Building Elliptic Curve Cryptography With Public Key To Encrypt Vietnamese Text

Mai Manh Trung, Do Trung Tuan, Le Phe Đo

***Abstract*—Today, Elliptic Curve Cryptography (ECC) has many practical applications. ECC was a direction in lightweight primitive cryptography. This paper is based on the arithmetic idea of an Elliptic curve. Elliptic curve arithmetic can be used to develop Elliptic curve encryption schemes such as key exchange, encryption, and digital signature. Compared with traditional cryptosystems with the same level of security, Elliptic curve cryptography has a smaller key size, reducing processing costs. To encode the Vietnamese text, we are based on the sound of Vietnamese characters to make a table of these characters' order. In the present paper, we apply a new encryption algorithm with a public key using an Elliptic curve over finite fields on our proposed Elliptic curve equation.**

***Tóm tắt*—Ngày nay, mật mã đường cong Elliptic (ECC) có nhiều ứng dụng trong thực tế. ECC là một hướng đi trong mật mã nguyên thủy hạng nhẹ. Bài báo này dựa trên ý tưởng số học của một đường cong Elliptic. Số học đường cong Elliptic có thể được sử dụng để phát triển các sơ đồ mã hóa đường cong Elliptic như trao đổi khóa, mã hóa và chữ ký số. So với các hệ thống mật mã truyền thống có cùng mức độ bảo mật, mật mã đường cong Elliptic có kích thước khóa nhỏ hơn, giảm chi phí xử lý. Để mã hóa văn bản tiếng Việt, chúng tôi dựa trên âm của các ký tự Việt Nam để lập bảng thứ tự các ký tự này. Trong bài báo này, nhóm tác giả áp dụng một thuật toán mã hóa mới với khóa công khai bằng cách sử dụng đường cong Elliptic trên các trường hữu hạn trên phương trình đường cong Elliptic được đề xuất.**

Keywords—Decryption; Discrete logarithm; Elliptic curve; Elliptic curve cryptosystem; Encryption, Public key.

Từ khóa: Giải mã, logarith rời rạc, đường cong Elliptic, mật mã trên đường cong Elliptic, mã hóa, khóa công khai

I. INTRODUCTION

The elliptic curve cipher systems (ECC) invented by Neal Koblitz [1] and Victor Miller [2] in 1985 can be considered as elliptic curves of discrete logarithmic cryptographic systems, in which the group $\boldsymbol{Z_P^*}$ is replaced by the group of points on an elliptic curve over a finite field. The mathematical basis for the security of elliptic curve cryptographic systems is the computational computation of the discrete elliptic logarithm problem (ECDLP).

In recent years in Vietnam, the Elliptic curve has played an important role, according to the Circular No. 39/2017/TT-BTTTT, dated December 15, 2017 of the Ministry of Information and Communications on the Promulgation of the technical standards of information technology application in state agencies have recommended applying encryption algorithm on Elliptic curve of Information Security Standards.

The Elliptic curve cryptography system is used in dynamic secure routing link detection [3], in an effective and secure RFID authentication [4], as well as in wireless sensor networks using the number-theoretic to transform [5]. In the paper [6], the authors presented the implementation of ECC by first converting the message into an affine point on the Elliptic curve, then applying the knapsack algorithm on the ECC encrypted message over the finite field $GF_{(p)}$. They will illustrate encryption/decryption involving the embedding system $m \rightarrow P_m$, which imbeds the characters constituting the message and then subjected it.

II. OVERVIEW OF ELLIPTIC CURVE CRYPTOSYSTEMRSYMBOLS AND ABBREVIATIONS

Elliptic curve E over a finite field $GF_{(p)}$ where p is a prime number, a set of points (x, y) satisfying the following equation: E: $y^2 = x^3 + ax + b$ (1) Where a, b are integers modulo p, satisfying: $4a^3 + 27b^2 \neq 0$ which is an Elliptic curve. That is, no point of a curve has two or more distinct tangent lines. And includes a point ∞ called infinity. Forgiven values of a and b, the graph consists of positive and negative values of

y for each value of x. Hence this curve is symmetrical with the x-axis.

