DOI: 10.15625/vap.2020.00235

XÂY DỰNG HỆ MẬT MÃ ĐƯỜNG CONG ELLIPTIC VỚI KHÓA ĐỐI XỨNG AFFINE ĐỂ MÃ HÓA GIẢI MÃ VĂN BẢN TIẾNG VIỆT

Mai Mạnh Trừng[1,3], Đỗ Trung Tuấn[2], Lê Phê Đô[3], Lê Trung Thực[4], Đào Thị Phương Anh[1]

[1]Khoa Công nghệ thông tin, Trường Đại học Kinh tế Kỹ thuật Công nghiệp
[2]Trường Đại học Khoa học Tự nhiên, Đại học Quốc gia Hà Nội
[3]Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
[4]Khoa Công nghệ thông tin, Trường Đại học Công nghệ Đông Á

mmtrung@uneti.edu.vn, tuandt@vnu.edu.vn, dolp.cntt@gmail.com, thuclt12a@gmail.com, dtpanh@uneti.edu.vn

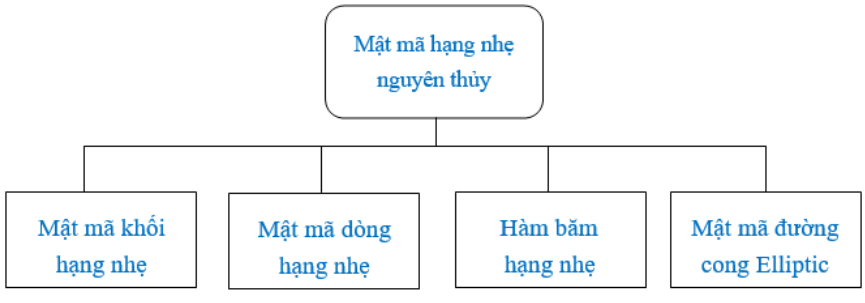
TÓM TẮT: *Mật mã đường cong Elliptic là một hướng trong mật mã nguyên thủy hạng nhẹ. Bài báo này dựa trên ý tưởng khóa đối xứng của mật mã Affine, hệ mật đường cong Elliptic (ECC- Elliptic Curve Cryptography). Số học đường cong Elliptic có thể được sử dụng để phát triển các sơ đồ mã hóa đường cong Elliptic bao gồm trao đổi khóa, mã hóa và chữ ký số. Điểm thu hút chính của mật mã đường cong Elliptic so với RSA là nó cung cấp bảo mật tương đương nhưng cho kích thước khóa nhỏ hơn, do đó giảm chi phí xử lý. Để mã hóa văn bản tiếng Việt, chúng tôi dựa trên âm thanh của các ký tự tiếng Việt để tạo một bảng các ký tự này theo thứ tự. Để tăng tính bảo mật chúng tôi áp dụng thuật toán tạo chuỗi dữ liệu. Sau đó, xây dựng thuật toán mã hóa mới bằng cách sử dụng các đường cong Elliptic trên các trường hữu hạn với các khóa đối xứng AFFIN để mã hóa văn bản tiếng Việt này. Thuật toán đề xuất được đã được cài đặt và thử nghiệm thành công trên ngôn ngữ lập trình C# 2019.*

Từ khóa: *Đường cong Elliptic, hệ mật mã Affine, mã hóa hạng nhẹ, thuật toán tạo chuỗi.*

I. GIỚI THIỆU

Mật mã hạng nhẹ (mật mã nhẹ) là một nhánh của mật mã hiện đại, bao gồm các thuật toán mật mã được thiết kế để sử dụng trong các thiết bị có tài nguyên hạn chế [1]. Với các hạn chế về tài nguyên này buộc các nhà nghiên cứu mật mã phải thiết kế các thuật toán nhẹ với kích thước khối và độ dài khóa nhỏ hoặc tương đối nhỏ.

Trong mật mã nguyên thủy hạng nhẹ có 4 hướng chính đó là mật mã khối, mật mã dòng, hàm băm, mật mã ECC ngoài ra còn có mật mã xác thực thông báo [2].



Hình 1. Các nhóm mật mã hạng nhẹ

Nghiên cứu về các đường cong Elliptic của các nhà đại số, các nhà lý thuyết số có từ giữa thế kỷ XIX. Mật mã đường cong Elliptic (ECC) được phát hiện vào năm 1985 bởi Neil Koblitz và Victor Miller [3, 4]. Chúng có thể được xem như các đường cong Elliptic của các hệ mật mã logarit rời rạc. Trong đó nhóm $\boldsymbol{Z_P^*}$ được thay thế bằng nhóm các điểm trên một đường cong Elliptic trên một trường hữu hạn. Cơ sở toán học cho tính bảo mật của các hệ thống mật mã đường cong Elliptic là tính hấp dẫn tính toán của bài toán logarit rời rạc đường cong Elliptic (ECDLP).

