International Journal of Advanced Science and Technology
Vol. 29, No. 6, (2020), pp. 3264 - 3273

# Implementation of Elliptic Curve Diffie-Hellman (ECDH) for Encoding Messeges Becomes a Point on the GF($p$)

[1*]Asep Saepulrohman, Teguh Puja Negara[2]

[1,2]*Department of Computer Science, Faculty of Mathematics and Natural Science, Pakuan University, Bogor, West Java, 16143, Indonesia*

[1*]*asepspl@unpak.ac.id,* [2]*teguhpuja795@gmail.com*

***Abstract***

*In data communication systems, the authenticity of data becomes important in the process of exchanging messages on insecure channels. If there is no security in the transmission process, then the possibility that occurs is an intercept from an irresponsible party. The elliptic curve defined in GF(p) is only closed to the sum, the process of adding two points in the elliptic curve always produces a point located on the elliptic curve, in this work using p = 149. The cryptography used by Elliptic Curve Diffe-Hellman (ECDH) to encrypt plaintext by changing the original message using a point on the curve with the help of the Python program. Elliptic Curve Cyptography (ECC) offers a better level of security compared to non-ECC cryptography because it has a shorter key size for example, a 160-bit ECC has a strength equivalent to 1024-bit RSA keys*

***Keywords:*** *Cryptography, Curve elliptic Diffie-Hellman, Encoding message, Algebraic group.*

## 1. Introduction

The public key cryptographic system or often called asymmetric key cryptography was first proposed by Diffe and Hellman in 1976 who discovered a special method of key exchange implemented in the field of cryptography [1], [2]. The key for $P_e$ encryption is called a non-confidential public key [3], so it can be distributed on insecure channels. Whereas the $P_d$ decryption key is called a private key which is confidential and must be kept confidential. Elliptic-curve Diffe-Hellman (ECDH) is a key agreement protocol for constructing a public key or a partnership key that is formed from a mutually agreed private key. The key, or derived key, can then be used to encrypt messages which then use a symmetric-key password.

In a previous study [4], we presented a decoding of the minimum binary Gilbert-Varshamove code syndrome. In this paper, we discuss cryptographic implementations of elliptic curves [5]-[7] using elliptic curves over binary fields. We will discuss a number of issues, including coding the point to point, key generation process, and encryption. Arithmetic operations on elliptic curves are defined on real numbers, whereas cryptography operates on integers because in cryptography plaintext, ciphertext, and keys are expressed as integer numbers. Therefore, elliptic curves in real numbers are not used for the ECDH algorithm. For example $P(x_1, y_1)$ and $Q(x_2, y_2)$ two points on the elliptic curve, the sum of the two points with operator $+$ produces point $R(x_3, y_3)$ which is also on the elliptic curve which also fulfills the closure axiom of the group $\langle G, + \rangle$ [8].

ISSN: 2005-4238 IJAST

Arithmetic operations on elliptic curves are defined on integers or modular arithmetic so that arithmetic operations always produce integers in the same scope. Modular operation input requires 2 numbers, namely an integer $a$ and a positive number (modulus $p$) to return the remainder of division $r$ (written $a$ mod $b$) with the result of any modular operation integer number $a$ with an integer number $p$ always in the range 0 to $p-1$ or the modular operation $p$ against $a$ is a mapping from the set of integer numbers ($Z$) to the set of modular residue sets $\{0, 1, 2, \dots, p-1\}$ denoted $Z_p$, for example the modular resuda set $p = 7$, written $Z_p = \{0, 1, 2, 3, 4, 5, 6\}$.

## 2. Material and Method

In this section, the materials and methods used are described as follows.

### 2.1. Material

The research material used to convert messages into code is the ASCII table which is accessed through the website http://www.asciitable.com. The process of encrypting and decrypting messages using the ECDH algorithm using the help of a program written by Ashutosh Ahelleya that requires a message mapping table to be a point on the elliptic curve.

### 2.2. Method

In this section, we discuss the methods used in converting messages into codes, using cryptography Elliptic curves include: the sum of points on a curve, doubling of points, point release, and point multiplication.

## 3. Mathematical models

This section discusses the related material (theory) of elliptic curves that will be used in the process of converting messages into codes.