We also illustrate the implementation of a cryptographic system based on an Elliptic curve with a public key that corresponds to the chosen Elliptic curve equation:

$$y^2 = x^3 + 18x + 29 \pmod{139} \quad (2)$$

For equation (2) then a = 18, b = 29, we have $4*(18)^3 + 27*(29)^2 = 46035 \neq 0$. Therefore, equation (2) is an Elliptic curve equation.

C. Addition formula

There is a rule, called the chord – and - tangent rule, for adding two points on an elliptic curve E(Fp) to give a third elliptic curve point. Together with this addition operation, the set of points E(Fp) forms a group with ∞ serving as its identity. It is this group that is used in the construction of elliptic curve cryptosystems. The addition rule is best explained geometrically. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two distinct points on an elliptic curve E. If $x_1 = x_2$ and $y_1 = -y_2$ then we define $P + Q = \infty$. Otherwise, $P + Q = (x_3, y_3) \in E$ where $x_3 = \lambda_2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, with:

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1), \text{khi } P \neq Q \\ (3x_1^2 + a)/(2y_1), \text{khi } P = Q \end{cases}$$

So if $P \neq Q$ means $x_1 \neq x_2$, we have:

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \end{cases} \quad (3)$$

If P = Q means $x_1 = x_2$, we have:

$$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1 \end{cases} \quad (4)$$

Note that the points (x_3, y_3), $(x_3, -y_3)$ are also on the E curve and geometrically, the points (x_1, y_1), (x_2, y_2), $(x_3, -y_3)$) are also on a straight line. Besides, define an infinite plus point by itself. $P + \infty = \infty + P = P$ [9].

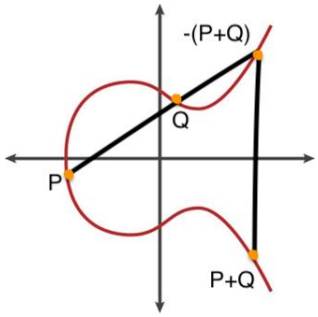

Figure 1. Summation of two points of an elliptic curve

D. Point Multiplication

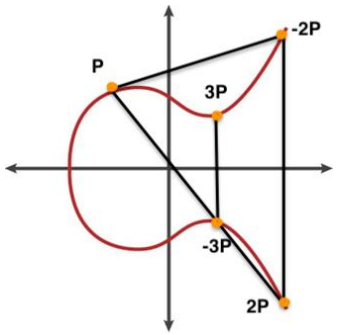

Figure 2. Geometric doubling

If P is a point on an elliptic curve and k is a positive integer, kP denotes P + P + · · · + P (with k summands). If k < 0, then kP = (-P) + (-P) + · · · + (-P), with |k| summands. To compute kP for a large integer k, it is inefficient to add P to it repeatedly. It is much faster to use successive doubling. For example, to compute 19P, we compute 2P, 4P = 2P+2P, 8P = 4P + 4P, 16P = 8P + 8P, 19P = 16P + 2P + P. This method allows us to compute kP for very large k, say of several hundred digits, very quickly. The only difficulty is that the size of the coordinates of the points increases rapidly if we are working over the rational numbers. However, when we are working over a finite field, for example Fp, this is not a problem because we can continually reduce mod p and keep the numbers involved relatively small. It should be noted that the associative law allows us to make these computations without worrying about what order we use to combine the summands [8].

When the sum of the points P and Q on the elliptic curve E is shown in Figure 1. The result is determined that the point S is obtained by reversing the sign of the y coordinate of the point R, where R is the intersection point of E and the

line through P and Q. If P and Q are in the same position, the line is the tangent of E at P. In addition, the sum of the points at infinity and the point P is determined to be exactly the point P as Figure 2.

III. Description of the algorithm

When two communicating parties Alice and Bob want to transmit the messages, they agree upon to use an elliptic curve $E_p(a, b)$ where p is a prime number and a random point C on the elliptic curve. Alice chooses a great random number α which is less than the order of $E_p(a, b)$ and a point A on the elliptic curve. Alice computes $A_1 = \alpha(C + A)$ and $A_2 = \alpha A$. She keeps the random number α and the point A as her private keys and publishes A_1 and A_2 as her general public keys. Similarly, Bob selects a large random number β and a point B on the elliptic curve. He computes $B_1 = \beta(C+B)$ and $B_2 = \beta B$. He keeps the random number β and point B as his private keys and publishes B_1 and B_2 as his general public keys. After publishing the public keys, the communicating parties again calculate the following quantities and publish them as their specific public keys of each other.