Những năm gần đây ở Việt Nam, đường cong Elliptic có vai trò quan trọng, theo Thông tư số: 39/2017/TT-BTTTT, ngày 15 tháng 12 năm 2017 của Bộ Thông tin và Truyền thông về việc Ban hành Danh mục tiêu chuẩn kỹ thuật ứng dụng công nghệ thông tin trong cơ quan Nhà nước đã khuyến nghị áp dụng giải thuật mã hóa trên đường cong Elliptic của Tiêu chuẩn về an toàn thông tin.

ECC hiện đang được sử dụng trong một loạt các ứng dụng: Chính phủ Mỹ sử dụng để bảo vệ thông tin liên lạc nội bộ, các dự án Tor sử dụng để giúp đảm bảo ẩn danh, đây cũng là cơ chế được sử dụng để chứng minh quyền sở hữu trong Bitcoins, cung cấp chữ ký số trong dịch vụ iMessage của Apple, để mã hóa thông tin DNS với DNSCurve và là phương pháp tốt để xác thực cho các trình duyệt web an toàn qua SSL/TLS. Thế hệ đầu tiên của thuật toán mã hóa khóa công khai như RSA và Diffie-Hellman vẫn được duy trì trong hầu hết các lĩnh vực, nhưng ECC đang nhanh chóng trở thành giải pháp thay thế cho RSA.

Hệ mật đường cong Elliptic được ứng dụng trong thương mại điện tử với tài nguyên hạn chế [5], trong công nghệ nhận dạng đối tượng bằng sóng vô tuyến hiệu quả và an toàn [6], trong các mạng cảm biến không dây sử dụng phép biến đổi lý thuyết số [7]. Trong bài báo [8], các tác giả đã trình bày việc triển khai ECC bằng cách trước tiên là

chuyển đổi thông điệp thành một điểm affine trên đường cong Elliptic, sau đó áp dụng thuật toán đọc chuỗi trên bản rõ. Với chúng tôi trong công việc mã hóa và giải mã, đầu vào là bản rõ văn bản, mỗi ký tự được xác định là một điểm trên đường cong Elliptic. Sử dụng khóa đối xứng là một cặp giá trị ngẫu nhiên để mã hóa và giải mã. Vận dụng ý tưởng tạo chuỗi chúng tôi áp dụng đọc chuỗi điểm của tọa độ trên đường cong. Đầu ra là một bản mã gồm dãy số của các điểm trên đường cong Elliptic.

II. CƠ SỞ TOÁN HỌC ĐƯỜNG CONG ELLIPTIC

Đường cong Elliptic E trên trường hữu hạn GF(p) trong đó p là số nguyên tố, là tập hợp các điểm (x, y) thỏa mãn phương trình sau: $E: y^2 = x^3 + ax + b$ (1)

trong đó a, b là số nguyên modulo p, thỏa mãn: $4a^3 + 27b^2 \neq 0$ đảm bảo rằng là đường cong Elliptic. Tức là, không có điểm nào đó của đường cong có hai hoặc nhiều đường tiếp tuyến khác biệt. Và bao gồm một điểm ∞ gọi là điểm vô cực. Đối với các giá trị đã cho của a và b, đồ thị bao gồm giá trị dương và giá trị âm của y cho mỗi giá trị của x. Do đó đường cong này đối xứng với trục x. Chúng tôi cũng minh họa việc triển khai hệ thống mật mã dựa trên một đường cong Elliptic với khóa đối xứng với phương trình đường cong Elliptic nhóm lựa chọn là:

$$y^2 = x^3 - 2x + 3 \pmod{137} \quad (2)$$

Với phương trình (2) thì a = -2, b = 3, ta có $4\times(-2)^3 + 27\times (3)^2 = 211 \neq 0$. Do vậy, phương trình (2) là phương trình đường cong Elliptic. Chúng tôi chọn phương trình này bởi lẽ tìm được tổng số điểm của đường cong là 131 điểm. Do vậy, tổng số điểm là số nguyên tố thì tất cả các điểm trên đường cong đều là điểm sinh. Ngoài ra, với số điểm này đủ để chứa các ký tự trên bảng chữ cái tiếng Anh và tiếng Việt, một số ký tự đặc biệt.

A. Phép cộng

Giả sử $P = (x_p, y_p)$ và $Q = (x_q, y_q)$ là hai điểm của E. Nếu $x_p = x_q$ và $y_p = - y_q$ thì ta định nghĩa $P + Q = \infty$. Ngược lại thì $P + Q = R = (x_r, y_r) \in E$ trong đó $x_r = \gamma^2 - x_p - x_q$, $y_r = \gamma(x_p - x_r) - y_p$, với:

$$\gamma = \begin{cases} \dfrac{y_q - y_p}{x_q - x_p}, & \text{khi } P \neq Q \\ \dfrac{3x_p^2 + a}{2y_p}, & \text{khi } P = Q \end{cases}$$