### 3.1. Elliptic Curve over Real Number

The elliptic curve over a finite field is not an ellipse, the elliptic curve has the same common equation:

$$ax^2 + by^2 + cx + dy + e = 0 \quad (1)$$

where $a, b, c, d$ and $e$ are coefficients in the form of real numbers. Given $a, b$ the set of real numbers that satisfy $4a^2 + 27b^2 \neq 0$. Elliptic curves that are non-singular are the set $E$ consisting of pairs $(x, y) \in R \times R$ together with infinity point $\mathcal{O}$ that satisfy:

$$E = \{x, y | \, y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\} \quad (2)$$

For each $x$ there are always two different $y$ values, where the $y$ value is the result of the $x$-axis reflection. The most interesting thing in the elliptic curve that is used in cryptography is the nature of the group. The points $(x, y)$ on the elliptic curve together with the addition operation form a group $\langle G, + \rangle$ where the elliptic curve equation solution and the infinity point $E = \{(x_0, y_0), (x_1, y_1), \dots, (x_n, y_n), \mathcal{O}\}$. For example, elliptic curve charts mapped to real numbers with $a = -5$ and $b = 3$, write $y^2 = x^3 - 5x + 3$ in Figure 1.

ISSN: 2005-4238 IJAST

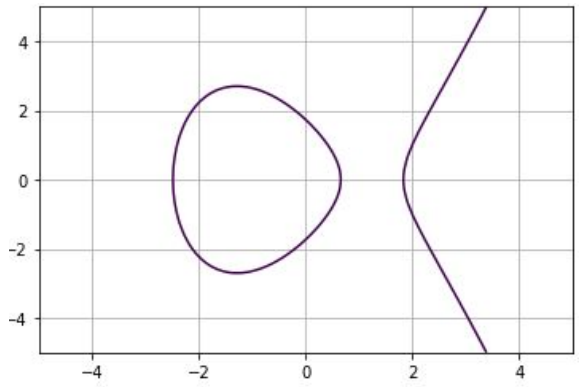


**Figure 1.** Elliptic curve over real number

We define the point operations as follows. First, let $E$ be an elliptic curve over real numbers. If $P, Q \in E$ where $P$ is the point $(x_1, y_1)$ and $Q$ is the point $(x_2, y_2)$. If $x_1 \neq x_2$ then the sum operation $P + Q = R$. Addition $R = (x_3, y_3)$. is sought by determining lines $l$ through $P$ and $Q$ that intersect at $-R$, where $R$ is the result of reflection $-R$ on the $x$-axis. The coordinates of the point $R$ can be determined by the following equation $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = (y_2 - y_1)/(x_2 - x_1)$ [9]-[11] The second case, point $P$ and $Q$ the same point $x_1 = x_2$ can then be written $P + P = R$. $R$ is found by determining the line $l$ which is tangent to the elliptic curve at point $P$, then the intersection of line $l$ with the elliptic curve is $-R$ which is a reflection of the x-axis. The last case if $x_1 = x_2$ and $y_1 = -y_2$, in this case $Q = -P$ where the lines $l$ through $P$ and $Q$ do not intersect the elliptic curve so that they are said to have an infinity point, written $P + Q + P + (-P) = \mathcal{O}$.

### 3.2. Elliptic Curve over GF($p$)

Cryptographic systems based on eilptic curves do not actually use real numbers, but use limited fields such as modular fields of prime numbers GF($p$), where arithmetic operations correspond to addition and multiplication operations on $Z_p$. Adding operations on elliptic curves on GF($p$) have the same rules as real numbers. First case if $x_1 \neq x_2$ then the sum operation $P + Q = R$. Addition $R = (x_3, y_3)$ is sought by determining lines $l$ through $P$ and $Q$ that intersect at $-R$, where $R$ is the result of reflection $-R$ on the $x$-axis. The coordinates of the point $R$ can be determined by the following equation $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = (3{x_2}^2 + a)/2y_1$. The second case, point $P$ and $Q$ the same point $x_1 = x_2$ can then be written $P + P = R$. $R$ is found by determining the line $l$ which is tangent to the elliptic curve at point $P$, then the intersection of line $l$ with the elliptic curve is $-R$ which is a reflection of the x-axis. The last case if $x_1 = x_2$ and $y_1 = -y_2$, in this case $Q = -P$ where the lines $l$ through $P$ and $Q$ do not intersect the elliptic curve so that they are said to have an infinity point, written $P + Q + P + (-P) = \mathcal{O}$. Although, the elliptic curve E on GF($p$) cannot be described in the form of an elliptic curve E and the sum (+) operation forms the Abelian group $\langle G, + \rangle$ [12].