Alice calculates $A_B = \alpha B_2$ and publishes it as her specific public key for Bob calculates $B_A = \beta A_2$ and publishes it as his specific public key for Alice

Alice's private key 1 = α, a large random number less than the order of the generator.

Alice's private key 2 = a point A on the elliptic curve $E_p(a,b)$ Alice's general public key 1 = a point A_1 on the elliptic curve $E_p(a,b)$

Alice's general public key 2 = a point A_2 on the elliptic curve $E_p(a, b)$

Alice's specific public key for Bob = a point AB on the elliptic curve $E_p(a, b)$

Bob's private key 1 = β, a large random number less than the order of the generator

Bob's private key 2 = B, a point on the elliptic curve $E_p(a,b)$

Bob's general public key 1 = B_1, a point on the elliptic curve $E_p(a, b)$

Bob's general public key 2 = B_2, a point on the elliptic curve $E_p(a,b)$ Bob's specific public key for Alice = B_A, a point on the elliptic curve E_p (a, b) [10]

A. Encryption

If Bob wants to communicate the message M then all the characters of the Vietnamese text are coded to the points on the elliptic curve using the code table which is agreed upon by the communicating parties Alice and Bob. Then each message point is encrypted to a pair of cipher points E_1, E_2. He uses a random number γ which is different for the encryption of different message points.

$E_1 = \gamma C$

$E_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B$

After encrypting all the characters of the message Bob converts the pair of points of each message point into the text characters using the code table. Then he communicates the ciphertext to Alice in a public channel.

B. Decryption

After receiving the ciphertext, Alice converts the ciphertext into the points on the elliptic curve and recognizes the points E_1 and E_2 of each character. Then she decrypts the message as follows. $M = E_2 - (\alpha E_1 + \alpha B_1 + B_A)$

C. Decryption works out properly

$(\beta + \gamma)A_1 - \gamma A_2 + A_B = \gamma(A_1 - A_2) + \beta A_1 + A_B$

$= \gamma\alpha C + \beta\alpha C + \beta\alpha A + \beta\alpha B$

$= \gamma\alpha C + \beta\alpha(A+B+C)$

$\alpha E_1 + \alpha B_1 + B_A = \alpha\gamma C + \alpha\beta C + \alpha\beta B + \alpha\beta A$

$= \gamma\alpha C + \beta\alpha(A+B+C)$

Therefore, $(\beta + \gamma)A_1 - \gamma A_2 + A_B = \alpha E_1 + \alpha B_1 + B_A$

$E_2 - (\alpha E_1 + \alpha B_1 + B_A = [M + (\beta + \gamma)A_1 - \gamma A_2 + A_3] - [\alpha E_1 + \alpha B_1 + B_A]$

$= M + [\gamma\alpha C + \beta\alpha(A+B+C)] - [\gamma\alpha C + \beta\alpha(A+B+C)]$

$= M$ [10]

In this method a group of communicating parties A, B, C, D…can communicate with one

another securely, non-repudiatively in an authentic manner. Here each communicating party say X publishes two general public keys X_1, X_2. X also publishes a specific public key X_Y to be used by the communicating party Y for communication with Y. When Y wants to communicate with X, Y uses the general public keys of X (X_1, X_2), the specific public key published by X for Y (X_Y) and Y's secret key y. To decrypt the message X uses Y's general public keys (Y_1, Y_2), the specific public key published by Y for X (Y_X) and X's secret key x. Here X creates specific public key X_Y for Y using Y's public keys and X's secret key. So, this method of encryption using elliptic curves over finite fields is highly suitable for communication between groups of corporate/ government institutions.