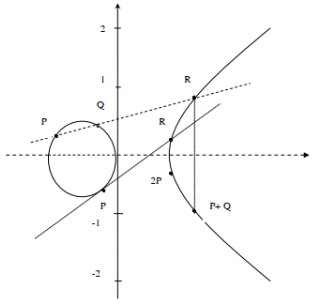
Vậy nếu $P \neq Q$ tức là $x_p \neq x_q$, ta có:

$$\begin{cases} \mathbf{x_r = \left(\dfrac{y_q - y_p}{x_q - x_p}\right)^2 - x_p - x_q} \\ \mathbf{y_r = \left(\dfrac{y_q - y_p}{x_q - x_p}\right)(x_p - x_r) - y_p} \end{cases} \quad (\mathbf{3})$$

Nếu P = Q tức là $x_p = x_q$, ta có:

$$\begin{cases} \mathbf{x_r = \left(\dfrac{3{x_p}^2 + a}{2y_p}\right)^2 - 2x_p} \\ \mathbf{y_r = \left(\dfrac{3{x_p}^2 + a}{2y_p}\right)(x_p - x_r) - y_p} \end{cases} \quad (\mathbf{4})$$

Chú ý rằng các điểm (x_r, y_r), $(x_r, -y_r)$ cũng nằm trên đường cong E và xét về mặt hình học, thì các điểm (x_p, y_p), (x_q, y_q), $(x_r, -y_r)$ cũng nằm trên một đường thẳng. Ngoài ra, định nghĩa một điểm cộng vô cực bằng chính nó. $P + \infty = \infty + P = P$.



Hình 2. Tổng hai điểm của đường cong Elliptic

B. Phép nhân

Phép nhân một số nguyên k với một điểm P thuộc đường cong Elliptic E là điểm Q được xác định bằng cách cộng k lần điểm P và dĩ nhiên Q ∈ E: k × P = P + P + P……+ P (k phép cộng điểm P). Vì vậy nếu G là một điểm thuộc đường cong Elliptic E thì với mỗi số nguyên dương k luôn dễ dàng xác định được điểm Q = k×G.

Khi tổng các điểm P và Q trên đường cong Elliptic E được chỉ ra trong Hình 2. Kết quả được xác định là điểm S thu được bằng cách đảo ngược dấu của tọa độ y của điểm R, trong đó R là giao điểm của E và đường thẳng đi qua P và Q. Nếu P và Q ở cùng một vị trí, đường thẳng là tiếp tuyến của E tại P. Ngoài ra, tổng điểm tại vô cực và điểm P được xác định là chính điểm P.

III. THUẬT TOÁN ĐỀ XUẤT – AECC (Affine Elliptic Curve Cryptography)

Thành phần mật mã: ($\mathcal{P}$, $\mathcal{C}$,$\mathcal{E}$,$\mathcal{D}$,$\mathcal{K}$)

$\mathcal{P}$: Là bản rõ

$\mathcal{C}$: Là bản mã

$\mathcal{E}$: Là hàm mã hóa

$\mathcal{D}$: Là hàm giải mã

$\mathcal{K}$: Là khóa

Sinh chuỗi:

Theo [8] sinh chuỗi dựa vào hệ đếm cơ số 3.

Bước 1: Xác định tổng số điểm của đường cong Elliptic, tìm điểm sinh của đường cong Elliptic.

Bước 2: Chuyển đổi tổng số điểm (n) sang hệ đếm cơ số 3. Tìm được m là số chữ số của chuỗi số vừa đổi. Ví dụ n =89 ta được dãy số 10022. Ta có m = 5.

Bước 3: Lập ma trận M với kích thước (n + 1) × m. Trong đó n + 1 là số hàng, n là tổng số điểm của đường cong E, m là số cột (m số chữ của một hàng). Ta có ma trận:

$$M = \begin{pmatrix} a_{0,0}a_{0,1} \dots \dots a_{0,m} \\ a_{1,0}a_{1,1} \dots \dots a_{1,m} \\ a_{2,0}a_{2,1} \dots \dots a_{2,m} \\ \dots \dots \\ a_{n,0}a_{n,1} \dots \dots a_{n,m} \end{pmatrix}$$

Ví dụ với n = 89 ta có kích thước của ma trận M là 90 × 5.

$$M = \begin{pmatrix} 00000 \\ 00001 \\ 00002 \\ 00010 \\ \dots \dots \\ 10022 \end{pmatrix}$$

Bước 4: Dịch chuyển 1 phần tử của hàng ở ma trận M sang phải

$$[a_{i,0}\ \ a_{i,1}\,a_{i,2}\dots.a_{i,m-1}] = [a_{i,m-1}\ a_{i,0}\ \ a_{i,1}\,a_{i,2}\ \dots.a_{i,m-2}]$$

Bước 5: Trình tự được hình thành là:

$S:[S_0 = [a_{0,m-1}\ \ a_{0,0}\ \ a_{0,1}\ \ a_{0,2}\dots a_{0,m-2}],\ S_1 = [a_{1,m-1}\ \ a_{1,0}\ \ a_{1,1}\ \ a_{1,2}\dots a_{2,m-2}],\dots,\ S_n = [a_{n,m-1}\ \ a_{n,0}\ \ a_{n,1}\ \ a_{n,2}\dots a_{n,m-2}]]$