### 3.3. Elliptic Curve over GF($2^n$)

The cryptographic curve of the elliptic curve over GF($2^n$) is almost similar to the elliptic curve over GF$(p)$,but the elliptic curve in GF($2^n$) is a finite field whose elements are polynomials represented by binary numbers 0 and 1, besides the elliptic curve used $y^2 = x^3 + ax + b$ with $b \neq 0$ and $a, b, x, y$ is a polynomial. The elliptic curve addition rule in GF($2^n$)) has several cases.First case if $x_1 \neq x_2$ then the sum operation $P + Q = R$. Addition $R = (x_3, y_3)$ is sought by determining lines $l$ through $P$ and $Q$ that intersect at $-R$, where $R$ is the result of reflection $-R$ on the $x$-axis. The coordinates of the point $R$ can be determined

by the following equation $x_3 = \lambda^2 + x_1 + x_2 + a$ and $y_3 = \lambda(x_1 + x_3) + x_3 + y_1$ where $\lambda = (y_2 + y_1)/(x_2 + x_1)$ [13]-[15].

### 3.4. Elliptic Curve Diffie-Hellman (ECDH)

The Diffe-Hillman key algorithm is a public-key algorithm that involves a large number of operations. The security of an algorithm is determined by the difficulty of calculating the discrete logarithm of a modulo continuity. Where a discrete logarithm problem occurs, if $p$ are prime numbers, $y$ is any integer, and $q$ is the primary root of $p$ then finding $x$ of $y = q^x \pmod p$ is very difficult. For example, Alice and Bob agree on a prime number $n$ and an integer $q$ is the primitive of $n$ ($n$ and $g$ are not secret). This algorithm is done by generating random integers $x$ and sending the calculation results to Bob, which is $X = q^x \bmod n$. After that, Bob generates random integers y and sends the calculation result to Alice $Y = g^x \bmod n$, Alice calculates is $K = Y^x \bmod n$ and Bob calculates $K' = X^y \bmod n$. If the calculation is correct then $K = K'$, which means the symmetry key has been successfully accepted by both parties.

The $K$ symmetry key calculation algorithm is much simpler and more computationally efficient when using the Diffie-Hellman Elliptic Curve [13]-[15]. First, Alice and Bob approve the parameters of integers $a$ and b prime numbers in the elliptic curve equation $y^2 \equiv x^3 + ax + b \pmod p$ and a base point $G(x, y)$ selected from the elliptic group to the addition operation. Domain parameter creation is not done by each sender or recipient as they will involves calculating the number of points on the curve to be takes a long time and is difficult to implement. The elliptic curve parameter domain above $F_p$ is defined as the equation $T(p, a, b, G, n, h)$, where $p$ is field that the curve is defined over, $a, b$ he elliptic curve equation coefficient, $G$ the generator point is the group building elements, $n$ is prime order of $G$ i.e. positive integers smallest is $nG = 0$, and $h$ cofactor, number of points in the group elliptic $E_p(a, b)$ divided by $n$.

| **Algorithm 1** | ECDH key generator algorithm |
|---|---|
| Input: | Domain parameter $(p, a, b, G, n, h)$ |
| Output: | Private key: $x, y$ and Public key: $P_A, P_B$ |
| 1. | Choose an integer $x, y \in [1, n-1]$ |
| 2. | User A computes $P_A = x.G$ send to User B |
| 3. | User B computes $P_B = y.G$ send to User A |
| 4. | User A calculate $K = x.P_B = x(y.G)$ |
| 5. | User B calculate $K' = y.P_A = y(x.G)$ |

Then the next process is the message encryption process with ECDH which is a variant of the Diffie-Hellman algorithm for elliptical curves. The problem he solved was as follows: two parties (usually Alice and Bob) wanted to exchange information safely, so that third parties could not decipher their code. Next is the ECDH encryption process in Algorithm 2.

| **Algorithm 2** | ECDH encryption algorithm |
|---|---|
| Input: | Domain parameter $(p, a, b, G, n, h)$ |
| | Private key: $x, y$ and Public key: $P_A, P_B$, plaintext $M$ |
| Output: | Chipertext: $C$ |
| 1. | Calculate $S = yP_A = x.P_B$ |
| 2. | Calculate C= $M + S$ |

In this decryption system design, will return the encrypted message to an original message again. The decryption process is then performed by reducing the cipher point with the shared secret key in Algorithm 3.

| **Algorithm 3** | ECDH decryption algorithm |
|---|---|
| Input: | Domain parameter $(p, a, b, G, n, h)$, secret lock together $S$, chipertext $C$ |
| Output: | Plaintext $M$ |
| 1. | Calculate $M = C - S$ |
| 2. | Plaintext $M = C - S$ |