IV. Implement Vietnamese text encryption of the above algorithm.

Alice sends Bod a plaintext (input document) as "VIỆT NAM". To ensure the confidentiality of the transmission process, Alice will encrypt the plaintext before sending it on the channel. The encoding process is presented as follows:

Determine the total number of points on an elliptic curve, and find P as a point generator.

For curve E at "(1)" we have 131 points on the curve including the infinity. We find the point P = (7, 9). Using the formula "(4)" and formula "(5)" calculates points on the curve as the set of points below.

{∞, (7, 9), (43, 78), (28, 55), (30, 73), (79, 117), (90, 75), (23, 129), (61, 3), (59, 74), (118, 26), (11, 53), (103, 47), (70, 79), (113, 74), (71, 96), (47, 93), (63, 68), (37, 14), (68, 4), (111, 77), (57, 108), (109, 17), (106, 65), (78, 7), (133, 20), (54, 127), (132, 106), (9, 124), (128, 53), (34, 57), (84, 24), (52, 40), (108, 11), (91, 32), (105, 80), (94, 23), (72, 78), (48, 110), (24, 61), (0, 86), (114, 56), (124, 89), (89, 87), (21, 76), (41, 7), (129, 129), (99, 19), (119, 3), (104, 93), (32, 41), (137, 47), (42, 77), (126, 10), (55, 49), (97, 55), (98, 136), (8, 95), (14, 84), (125, 77), (107, 103), (102, 138), (20, 7), (38, 92), (18, 114), (127, 46), (127, 93), (18, 25), (38, 47), (20, 132), (102, 1), (107, 36), (125, 62), (14, 55), (8, 44), (98, 3), (97, 84), (55, 90), (126, 129), (42, 62), (137, 92), (32, 98), (104, 46), (119, 136), (99, 120), (129, 10), (41, 132), (21, 63), (89, 52), (124, 50), (114, 83), (0, 53), (24, 78), (48, 29), (72, 61), (94, 116), (105, 59), (91, 107), (108, 128), (52, 99), (84, 115), (34, 82), (128, 86), (9, 15), (132, 33), (54, 12), (133, 119), (78, 132), (106, 74), (109, 122), (57, 31), (111, 62), (68, 135), (37, 125), (63, 71), (47, 46), (71, 43), (113, 65), (70, 60), (103, 92), (11, 86), (118, 113), (59, 65), (61, 136), (23, 10), (90, 64), (79, 22), (30, 66), (28, 84), (43, 61), (7, 130)}

Let C = (23, 129). Alice selects a random number α = 3, any point A = (32, 98) on the elliptic curve. She computes

$A_1 = \alpha(C+A) = 3[(23, 129) + (32, 98)] = (43, 78)$

$A_2 = \alpha A = 3(32, 98) = (68, 135).$

She keeps the random number α = 3 and the point A on the elliptic curve as her secret keys and publishes A_1 and A_2 as her public keys. Bob selects β = 5, B = (78, 132) on the elliptic curve. He computes

$B_1 = \beta(C+B) = 5[(23, 129) + (78, 132)] = (105, 80)$

$B_2 = \beta B = 5(78, 132) = (11, 53).$

He keeps the random number β = 5 and the point B on the elliptic curve as his secret keys and publishes B_1 and B_2 as his public keys.

Alice calculates $A_B = \alpha B_2 = 3(11, 53) = (108, 11)$ and Bob calculates $B_A = \beta A_2 = 5(68, 135) = (8, 44)$. Alice publishes A_B as the specific public key for Bob and Bob publishes B_A as specific public key for Alice.

A. Encryption

When Bob wants to communicate the message 'Việt Nam' to Alice, Bob converts all the text characters of the message into the points on the elliptic curves using the agreed-upon code table.

