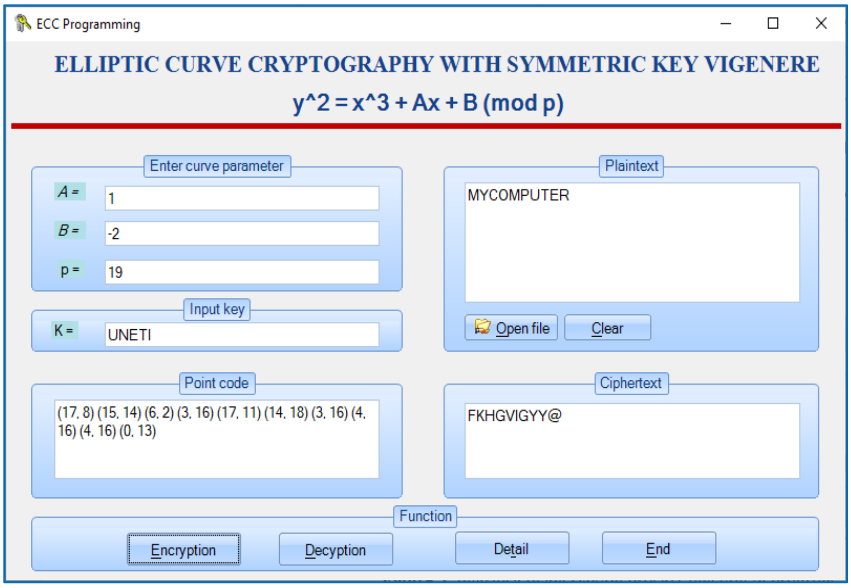
Table 8. Comparison between RSA and ECC key sizes at the same security level

| Time it takes Key (unit: year) | Key size |  | Key size ratio RSA: ECC |
|---|---|---|---|
|  | RSA/DSA | ECC |  |
| $10^4$ | 512 | 106 | 5:1 |
| $10^8$ | 768 | 132 | 6:1 |
| $10^{11}$ | 1024 | 160 | 7:1 |
| $10^{20}$ | 2048 | 210 | 10:1 |
| $10^{78}$ | 21000 | 600 | 35:1 |

## 6. INSTALLATION OF OUR PROPOSAL IN REAL DEVICE

Our cryptosystem was installed in a program run in a personal computer. Information about hardware: CPU Intel(R) Core(TM) i5, 2.5 GHZ; memory size of RAM: 4 GB and memory size of hard disk drive (HDD): 500 GB; Information about software: operating system: Windows 10. Our proposal run in platform of integrated development environment: Visual studio NET–2019.

This program launched encryption and decryption process in the elliptic curve was created by C# programming language of visual studio NET-2019. The interface of this program with each process was shown in Figures 3 and 4. We select the plain text and parameters of our describe part 4 about algorithm as the input value and the result of each process in the program is accurate and compatible to our indication in part 4.



ELLIPTIC CURVE CRYPTOGRAPHY WITH SYMMETRIC KEY VIGENERE

y^2 = x^3 + Ax + B (mod p)

A = 1

B = -2

p = 19

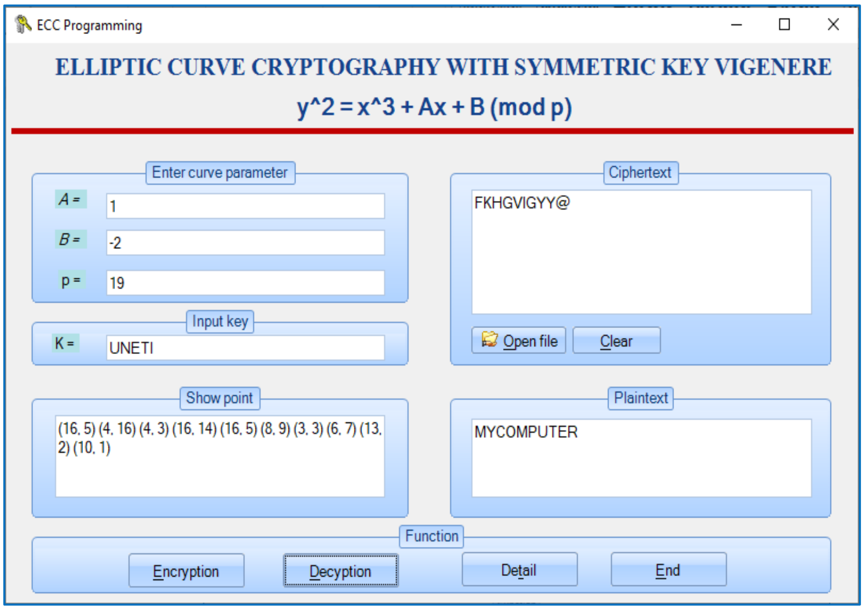
K = UNETI

Point code: (17, 8) (15, 14) (6, 2) (3, 16) (17, 11) (14, 18) (3, 16) (4, 16) (4, 16) (0, 13)