## 4. Numerical Simulation

The process of encrypting and decrypting messages using the ECDH algorithm using the help of a program written by Ashutosh Ahelleya which requires a message mapping table to be a point on the elliptic curve. In the encryption and decryption program this message uses the elliptic curve cryptography method to determine the point. Example of an algebraic calculation for making elliptic curve points, given an elliptic curve equation $y^2 = x^3 - 5x + 3$ mod 149. If substituted value $a = 1$ dan $b = 5$ then for $4a^2 + 27b^2 \neq 0$, so $E$ is in the elliptic curve. To be able to make $(x, y)$ curve points, first determine the elements of the top elliptic curve, which are: $F_{149} = \{0, 1, 2, 3, \ldots, 148\}$ then determine the Quadratic Residue Module to determine the elliptic curve group element which is the set of resolutions from $y^2 = x^3 - 5x + 3$ mod 149 for $x, y \in F_{149}$. The elements inside $F_{149}$ are calculated to determine all points in the elliptic curve, for example $(x_1, y_1) = (2, 1)$ and $(x_1, y_1) = (8, 37)$, then $P + \mathrm{Q}$ can be calculated. Gradient value $\lambda = (y_p - y_q)/(x_p - x_q)$ mod 149 = $(37 - 1)/(8 - 2)$ mod 149 = 6 mod 149 = 6. The value of $R = (x_3, y_3)$ is the sum result:

$$x_3 = \lambda^2 - x_1 - x_2 \bmod 149 = 6^2 - 2 - 8 \bmod 149 = 26$$
$$y_3 = \lambda(x_1 - x_3) - y_1 \bmod 149 = 6(2 - 26) - 1 \bmod 149 = 4$$

The results of the addition and multiplication operations of all messages into points located in the elliptic curve can be seen in Table 1.

**Table 1.** The encoding of message a point on the elliptic $y^2 = x^3 - 5x + 3$ mod 149

| $x$ | $(x_1, y_1)$ | $(x_1, y_2)$ | $x$ | $(x_1, y_1)$ | $(x_1, y_2)$ | $x$ | $(x_1, y_1)$ | $(x_1, y_2)$ |
|---|---|---|---|---|---|---|---|---|
| 1 | (1, 44) | (1, 105) | 49 | (1, 44) | (1, 105) | 108 | (108, 42) | (108, 107) |
| 2 | **(2, 1)** | (2, 148) | 52 | (52, 69) | (52, 80) | 109 | (109, 71) | (109, 78) |
| 4 | (4, 14) | (4, 135) | 58 | (58, 23) | (58, 126) | 111 | (111, 2) | (111, 147) |
| 8 | **(8, 37)** | (8, 112) | 59 | (59, 19) | (59, 130) | 112 | (112, 33) | (112, 116) |
| 13 | (13, 7) | (13, 147) | 60 | (60, 40) | (60, 109) | 116 | (116, 17) | (116, 132) |
| 14 | (14, 12) | (14, 137) | 62 | (62, 51) | (62, 98) | 117 | (117, 18) | (117, 131) |
| 15 | (15, 5) | (15, 144) | 65 | (65, 21) | (65, 128) | 120 | **(120, 33)** | (120, 116) |
| 17 | (17, 19) | (17, 130) | 66 | (66, 33) | (66, 116) | 122 | (122, 47) | (122, 102) |
| 20 | (20, 30) | (20, 119) | 70 | (70, 20) | (70, 129) | 124 | **(124, 44)** | (124, 105) |
| 24 | (24, 44) | (24, 105) | 73 | (73, 19) | (73, 130) | 125 | (125, 56) | (125, 93) |
| 25 | (25, 56) | (25, 93) | 74 | (74, 60) | (74, 89) | 126 | (126, 13) | (126, 136) |
| 26 | **(26, 4)** | (26, 145) | 80 | (80, 58) | **(80, 91)** | 128 | (128, 54) | (128, 95) |
| 28 | (28, 43) | (28, 106) | 85 | (85, 11) | (85, 138) | 129 | (129, 0) | - |
| 30 | (30, 35) | (30, 114) | 86 | (86, 12) | (86, 137) | 134 | (134, 32) | (134, 117) |
| 32 | (32, 24) | (32, 125) | 91 | (91, 64) | (91, 85) | 137 | (137, 47) | (137, 102) |
| 36 | (36, 17) | (36, 132) | 92 | (92, 2) | (92, 147) | 138 | (138, 51) | (138, 98) |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 39 | (39, 47) | (39, 102) | 95 | (95, 2) | (95, 147) | 140 | (140, 8) | (140, 141) |
| 40 | (40, 39) | (40, 110) | 98 | (98, 51) | (98, 98) | 141 | (141, 53) | (141, 196) |
| 41 | (41, 46) | (41, 103) | 102 | (102, 62) | (102, 87) | 142 | (142, 69) | (142, 80) |
| 44 | (44, 22) | (44, 127) | 103 | (103, 55) | (103, 94) | 146 | (146, 17) | (146, 17) |
| 46 | (46, 40) | (46, 109) | 104 | (104, 69) | **(104, 80)** | 147 | (147, 68) | (147, 81) |
| 47 | (47, 6) | (47, 143) | 105 | (105, 72) | (105, 77) | 148 | (148, 56) | (148, 93) |
| 48 | (48, 63) | (48, 86) | 107 | (107, 25) | (107, 124) | | | |