TABLE I. CHARACTERS CORRESPONDING TO POINTS ON THE CURVE CONSIDERED FROM POINT P

~ ∞	a (7, 9)	à (43, 78)	ã (28, 55)
ả (30, 73)	á (79, 117)	ạ (90, 75)	ă (23, 129)
ằ (61, 3)	ẵ (59, 74)	ẳ (118, 26)	ắ (11, 53)
ặ (103, 47)	â (70, 79)	ầ (113, 74)	ẫ (71, 96)
ẩ (47, 93)	ấ (63, 68)	ậ (37, 14)	b (68, 4)
c (111, 77)	d (57, 108)	đ (109, 17)	e (106, 65)
è (78, 7)	ẽ (133, 20)	ẻ (54, 127)	é (132, 106)
ẹ (9, 124)	ê (128, 53)	ề (34, 57)	ễ (84, 24)
ể (52, 40)	ế (108, 11)	ệ (91, 32)	f (105, 80)
g (94, 23)	h (72, 78)	i (48, 110)	ì (24, 61)
ĩ (0, 86)	ỉ (114, 56)	í (124, 89)	ị (89, 87)
k (21, 76)	l (41, 7)	m (129, 129)	n (99, 19)
o (119, 3)	ò (104, 93)	õ (32, 41)	ỏ (137, 47)
ó (42, 77)	ọ (126, 10)	ô (55, 49)	ồ (97, 55)
ỗ (98, 136)	ổ (8, 95)	ố (14, 84)	ộ (125, 77)
ơ (107, 103)	ờ (102, 138)	ỡ (20, 7)	ở (38, 92)
ớ (18, 114)	ợ (127, 46)	p (127, 93)	q (18, 25)
r (38, 47)	s (20, 132),	t (102, 1)	u (107, 36)
ù (125, 62)	ũ (14, 55)	ủ (8, 44)	ú (98, 3)
ụ (97, 84)	ư (55, 90)	ừ (126, 129)	ữ (42, 62)
ử (137, 92)	ứ (32, 98)	ự (104, 46)	v (119, 136)
x (99, 120)	y (129, 10)	ỳ (41, 132)	ỹ (21, 63)
ỷ (89, 52)	ý (124, 50)	ỵ (114, 83)	z (0, 53)
0 (24, 78)	1 (48, 29)	2 (72, 61)	3 (94, 116)
4 (91, 107)	5 (105, 59)	6 (108, 128)	7 (52, 99)
8 (84, 115)	9 (34, 82)	space (128, 86)	. (9, 15)
, (132, 33)	; (54, 12)	? (133, 119)	! (78, 132)
@ (106, 74)	# (109, 122)	$ (57, 31)	% (111, 62)
^ (68, 135)	& (37, 125)	- (63, 71)	+ (47, 46)
* (71, 43)	/ (113, 65)	((70, 60)	) (103, 92)
[(11, 86)	] (118, 113)	{ (59, 65)	} (61, 136)
= (23, 10)	| (90, 64)	< (79, 22)	> (30, 66)
_ (28, 84)	: (43, 61)	‘ (7, 130)	

In a cell, the upper part is the character, the bottom is the point on the Elliptic curve. As can be seen, there are 131 characters including spaces. The order of alphabetic characters is referenced in specialists [11], the phonetic Room-Vietnam Institute of Linguistics.

a) In the message ‘Việt Nam’ the first character ‘V’ corresponds to the point (119, 136) using the code TABLE I. Bob selects a random number $\gamma = 6$ for encrypting the character ‘V’. Then the point (119, 136) is encrypted as $E_1 = \gamma C = 6(23, 129) = (124, 89)$ which corresponds to the character ‘í’ in the conversion table. $E_2 = M + (\beta + \gamma) A_1 - \gamma A_2 + A_B = (118, 113)$ which corresponds to ‘]’ in the code TABLE I. So, the character ‘V’ in the plain text is encrypted to two characters {í,]} in the ciphertext.

b) The same ‘i’ is a point (48, 110) in the code TABLE I. Let $\gamma = 10$

$E_1 = 10(23, 129) = (102, 1)$ which corresponds to ‘t’ in the code TABLE I.

$E_2 = M + (\beta + \gamma) A_1 - \gamma A_2 + A_B = (128, 53)$ which corresponds to 'ê' in the code TABLE I. So, 'i' is encrypted as {t, ê}

c) 'ệ' is a point (91, 32) in the code TABLE I. Let $\gamma = 17$

$E_1 = 17(23, 129) = (103, 92)$ which corresponds to ')' in the code TABLE I.