Mã hóa:

Bước 6: Chọn giá trị khóa $\mathcal{K}$ (u, v) ∈ Z_n x Z_n . Khóa là ngẫu nhiên thỏa mãn: UCLN (u, n) = 1, trong đó n là tổng điểm điểm trên đường cong Elliptic. Với k = (u, v) ∈ $\mathcal{K}$, ta định nghĩa:

Bước 7: Hàm mã hóa

$$\mathcal{C} = \mathcal{E}(\mathcal{P}) = [(u \times \mathcal{P}_i + v) \bmod (n)]P \quad (5)$$

Bước 8: Đọc chuỗi số của tọa độ điểm mã hóa theo bước 5. Ta được chuỗi mã nhị phân gửi cho bên B.

Giải mã:

Bước 9: Xét đoạn gồm m chữ số của chuỗi số mã hóa rồi dịch chuyển 1 phần tử sang trái và chuyển đổi dãy số cơ số 3 nhận này sang thập phân ta tìm được tọa độ điểm.

Bước 10: Hàm giải mã

$$\mathcal{P} = \mathcal{D}(\mathcal{C}) = [u^{-1}(\mathcal{C}_i - v) \bmod (n)]P \quad (6)$$

Trong đó tham số ở (5), (6):

$\mathcal{P}_i$: Là vị trí của ký tự bản rõ

$\mathcal{C}_i$: Là vị trí của ký tự bản mã

$\mathcal{E}$: Là hàm mã hóa

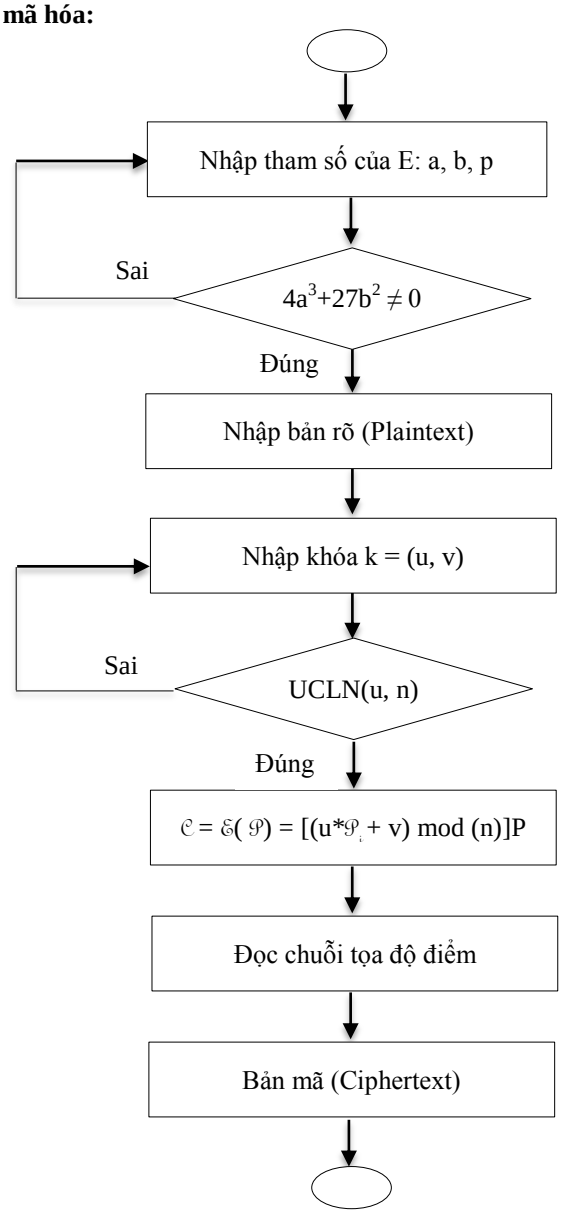
$\mathcal{D}$: Là hàm giải mã

u, v: Là một số nguyên của khóa, là một giá trị ngẫu nhiên, u thỏa mãn là số nguyên tố cùng nhau với n.

n: Là tổng số điểm trên đường cong Elliptic.

P: Là điểm sinh của đường cong Elliptic.

Lưu đồ thuật toán mã hóa:



Hình 3. Lưu đồ thuật toán mã hóa AECC

IV. ÁP DỤNG THUẬT TOÁN

Bên A gửi cho bên B một bản rõ (văn bản đầu vào) là Khánh Hòa. Để đảm bảo bí mật trên quá trình truyền. Bên A sẽ mã hóa bản rõ trên trước khi gửi trên kênh truyền. Quá trình mã hóa được thể hiện như sau:

Bước 1: Xác định tổng số điểm của đường cong Elliptic, tìm điểm sinh của đường cong Elliptic.

Với đường cong E ở (2) ta có 131 điểm trên đường cong tính cả điểm vô cực. Ta tìm được điểm sinh P = (51, 22). Sử dụng công thức (3) và công thức (4) điểm tính các điểm trên đường cong như Bảng 1.