Based on the points on the elliptic curve in modulus p are limited in number, this is di erent from the points on the elliptic curve in the realm of real numbers which have many infinite points. Where the addition and multiplication between two points will produce points located on the curve elliptic too. Figure 2 shows the discrete points on the elliptic curve $y^2 = x^3 - 5x + 3 \bmod 149$ visually it does not seem to form an elliptic curve in Figure 2 below, although the elliptic curve $E$ in $F_{149}$ cannot be depicted in the form of an elliptic graph $E$ and the summation operations form the Abelian group $G = \langle E, + \rangle$.

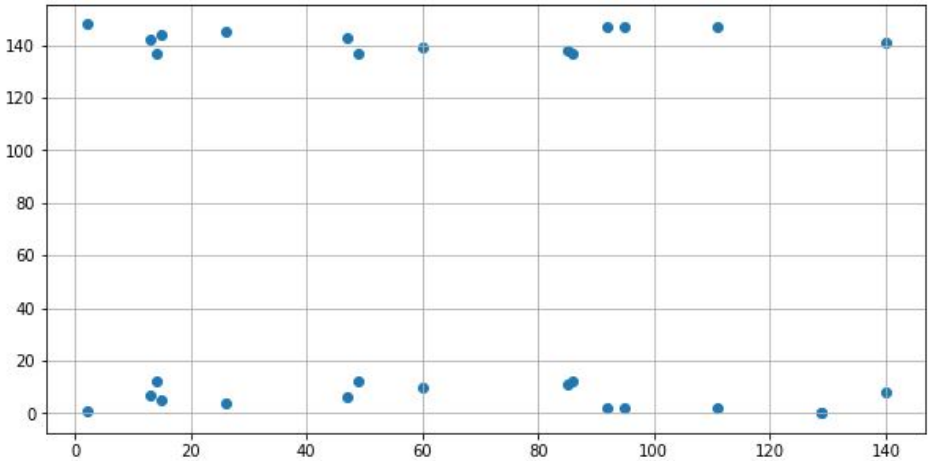


**Figure 2.** The points on the elliptic curve $y^2 = x^3 - 5x + 3 \bmod 149$

For example Alice and Bob agree on point $G(2, 1)$ as a generator on the elliptic curve $y^2 = x^3 - 5x + 3 \bmod 149$ in Figure 3

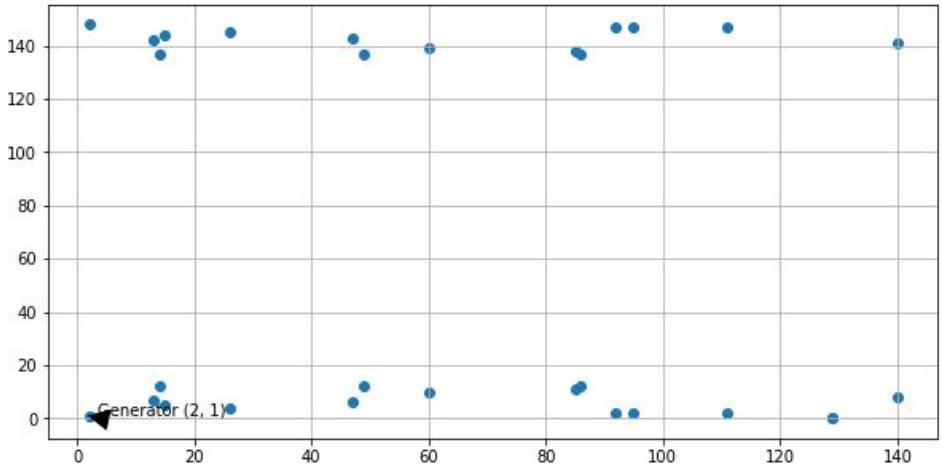


**Figure 3.** Generator point on the elliptic curve $y^2 = x^3 - 5x + 3 \bmod 149$

Points that can be generated by $(2,1)$ can be calculated using the sum of $P+P$ repeatedly. First calculated $P+P=2P=2(2,1)=(2,1)+(2,1)=R$ as follows. Gradient value $\lambda = (3{x_2}^2+a)/2y_1 \bmod 149 = \frac{3.2^2+(-5)}{(2.1)} \bmod 149 = 7.2^{-1} \bmod 149 = 7.75 \bmod 149 = 525 \bmod 149 = 78$. The value of $R=(x_3,y_3)$ is the sum result,