$E_2 = M + (\beta + \gamma) A_1 - \gamma A_2 + A_B = (114, 56)$ which corresponds to 'ỉ' in the code TABLE I. So, 'ệ' is encrypted as {), ỉ}.

d) 't' is a point (102, 1) in the code TABLE I. Let $\gamma = 4$

$E_1 = 4(23, 129) = (9, 124)$ which corresponds to 'ẹ' in the code TABLE I.

$E_2 = M + (\beta + \gamma) A_1 - \gamma A_2 + A_B = (127, 93)$ which corresponds to 'p' in the code TABLE I. So, 't' is encrypted as {ẹ, p}.

e) ' ' (space) is a point (128, 86) in the code TABLE I. Let $\gamma = 8$

$E_1 = 8(23, 129) = (98, 136)$ which corresponds to 'ỗ' in the code TABLE I.

$E_2 = M + (\beta + \gamma) A_1 - \gamma A_2 + A_B = (137, 92)$ which corresponds to 'ử' in the code TABLE I. So, ' ' (space) is encrypted as {ỗ, ử}.

f) 'N' is a point (99, 19) in the code TABLE I. Let $\gamma = 21$

$E_1 = 21(23, 129) = (47, 93)$ which corresponds to 'ẩ' in the code TABLE I.

$E_2 = M + (\beta + \gamma) A_1 - \gamma A_2 + A_B = (23, 129)$ which corresponds to 'ă' in the code TABLE I. So, 'N' is encrypted as {ẩ, ă}.

g) 'a' is a point (7, 9) in the code TABLE I. Let $\gamma = 12$

$E_1 = 12(23, 129) = (99, 120)$ which corresponds to 'x' in the code TABLE I.

$E_2 = M + (\beta + \gamma) A_1 - \gamma A_2 + A_B = (91, 32)$ which corresponds to 'ệ' in the code TABLE I. So, 'a' is encrypted as {x, ệ}.

h) 'm' is a point (129,129) in the code TABLE I. Let $\gamma = 29$

$E_1 = 29(23, 129) = (68, 135)$ which corresponds to '^' in the code TABLE I.

$E_2 = M + (\beta + \gamma) A_1 - \gamma A_2 + A_B = (89, 87)$ which corresponds to 'ị' in the code TABLE I. So, 'a' is encrypted as {^, ị}.

Bob communicates { í,]; t, ê;), ỉ; ẹ, p; ỗ, ử; ẩ, ă; x, ệ; ^, ị}as the ciphertext to Alice in public channel.

B. Decryption

Alice after receiving the cipher text { í,]; t, ê;), ỉ; ẹ, p; ỗ, ử; ẩ, ă; x, ệ; ^, ị} converts the cipher characters into the points (124, 89), (118, 113), (102, 1), (128, 53), (103, 92), (114, 56), (9, 124), (127, 93), (98, 136), (137, 92), (47, 93), (23, 129), (99, 120), (91, 32), (68, 135), (89, 87). She decrypts the message taking two points at a time as the points E_1 and E_2.

a) $M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (119, 136)$ which corresponds to the character 'V' in the code TABLE I.

b) $M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (48, 110)$ which corresponds to the character 'i' in the code TABLE I.

c) $M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (91, 32)$ which corresponds to the character 'ệ' in the code TABLE I.

d) $M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (102, 1)$ which corresponds to the character 't' in the code TABLE I.

e) $M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (128, 86)$ which corresponds to the character ' ' (space) in the code TABLE I.

f) $M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (99, 19)$ which corresponds to the character 'N' in the code TABLE I.

g) $M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (7, 9)$ which corresponds to the character 'a' in the code TABLE I.

h) $M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (129, 129)$ which corresponds to the character 'm' in the code TABLE I.

Then 'Việt Nam' is the original message (plaintext).