Bảng 1. Tập hợp tất cả các điểm trên ECC

(51, 22)	(69, 56)	(73, 43)	(111, 120)	(134, 121)	(119, 57)	(72, 78)	(82, 78)
(65, 19)	(121, 130)	(80, 82)	(8, 15)	(117, 117)	(43, 85)	(120, 59)	(99, 125)
(12, 36)	(88, 51)	(116, 127)	(48, 25)	(39, 103)	(84, 98)	(38, 37)	(85, 91)
(5, 23)	(90, 95)	(132, 132)	(15, 103)	(136, 135)	(71, 32)	(118, 13)	(4, 123)
(126, 8)	(53, 35)	(41, 43)	(59, 77)	(55, 19)	(23, 94)	(78, 67)	(26, 111)
(49, 75)	(20, 47)	(36, 125)	(32, 85)	(76, 133)	(17, 118)	(113, 8)	(66, 30)
(83, 34)	(1, 31)	(35, 8)	(101, 37)	(44, 76)	(40, 128)	(63, 131)	(135, 37)
(127, 121)	(62, 52)	(2, 12)	(93, 126)	(74, 45)	(13, 16)	(92, 22)	(131, 115)
(81, 63)	(81, 74)	(131, 22)	(92, 115)	(13, 121)	(74, 92)	(93, 11)	(2, 125)
(62, 85)	(127, 16)	(135, 100)	(63, 6)	(40, 9)	(44, 61)	(101, 100)	(35, 129)
(1, 106)	(83, 103)	(66, 107)	(113, 129)	(17, 19)	(76, 4)	(32, 52)	(36, 12)
(20, 90)	(49, 62)	(26, 26)	(78, 70)	(23, 43)	(55, 118)	(59, 60)	(41, 94)
(53, 102)	(126, 129)	(4, 14)	(118, 124)	(71, 105)	(136, 2)	(15, 34)	(132, 5)
(90, 42)	(5, 114)	(85, 46)	(38, 100)	(84, 39)	(39, 34)	(48, 112)	(116, 10)
(88, 86)	(12, 101)	(99, 12)	(120, 78)	(43, 52)	(117, 20)	(8, 122)	(80, 55)
(121, 7)	(65, 118)	(82, 59)	(72, 59)	(119, 80)	(134, 16)	(111, 17)	(73, 94)
(69, 81)	(51, 115)	∞					

Bước 2: Chuyển đổi tổng số điểm (n) sang hệ đếm cơ số 3. Tìm được m là số chữ số của chuỗi số vừa chuyển đổi.

Xác định đươc tổng số của đường cong là 131 điểm, tức là n = 131. Chuyển sang hệ đếm cơ số 3 ta được dãy số 11212. Ta có m = 5.

Bước 3: Lập ma trận m có kích thước 132 × 5

$$M = \begin{pmatrix} 00000 \\ 00001 \\ 00002 \\ 00010 \\ \dots\ \dots \\ 11212 \end{pmatrix}$$

Bước 4: Dịch chuyển 1 phần tử của hàng ở ma trận M sang phải. Ta được ma trận mới M^*

$$M^* = \begin{pmatrix} 00000 \\ 10000 \\ 20000 \\ 00001 \\ \dots\ \dots \\ 21121 \end{pmatrix}$$

Bước 5: Trình tự được hình thành là:

[00000], [10000], [20000], [00001], [10001], [20001], [00002], [10002], [20002], [00010], [10010], [20010], [00011], [10011], [20011], [00012], [10012], [20012], [00020], [10020], [20020], [00021], [10021], [20021], [00022], [10022], [20022], [00100],[10100], [20100], [00101], [10101], [20101], [00102], [10102], [20102], [00110], [10110], [20110], [00111], [10111], [20111], [00112], [10112], [20112], [00120], [10120], [20120], [00121], [10121], [20121], [00122],

[10122], [20122], [00200], [10200], [20200], [00201], [10201], [20201], [00202], [10202],[20202], [00210], [10210], [20210], [00211], [10211], [20211], [00212], [10212], [20212], [00220], [10220], [20220], [00221], [10221], [20221], [00222], [10222], [20222], [01000], [11000], [21000], [01001], [11001], [21001], [01002], [11002], [21002], [01010], [11010], [21010], [01011], [11011], [21011], [01012], [11012], [21012], [01020], [11020], [21020], [01021], [11021], [21021], [01022], [11022], [21022], [01100], [11100], [21100], [01101], [11101], [21101], [01102], [11102], [21102], [01110], [11110], [21110], [01111], [11111], [21111], [01112], [11112], [21112], [01120], [11120], [21120], [01121], [11121], [21121]

Mã hóa:

Bước 6: Chọn khóa ngẫu nhiên là $\mathcal{K}$ = (7, 23)