$$
\begin{aligned}
x_3 &= \lambda^2 - 2x_1 \bmod 149 \\
&= 78^2 - 2.2 \bmod 149 \\
&= 120 \\
y_3 &= \lambda(x_1 - x_3) - y \bmod 149 \\
&= 78(2-120) - 1 \bmod 149 \\
&= 33
\end{aligned}
$$

The coordinate of point R which is the result of doubling the point P on the elliptic curve $y^2 = x^3 - 5x + 3 \bmod 149$ can be illustrated in Figure 4.

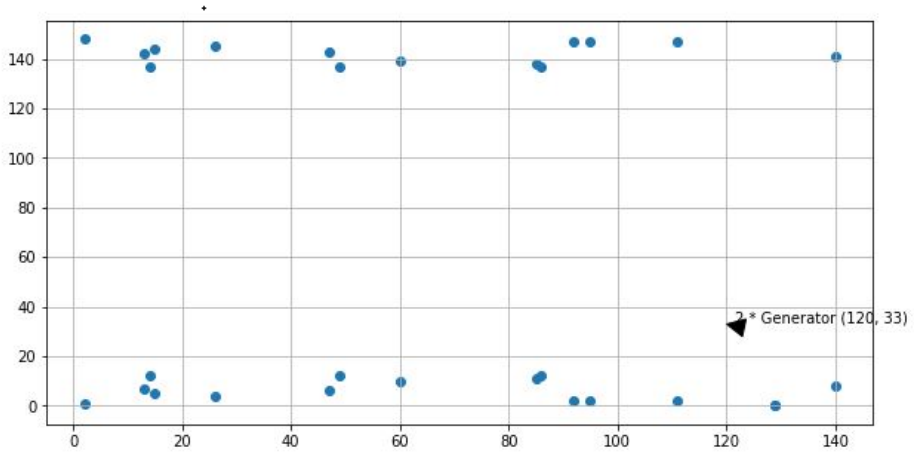


**Figure 4.** The point on the elliptic curve $y^2 = x^3 - 5x + 3 \bmod 149$

In the case of private key exchanges that User 1 and User 2 will do, for example Alice and Bob. The first step the two of them have to do is create a shared key but the only channel available is unsafe. Therefore, an elliptic curve of $E$ is constructed on a field up to $F_p$ wherein E forms a point $G(x,y)$ on the set of points to be used as a cryptographic parameter. Initially, the domain parameters $(p,a,b,G,n,h)$,in the main case or must be agreed upon. Next Alice chooses $x$ as a private key (a randomly chosen integer in the interval $[1,n-1]$ and the public key is represented by a point $P_A$ ($P_A = x.G$, that is, the result of adding $G$ to herself), as well as Bob chooses y as a private key (a randomly chosen integer in the interval $[1,n-1]$ and a public key $P_B$ ($P_B = y.G$, that is, the result of adding $G$ to himself). Then the two public keys are $P_A$ and $P_B$ is exchanged, so Alice knows $P_B$ and Bob knows $P_A$.

Based on the generator in Figure 3 and Figure 4 , it was agreed that Alice chose the private key $x=6$ and Bob chose her private key $y=11$ and then calculated her public key in accordance with Algorithm 1, then Alice's public key = (104, 80) and Bob's public key was obtained (80, 91) illustrated in Figure 5