V. CONCLUSION

We have presented above, that the communicating parties agree upon to use an elliptic curve and a point C on the elliptic curve. With the Elliptic curve equation to be proposed, it has a sufficient number of points to contain the number of characters in the Vietnamese string. The elliptic curve parameters for cryptographic schemes should be carefully chosen to resist all known attacks of the Elliptic Curve Discrete Logarithmic Problem (ECDLP). Each message point is encrypted as a pair of points on the elliptic curve. Here a random number γ is used in the encryption of each message point and γ is different for the encryption of different message points. That is why the same characters in the message space are encrypted to different characters in the cipher space. The difference between the characters of the plain text is not the same as the difference between the characters of the ciphertext. Due to this, the linear cryptanalysis is highly difficult. In addition to this each character of the message is coded to the point on the elliptic curve using the code table which is agreed upon by the communicating parties and each message point is encrypted to a pair of points on the elliptic curve. Hence, the method of encryption proposed here provides sufficient security against cryptanalysis at a relatively low computational overhead. Moreover, the security of the Elliptic Curve Cryptography depends on the difficulty of finding the value of k, given kP where k is a large number and P is a random point on the elliptic curve. This is the Elliptic Curve Discrete Logarithmic Problem. The straightforward use of public key encryption provides confidentiality, but not authentication. Each communicating party publishes a specific public key for the communication with a specific communicator. With this, the receiver is assured that the cipher was constructed by the sender only because the sender uses the receiver's general public keys, the receiver's specific public key published for the sender alone, and the sender's private key for constructing the cipher. This ensures that the sender has "digitally signed" the message by using the specific public key published for him alone by the receiver. Hence, the cipher has achieved the qualities of confidentiality, authentication, and non-repudiation.

REFERENCES

[18] N.Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation", 203 – 209, 1987.

[19] V.Miller, "Uses of elliptic curves in cryptography, Advances in Cryptology – Crypto", Lecture Notes in Computer Science, SpringerVerlag, 417 -426, 1986.

[20] S.Sugantha Priya, Dr.M.Mohanraj, "A Review on Secure Elliptic Curve Cryptography (ECC) and Dynamic Secure Routing Link Path Detection Algorithm (DSRLP) Under Jamming Attack", ISSN: 0474-9030, Vol-68-Issue-30, February. 2020.

[21] Negin Dinarvand, Hamid Barati , "An efficient and secure RFID authentication protocol using elliptic curve cryptography", Springer Science+Business Media, LLC, 2017

[22] Utku Gulen, Selcuk Baktir, "Elliptic Curve Cryptography for Wireless Sensor Networks Using the Number Theoretic Transform", journal-sensors, Published: 9 March. 2020.

[23] D. Sravana Kumar, CH. Suneetha, A. ChandrasekhAR , "Encryption of Data Using Elliptic Curve Over Finite Fields", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January. 2012.

[24] Alfred J. Menezes and Scott A. Vanstone, "Elliptic Curve Cryptosystems and their implementations", Journal of Cryptology, Volume-6, Number-4, pages 209-224, 1993.

[25] Enge A. "Elliptic curves and their applications to cryptography", Norwell, MA: Kulwer Academic publishers, 1999.

[26] Neil Koblitz, "An Elliptic Curve implementation of the finite field digital signature algorithm", in Advances in cryptology,(CRYPTO 1998), Springer Lecture Notes in computer science, 1462, 327-337, 1998.

[27] D. Sravana Kumar, CH. Suneetha, A. ChandrasekhAR "Encryption of data using Elliptic curve over finite fields", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[28] Vu Thi Hai Ha, Dinh Thi Hang, Bui Dang Binh, "The influence of volume on the formant of vowels and the identification of Vietnamese speakers", Vietnam Institute of Linguistics, 2015.

ABOUT THE AUTHORS

Mai Manh Trung

Education: Vietnam National University, Hanoi.

Workplace: Currently a lecturer at the University of Economics Technology for Industries and researcher at the University of Engineering and Technology, Vietnam National University, Hanoi.

Email: mmtrung@uneti.edu.vn

Research field: Cryptography, lightweight cryptography, security for IoT networks, artificial intelligence, application programming.

Le Phe Do

Workplace: Faculty of Information Technology, University of Technology - Vietnam National University, Hanoi

Email: dolp@vnu.edu.vn

Research field: Advanced Mathematics, Statistical Probability, Cryptography, Light Cryptography, Information Security.

Do Trung Tuan

Workplace: University of Science - Vietnam National University, Hanoi

Email: tuandt@vnu.edu.vn

Research field: Database, Data Science, Data Mining, Data Security.