Bước 7, 8: Hàm mã hóa, đọc chuỗi số

Bảng 2. Ký tự ứng với điểm trên đường cong xét từ điểm P

(51, 22) **a**	(69, 56) **à**	(73, 43) **ã**	(111, 120) **ả**	(134, 121) **á**	(119, 57) **ạ**	(72, 78) **ă**	(82, 78) **ằ**
(65, 19) **ẵ**	(121, 130) **ẳ**	(80, 82) **ắ**	(8, 15) **ặ**	(117, 117) **â**	(43, 85) **ầ**	(120, 59) **ẫ**	(99, 125) **ẩ**
(12, 36) **ấ**	(88, 51) **ậ**	(116, 127) **b**	(48, 25) **c**	(39, 103) **d**	(84, 98) **đ**	(38, 37) **e**	(85, 91) **è**
(5, 23) **ẽ**	(90, 95) **ẻ**	(132, 132) **é**	(15, 103) **ẹ**	(136, 135) **ê**	(71, 32) **ề**	(118, 13) **ễ**	(4, 123) **ể**
(126, 8) **ế**	(53, 35) **ệ**	(41, 43) **f**	(59, 77) **g**	(55, 19) **h**	(23, 94) **i**	(78, 67) **ì**	(26, 111) **ĩ**
(49, 75) **ỉ**	(20, 47) **í**	(36, 125) **ị**	(32, 85) **k**	(76, 133) **l**	(17, 118) **m**	(113, 8) **n**	(66, 30) **o**
(83, 34) **ò**	(1, 31) **õ**	(35, 8) **ỏ**	(101, 37) **ó**	(44, 76) **ọ**	(40, 128) **ô**	(63, 131) **ồ**	(135, 37) **ỗ**
(127, 121) **ổ**	(62, 52) **ố**	(2, 12) **ộ**	(93, 126) **ơ**	(74, 45) **ờ**	(13, 16) **ỡ**	(92, 22) **ở**	(131, 115) **ớ**
(81, 63) **ợ**	(81, 74) **p**	(131, 22) **q**	(92, 115) **r**	(13, 121) **s**	(74, 92) **t**	(93, 11) **u**	(2, 125) **ù**
(62, 85) **ũ**	(127, 16) **ủ**	(135, 100) **ú**	(63, 6) **ụ**	(40, 9) **ư**	(44, 61) **ừ**	(101, 100) **ữ**	(35, 129) **ử**
(1, 106) **ứ**	(83, 103) **ự**	(66, 107) **v**	(113, 129) **x**	(17, 19) **y**	(76, 4) **ỳ**	(32, 52) **ỹ**	(36, 12) **ỷ**
(20, 90) **ý**	(49, 62) **ỵ**	(26, 26) **z**	(78, 70) **0**	(23, 43) **1**	(55, 118) **2**	(59, 60) **3**	(41, 94) **4**
(53, 102) **5**	(126, 129) **6**	(4, 14) **7**	(118, 124) **8**	(71, 105) **9**	(136, 2) **dấu cách**	(15, 34) **_**	(132, 5) **=**
(90, 42) **[**	(5, 114) **]**	(85, 46) **;**	(38, 100) **‘**	(84, 39) **,**	(39, 34) **.**	(48, 112) **!**	(116, 10) **?**
(88, 86) **@**	(12, 101) **$**	(99, 12) **%**	(120, 78) ^	(43, 52) **|**	(117, 20) **&**	(8, 122) **#**	(80, 55) **+**
(121, 7) **-**	(65, 118) *****	(82, 59) **:**	(72, 59) **/**	(119, 80) **(**	(134, 16) **)**	(111, 17) **{**	(73, 94) **}**
(69, 81) <	(51, 115) >	∞					

- Rõ điểm: Theo Bảng 2 ta có được các ký tự bản rõ tương ứng với số điểm cho kết quả ở bảng 3.

Bảng 3. Ký tự ứng với điểm trên đường cong

K	h	á	n	h		H	ò	a
(32, 85)	(55, 19)	(134, 121)	(113, 8)	(55, 19)	(136, 2)	(55, 19)	(83, 34)	(51, 22)

- Áp dụng: $\mathcal{C} = \mathcal{E}(\mathcal{P}) = [(u \times \mathcal{P}_i + v) \bmod (n)]P$

Xét ký tự ‘K’: Ta được $\mathcal{P}_i$ của ‘K’ là 44P ứng với điểm (32, 85)

Ta có $\mathcal{C} = [(7 \times 44 + 23) \bmod 131]P = 69P = 69(51, 22) = (13, 121)$. Với x = 13 và y = 121 đọc chuỗi số ở ma trận M^* ở bước 5. Ta có: 10011, 11111

Tương tự xét ký tự ‘h’: Ta được P_i của ‘h’ là 37P ứng với điểm (55, 19)

Ta có $\mathcal{C}$ = [(7 × 37 + 23) mod 131]P = 20P = 20(51, 22) = (48, 25). Với x = 48 và y = 25 đọc chuỗi số ở ma trận M ở bước 5. Ta có: 00121, 10022

Tương tự các ký tự còn lại ta được kết quả như bảng 4.