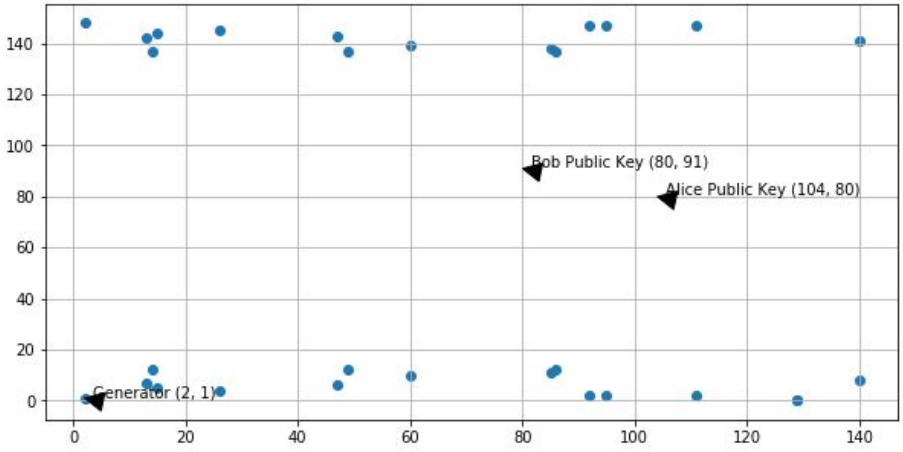


**Figure 5.** Public key on the elliptic curve $y^2 = x^3 - 5x + 3 \bmod 149$

The next stage exchanged public keys are recalculated to get the secret key $S$, where Alice calculates the secret key $S$ as follows $S = xP_B$ and Bob calculate the secret key $S'$ as follows $S' = yP_A$. If $S = S'$ then Alice and Bob now share the same secret key (124, 44). Messages that are changed to codes have a public key and a secret key as shown in Figure 6

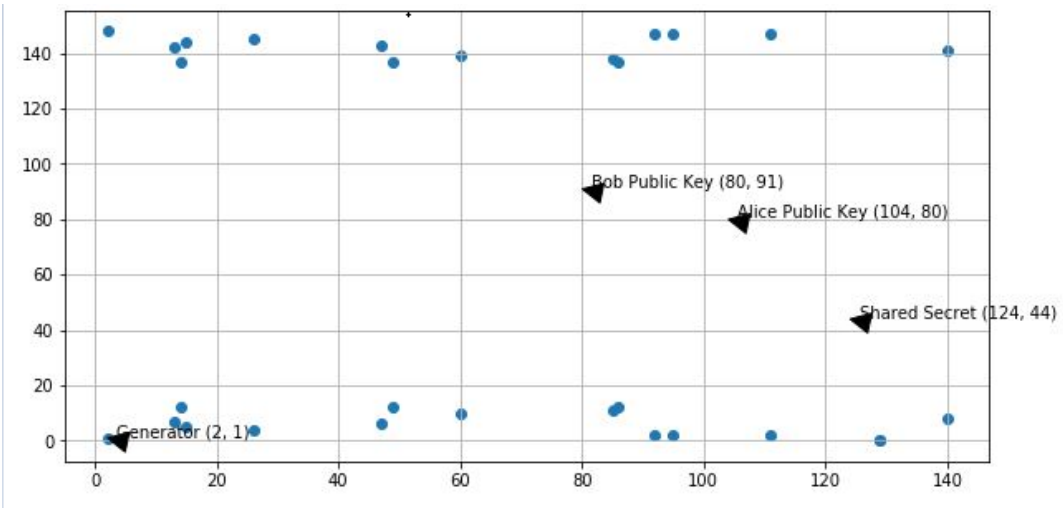


**Figure 6.** Private key on the elliptic curve $y^2 = x^3 - 5x + 3 \bmod 149$

Elliptic curve cryptographic systems can be applied to messages in the form of points on the elliptic curve. Therefore, any message must be coded first becoming a point on the elliptic curve. The simplest way is to encode each message character in the ASCII code. Some examples of encryption techniques can be seen in [16]-[18].

## 5. Conclusion

The resulting point is based on an elliptic curve test simulation influenced by $a, b$, and $p$. So the greater the value of $p$, the more points will be generated, but if the value of $a, b$ the greater the smaller the number of points. Therefore $a$ values $b$ and $p$ are the values used to produce curve points. In this work, the calculation results show the Diffie-Hellman Elliptic Curve key exchange protocol, in this case the user's private key is 6, the user's private key is worth 11 which results in the user's public key (104, 80) and the user's public key (80, 91) while the private key to maintaining the resulting secrecy is (124, 44). Elliptic curves in GF ($p$) or GF ($2^n$) form groups. The problem of

discrete logarithms as can be defined on an elliptic curve, where elliptic curve groups are formed by a set of pairs of values that satisfy the elliptic and infinity curve equations and an addition operation.

## References

[1] Shamir, A. "New directions in croptography." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *2162*, 159. https://doi.org/10.1007/3-540-44709-1_14, 2001.

[2] Kumar, R., Ravindranath, C. C. "Analysis of Diffie-Hellman Key Exchange Algorithm with Proposed Key Exchange Algorithm." *International Journal of Emerging Trends Technology in Computer Science (IJETTCS),* vol. no. 1, p. 40-43, 2015.