Plaintext: MYCOMPUTER

Ciphertext: FKHGVIGYY@

Figure 3. Interface of encryption process function in program



ECC Programming

ELLIPTIC CURVE CRYPTOGRAPHY WITH SYMMETRIC KEY VIGENERE

y^2 = x^3 + Ax + B (mod p)

Enter curve parameter

A = 1

B = -2

p = 19

Input key

K = UNETI

Show point

(16, 5) (4, 16) (4, 3) (16, 14) (16, 5) (8, 9) (3, 3) (6, 7) (13, 2) (10, 1)

Ciphertext

FKHGVIGYY@

Plaintext

MYCOMPUTER

Figure 4. Interface of decryption process function in program

## 7. CONCLUSION

The elliptic curve has important role in cryptography so our research team proposed a cryptosystem using the elliptic curve and the Vigenère symmetric key. Our proposed cryptosystem called VECC. The secure level of this algorithm depends on the parameters of the curve, the point on the curve and the length of key K. We also implemented the algorithm and installed it in a program coded by C# programming language. The output value in encryption and decryption process during running this program was accurate. In the future, we will continue to develop VECC to enhance its effectiveness for encrypting and decrypting passages with a variety of different languages.

## REFERENCES

[1] H. W. Lenstra, “Factoring integers with elliptic curves,” *The Annals of Mathematics*, vol. 126, no. 3, pp. 649–673, Nov. 1987, doi: 10.2307/1971363.

[2] S. S. Priya and M. Mohanraj, “A review on secure elliptic curve cryptography (ECC) and dynamic secure routing link path detection algorithm (DSRLP) under jamming attack,” *Our heritage*, vol. 68, no. 30, 2020.

[3] N. Dinarvand and H. Barati, “An efficient and secure RFID authentication protocol using elliptic curve cryptography,” *Wireless Networks*, vol. 25, no. 1, pp. 415–428, Jan. 2019, doi: 10.1007/s11276-017-1565-3.

[4] U. Gulen and S. Baktir, “Elliptic curve cryptography for wireless sensor networks using the number theoretic transform,” *Sensors*, vol. 20, no. 5, pp. 1507–1523, Mar. 2020, doi: 10.3390/s20051507.

[5] M. Kolhekar and A. Jadhav, “Implementation of elliptic curve cryptography on text and image,” *International Journal of Enterprise Computing and Business Systems*, vol. 1, no. 2, pp. 1–13, 2011.

[6] R. Balamurugan, V. Kamalakannan, G. D. Rahul, and S. Tamilselvan, “Enhancing security in text messages using matrix based mapping and ElGamal method in elliptic curve cryptography,” in *2014 International Conference on Contemporary Computing and Informatics (IC3I)*, Nov. 2014, pp. 103–106, doi: 10.1109/IC3I.2014.7019749.

[7] T. J. Wong, L. F. Koo, F. H. Naning, A. F. N. Rasedee, M. M. Magiman, and M. H. A. Sathar, “A cubic El-Gamal encryption scheme based on lucas sequence and elliptic curve,” *Advances in Mathematics: Scientific Journal*, vol. 10, no. 11, pp. 3439–3447, Nov. 2021, doi: 10.37418/amsj.10.111.5.

[8] L. Tawalbeh, M. Mowafi, and W. Aljoby, “Use of elliptic curve cryptography for multimedia encryption,” *IET Information Security*, vol. 7, no. 2, pp. 67–74, Jun. 2013, doi: 10.1049/iet-ifs.2012.0147.

[9] A. Abusukhon, Z. Mohammad, and A. Al-Thaher, “An authenticated, secure, and mutable multiple-session-keys protocol based on elliptic curve cryptography and text-to-image encryption algorithm,” *Concurrency and Computation: Practice and Experience*, vol. 34, no. 4, Feb. 2022, doi: 10.1002/cpe.6649.

[10] O. S. Rao and S. P. Setty, “Efficient mapping methods for elliptic curve cryptography,” *International Journal of Engineering Science and Technology*, vol. 2, no. 8, pp. 3651–3656, 2010.

[11] P. Perumal and S. Subha, “An analysis of a secure communication for healthcare system using wearable devices based on elliptic curve cryptography,” *World Review of Science, Technology and Sustainable Development*, vol. 18, no. 1, pp. 51–58, 2022, doi: 10.1504/WRSTSD.2022.119327.

[12] D. Sravana Kumar, “Encryption of data using elliptic curve over finite fields,” *International Journal of Distributed and Parallel systems*, vol. 3, no. 1, pp. 301–308, Jan. 2012, doi: 10.5121/ijdps.2012.3125.

[13] G. Ganapathy and K. Mani, “Maximization of speed in elliptic curve cryptography using fuzzy modular arithmetic over a micro-controller-based environment,” in *Proceedings of the World Congress on Engineering and Computer Science 2009*, 2009, vol. 1, pp. 1–5.