Bảng 4. Bảng các ký từ sau khi mã hóa

Ký tự	Rõ điểm	Mã điểm	Chuỗi số mã hóa
K	(32, 85)	(13, 121)	10011 11111
h	(55, 19)	(48, 25)	00121 10022
á	(134, 121)	(62, 52)	20202 10122
n	(113, 8)	(49, 62)	10121 20202
h	(55, 19)	(48, 25)	00121 10022
	(136, 2)	(83, 103)	21000 11021
H	(55, 19)	(48, 25)	00121 10022
ò	(83, 34)	(132, 5)	01122 20001
a	(51, 22)	(71, 32)	20212 20101

Vậy bản mã sau khi mã hóa là:
10011111110012110022202021012210121202020012110022210001102100121100220 01122200012021220101.
Bản mã này được gửi trên kênh truyền cho bên B.

Giải mã:

Khi bên B nhận được bản mã và tiến hành giải mã như sau:

Bước 9: Chuyển sang thập phân

Với m = 5, xét chuỗi 10011 dịch 1 bit sang trái ta được 00111 rồi chuyển sang thập phân.

$00111_{(3)} = 0\times3^4 + 0\times3^3 + 1\times3^2 + 1\times3^1 + 1\times3^0 = 13$.

Tương tự, xét chuỗi 11111 dịch 1 bít sang trái ta được 11111 rồi chuyển sang thập phân $11111_{(3)}$ = 121 do vậy, ta được điểm (31, 29)

Ta tính toán với các chuỗi số còn lại ta xác định được (13, 121); (48, 25); (62, 52); (49, 62); (48, 25); (83, 103); (48, 25); (132, 5); (71, 32).

Bước 10: Hàm giải mã

- Khóa để giải mã $\mathcal{K}$ = (7, 23)

- Áp dụng $\mathcal{P}$= $\mathcal{D}(\mathcal{C})$ = [u^{-1}($\mathcal{C}_i$ – v) mod (n)]P

Xét điểm (13, 121) có vị trí 69P trên đường cong, ta có:

P = [7^{-1}(69 - 23) mod 131]P = 44P= 44(51, 22) = (32, 85) ứng với ký tự 'K'

Tương tự xét điểm (48, 25) có vị trí 20P trên đường cong, ta có:

P = [7^{-1}(20 - 23) mod 131]P = 37P = 37(51, 22) = (55, 19) ứng với ký tự 'h'.

Tương tự với các điểm còn lại ta được kết quả giải mã như bảng 5:

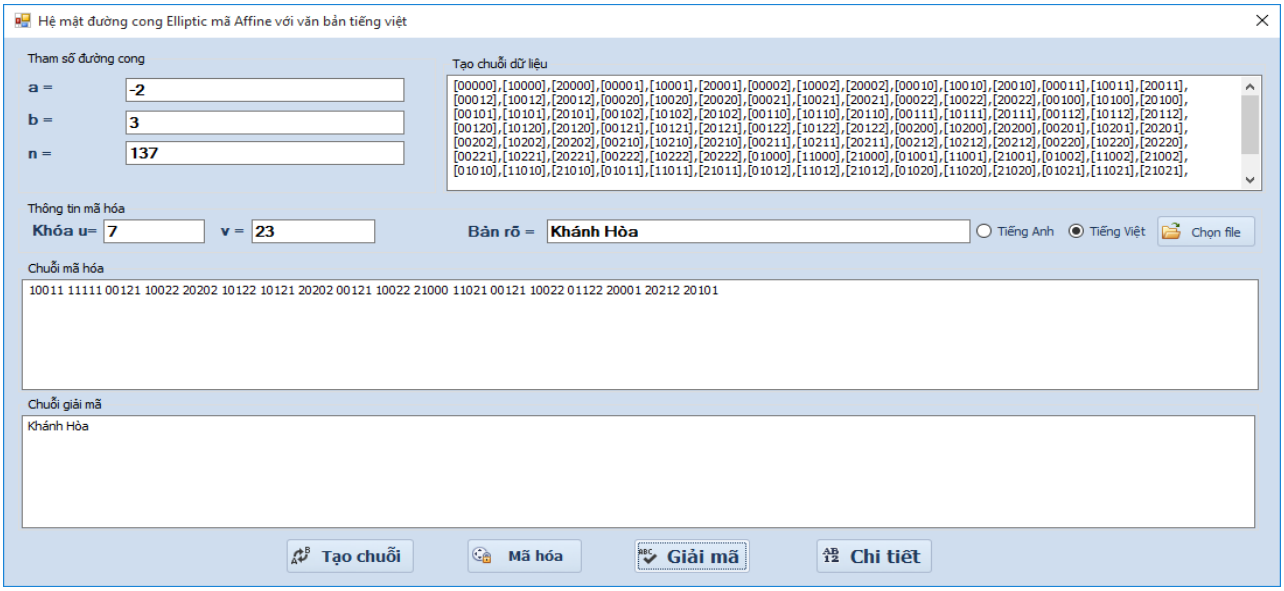
Bảng 5. Bảng kết quả giải mã

Chuỗi số mã hóa	Mã điểm	Rõ điểm	Ký tự
10011 11111	(13, 121)	(32, 85)	K
00121 10022	(48, 25)	(55, 19)	h
20202 10122	(62, 52)	(134, 121)	á
10121 20202	(49, 62)	(113, 8)	n
00121 10022	(48, 25)	(55, 19)	h
21000 11021	(83, 103)	(136, 2)	
00121 10022	(48, 25)	(55, 19)	H
01122 20001	(132, 5)	(83, 34)	ò
20212 20101	(71, 32)	(51, 22)	a