[3] Nagaraj, S., Raju, G. S. V. P., Srinadth, V. "Data encryption and authetication using public key approach." *Procedia Computer Science*, vol 48, p.126-132. https://doi.org/10.1016/j.procs.2015.04.161, 2015.

[4] Saepulrohman, A., Guritman, S., Silalahi, B. P. "Dekoding Sindrom Kode Gilbert-Varshamov Biner Berjarak Minimum Rendah." *Journal of Mathematics and Its Applications,* vol 14, no.1, p. 41-54 https://doi.org/10.29244/jmap.14.1.41-54 , 2015.

[5] Sonnino, A., & Sonnino, G. "Elliptic-Curves Cryptography on High- Dimensional Surfaces." *International Journal of Advanced Engineering Research and Science (IJAERS),* vol. 4, no. 2. https://dx.doi.org/10.22161/ijaers.4.2.28, 2017.

[6] Saudy, N. F., Ali, I. A., Barkouky, R. Al. "Error analysis and detection procedures for elliptic curve cryptography." *Ain Shams Engineering Journal*, vol. 10, no. 3, p. 587-597. https://doi.org/10.1016/j.asej.2018.11.007, 2019.

[7] Weng, J., Dou, Y., Ma, C. "Research on attacking a special elliptic curve discrete logarithm problem." *Mathematica. Problems in Engineering*, https://doi.org/10.1155/2016/5361695, 2016.

[8] Myasnikov, A. G., Roman Kov, V. "Verbally closed subgroups of free groups." *Journal of Group Theory* vol. 17, no. 1, p. 29-40. https://doi.org/10.1515/jgt-2013-0034, 2014.

[9] Susantio, D. R., Muchtadi-Alamsyah, I. "Implementation of Elliptic Curve Cryptography in Binary Field." *Journal of Physics: Conference Series*, vol.710, no. 1, https://doi.org/10.1088/1742-6596/710/1/012022, 2016.

[10] Johnson, D., Menezes, A., & Vanstone, S. *The Elliptic Curve Digital Signature Algorithm Validation System ( ECDSAVS )*. 56. http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf, 2004.

[11] Verma, S. K., Ojha, D. B. "A Discussion on Elliptic Curve Cryptography and Its Applications." *International Journal of Computer Science Issues 2012*, vol. 9, no. , p. 74-77. 2012.

[12] Bisson, G., Sutherland, A. V. "Computing the endomorphism ring of an ordinary elliptic curve over a finite field." *Journal of Number Theory*, vol. 131, no.5, p. 815-831. https://doi.org/10.1016/j.jnt.2009.11.00, 2011.

[13] Kefa R. "Elliptic Curve Cryptography over Binary Finite Field GF($2^m$)." *Information Technology Journal,* vol. 5, no.1, p. 204-229. 2006.

[14] Lopez, J., Dahab, R. "Fast multiplication on elliptic curves over GF($2^m$) without precomputation." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Articial Intelligence and Lecture Notes in Bioinformatics),* 1717(107), p. 316-327. https://doi.org/10.1007/3-540-48059-527, 1999.

[15] King, B. "An improved implementation of elliptic curves over gf($2^n$) when using projective point arithmetic." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Arti_cial Intelligence and Lecture Notes in Bioinformatics)*, 2259(1), p. 134-150. https://doi.org/10.1007/3-540-45537-x11, 2001.

[16] Mobayen, S., Vaidyanathan, S., Sambas, A., Kacar, S., & Çavuşoğlu, Ü. "A novel chaotic system with boomerang-shaped equilibrium, its circuit implementation and application to sound encryption." *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, *43*(1), p. 1-12, 2019. https://doi.org/10.1007/s40998-018-0094-0

[17] Vaidyanathan, S., Azar, A. T., Rajagopal, K., Sambas, A., Kacar, S., & Çavusoglu, Ü. "A new hyperchaotic temperature fluctuations model, its circuit simulation, FPGA implementation and an application to image encryption." *IJSPM*, *13*(3), p. 281-296, 2018. https://doi.org/10.1504/IJSPM.2018.093113

[18] Vaidyanathan, S., Sambas, A., Mamat, M., & Sanjaya W. S, M. "Analysis, synchronisation and circuit implementation of a novel jerk chaotic system and its application for voice encryption." *International Journal of Modelling, Identification and Control*, *28*(2), p. 153-166, 2017. https://doi.org/10.1504/IJMIC.2017.085934

ISSN: 2005-4238 IJAST