[14] M. Rashid, M. M. Hazzazi, S. Z. Khan, A. R. Alharbi, A. Sajid, and A. Aljaedi, "A novel low-area point multiplication architecture for elliptic-curve cryptography," *Electronics*, vol. 10, no. 21, Nov. 2021, doi: 10.3390/electronics10212698.

[15] N. Niyaz Ahamed and N. Duraipandian, "Secured data storage using deduplication in cloud computing based on elliptic curve cryptography," *Computer Systems Science and Engineering*, vol. 41, no. 1, pp. 83–94, 2022, doi: 10.32604/csse.2022.020071.

[16] Z. Salman, M. Hammad, and A. Y. Al-Omary, "A homomorphic cloud framework for big data analytics based on elliptic curve cryptography," in *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Sep. 2021, pp. 7–11, doi: 10.1109/3ICT53449.2021.9582001.

[17] A. B. Jivane, "Time efficient privacy-preserving multi-keyword ranked search over encrypted cloud data," in *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, Sep. 2017, pp. 497–503, doi: 10.1109/ICPCSI.2017.8392345.

[18] U. Priyatharsan, P. L. Rupasinghe, and I. Murray, "A new elliptic curve cryptographic system over the finite fields," in *2017 6th National Conference on Technology and Management (NCTM)*, Jan. 2017, pp. 164–169, doi: 10.1109/NCTM.2017.7872847.

[19] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology — CRYPTO '85 Proceedings*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 417–426.

[20] N. Koblitz, "Elliptic curve cryptosystem," *Mathematics of computation*, vol. 48, no. 16, pp. 203–209, 1987.

[21] R. Bhanot and R. Hans, "A review and comparative analysis of various encryption algorithms," *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 289–306, Apr. 2015, doi: 10.14257/ijsia.2015.9.4.27.

[22] H. Liang, G. Zhang, W. Hou, P. Huang, B. Liu, and S. Li, "A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography," *Applied Sciences*, vol. 11, no. 12, Jun. 2021, doi: 10.3390/app11125691.

[23] S. Narayan, "A review on elliptic curve cryptography," *International Journal of Emerging Technology and Innovative Engineering*, vol. 4, no. 12, pp. 132–138, 2019.

[24] G. Zhang, W. Ding, and L. Li, "Image encryption algorithm based on tent delay-sine cascade with logistic map," *Symmetry*, vol. 12, no. 3, pp. 355–342, Mar. 2020, doi: 10.3390/sym12030355.

[25] M. M. Trung, "Proposing an elliptic curve cryptosystem with the symmetric Key for Vietnamese text encryption and decryption," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 4158–4162, Jun. 2020, doi: 10.30534/ijatcse/2020/246932020.

[26] S. S. Kumar, "Elliptic curve cryptography for constrained devices," PhD Thesis, Ruhr-University Bochum, 2006.

## BIOGRAPHIES OF AUTHORS

**Mai Manh Trung** graduated from, Vietnam National University, Hanoi. Currently a lecturer at the University of Economics Technology for Industries and researcher at the University of Engineering and Technology, Vietnam National University, Hanoi. Research area: Cryptography, lightweight cryptography, security for IoT networks, artificial intelligence, application programming. Address: 144 Xuan Thuy Street, Cau Giay District, Hanoi City, Vietnam. He can be contacted by email: mmtrung@uneti.edu.vn.

**Le Phe Do** Lecturer at Faculty of Information Technology, University of Technology, Vietnam National University, Hanoi. His research areas are advanced mathematics, statistical probability, cryptography, light cryptography, and information security. Address: 144 Xuan Thuy Street, Cau Giay District, Hanoi City, Vietnam. He can be contacted by email: dolp@vnu.edu.vn.

**Do Trung Tuan** he is affiliated in University of Science, Vietnam National University, Hanoi. His research areas are database, data science, data mining, and data security. Address: 144 Xuan Thuy Street, Cau Giay District, Hanoi City, Vietnam. He can be contacted at tuandt@vnu.edu.vn.

**Nguyen Van Tanh** graduated from Hanoi University of Science and Technology, Vietnam. Lecturer and researcher at the International School, Vietnam National University, Hanoi. Author of much Research on information security, security for IoT networks and many scientific publications in the field of IT applications. 144 Xuan Thuy Street, Cau Giay District, Hanoi City, Vietnam. He can be contacted by email: Tanhnv@vnu.edu.vn.

**Ngo Quang Tri** Graduated from Hanoi University of Science and Technology. As a researcher, the author publishes many scientific articles in the fields of information technology, information security and computer network communication. Currently working in the Information Technology field at 1 Faculty of Information Technology, University of Economics Technology for Industries (UNETI). Address: 456 P. Minh Khai Street, Hai Ba Trung District, Hanoi City, Vietnam. He can be contacted by email: nqtri@uneti.edu.vn.