Vậy ta được bản rõ ban đầu là: Khánh Hòa

V. CÀI ĐẶT CHƯƠNG TRÌNH

Thuật toán được cài đặt trên thiết bị với cấu hình phần cứng là: CPU Intel(R) Core(TM) i5, 2.5 GHZ; RAM: 4GB; HDD: 500 GB; Và phần mềm với Hệ điều hành Windows 10, môi trường lập trình Visual studio .NET – 2019.



Hình 4. Giao diện chương trình

Chương trình thực hiện cài đặt thuật toán mã hóa và giải mã trên đường cong Elliptic dùng ngôn ngữ lập trình C# của Visual studio .NET -2019 với giao diện như Hình 4. Chương trình chạy cho kết quả đúng đắn với thuật toán đã trình bày ở trên.

VI. KẾT LUẬN

Trong thuật toán mã hóa AECC được đề xuất ở đây, các bên giao tiếp đồng ý sử dụng đường cong Elliptic và điểm sinh P trên đường cong này. Tính bảo mật của mật mã đường cong Elliptic phụ thuộc vào độ khó của việc tìm khóa mà khóa phụ thuộc cặp giá trị u, v. Với kP trong đó giá trị k là một số lớn ngẫu nhiên và P là một điểm sinh ngẫu nhiên trên đường cong Elliptic. Đây là vấn đề logarit rời rạc đường cong Elliptic. Độ bảo mật còn phụ thuộc m, m là số chữ số của một nhóm số và m dài hay ngắn phụ thuộc tổng số điểm (n) trên đường cong Elliptic mà n lại phụ thuộc tham số của đường cong. Các tham số đường cong Elliptic cho các sơ đồ mã hóa nên được lựa chọn cẩn thận để chống lại tất cả các cuộc tấn công đã biết của bài toán logarit rời rạc đường cong Elliptic (ECDLP). Do đó, phương pháp mã hóa được đề xuất ở đây cung cấp bảo mật đầy đủ chống lại việc phá mã chi phí tính toán tương đối thấp. Thuật toán được cài đặt và thử nghiệm trên ngôn ngữ lập trình C# cho kết quả đúng đắn theo thuật toán đề xuất. Tuy nhiên, đây là lĩnh vực đầy thách thức, có nhiều ứng dụng thực tế và là xu hướng phát triển của mật mã hiện đại.

TÀI LIỆU THAM KHẢO

[1] Ahmad H. Al-Omari, “Lightweight Dynamic Crypto Algorithm for Next Internet Generation”, Engineering, Technology & Applied Science Research, Vol. 9, No. 3, pp. 4203-4208, 2019.

[2] Morgan He, “Lightweight Cryptography: A Solution to Secure IoT”, A thesis presented to the University of Waterloo, Ontario, Canada, 2019.

[3] V.Miller, “Uses of Elliptic curves in Cryptography. In advances in Cryptography (CRYPTO 1985)”, Springer LNCS 218,pp. 417-426, 1985.

[4] 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, pp. 327-337, 1998.

[5] Javed R. Shaikh, Maria Nenova, Georgi Iliev, Zlatka Valkova-Jarvis, “Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications”, International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS), 2017

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

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

[8] F. Amounas and E. H. El Kinani, "ECC Encryption and Decryption with a Data Sequence, Applied Mathematical Sciences", Vol. 6, No. 101, pp. 5039-5047, 2012.

BUILDING AN ELLIPTIC CURVE CRYPTOGRAPHY WITH AFFINE SYMMECTRIC KEY TO ENCRYPT DECODING VIETNAMESE TEXT

Mai Manh Trung, Do Trung Tuan, Le Phe Do, Le Trung Thuc, Dao Thi Phuong Anh

ABSTRACT: *Elliptic curve cipher was a direction in lightweight primitive cryptography. The article describes the basic idea of symmetric key of Affine cipher, the Elliptic curve cryptography (ECC). 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 RSA is that it provides equivalent security for a smaller key size, which reduces processing costs. To encode the Vietnamese text, we are based on the sound of Vietnamese characters to make a table of these characters' order. To increase security we are also based on the algorithm to create the data sequence as the basis of building an encryption algorithm by using Elliptic curves on finite fields with Affine symmetric keys to encrypt this Vietnamese text. This algorithm has installed and tested successfully on C# 2019 programming language.*