CƠ SỞ TOÁN HỌC CHO CÁC BIẾN THỂ CỦA RSA

Trần Đình Long[1*], Võ Anh Duy[2]

[1] Khoa Toán, trường Đại học Khoa học, Đại học Huế

[2] Trường THCS Tôn Đức Thắng, thị xã Đông Hòa, tỉnh Phú Yên

* Email: tdlong@husc.edu.vn

Ngày nhận bài: 4/5/2021; ngày hoàn thành phản biện: 18/6/2021; ngày duyệt đăng: 02/11/2021

TÓM TẮT

Có rất nhiều biến thể của RSA từ khi hệ mã này dược công bố đầu tiên vào năm 1978. Các biến thể này của RSA được thiết lập trên các cấu trúc đại số khác nhau, vì vậy chúng được xây dựng về mặt toán học theo các cách khác nhau. Chúng tôi sẽ chỉ ra rằng, các biến thể này có thể được xây dựng trên cùng một nền tảng toán học sử dụng các công cụ trong lý thuyết nhóm.

Từ khóa: nhóm, RSA.

1. GIỚI THIỆU

RSA là một hệ mã khóa công khai RSA nổi tiếng, do các tác giả R. Rivest, A. Shamir và L. Adleman công bố vào năm 1978. Kể từ đó RSA được dùng rộng rãi trên khắp thế giới trong lĩnh vực bảo mật thông tin. Các nghiên cứu về RSA tập trung vào hai hướng chính: xây dựng các biến thể cho RSA và thám mã hệ mã này. Chúng ta có thể liệt kê các biến thể của RSA theo hướng thứ nhất như: RSA trên vành thương của các số nguyên [1], RSA trên vành thương của các đa thức hoặc vành thương của các số nguyên Gauss [2], RSA trên nhóm các ma trận khả nghịch [3], RSA trên nhóm đường cong elliptic [4]. Mục đích của chúng tôi trong bài báo này là trình bày cách xây dựng các hệ mã RSA theo một đường lối duy nhất. Điều này giúp chúng ta biết rõ những cấu trúc toán học cần thiết để xây dựng một hệ mã RSA và hiểu được các yếu tố đóng vai trò nền tảng cho một hệ mã RSA.

Cấu trúc bài báo như sau: chúng tôi trình bày ngắn gọn hệ mã RSA và chỉ ra phương trình thiết yếu để có thể xây dựng hệ mã này trong mục 2. Trong mục 3, chúng tôi đưa ra các giả thiết đảm bảo cho phương trình và kiểm tra các giả thiết này trong các biến thể của RSA.

2. GIỚI THIỆU VỀ RSA

Hệ mã RSA gốc được xây dựng trên vành $\mathbb{Z}_n$ các số nguyên theo modulo n. Chúng tôi mô tả tóm tắt hệ mã này như sau, người đọc có thể tìm hiểu thêm chi tiết về hệ mã này trong [1].

2.1. Mô tả hệ mã RSA

Sinh khóa.

- Chọn hai số nguyên tố phân biệt p, q và tính tích của chúng $n = pq$.

- Chọn một số nguyên d nguyên tố cùng nhau với $\varphi(n) = (p-1)(q-1)$.

- Tính $e \equiv d^{-1}(mod\ \varphi(n))$.

- Công bố khóa chung e và giữ d làm khóa riêng. n là thông tin công khai.

Mã hóa.

- Không gian văn bản là $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$.

- Một văn bản $m \in \mathbb{Z}_n$ được mã hóa thành $c \equiv m^e (mod\ n)$.

Giải mã.

- c được giải mã bằng cách tính $c^d \equiv m(mod\ n)$.

2.2. Chú ý về hệ mã RSA

Theo quy ước, một hệ mã trong đó các quá trình mã hóa và giải mã được tiến hành bằng lũy thừa sẽ được gọi là một biến thể của RSA. Phương trình $m^{ed} \equiv m(mod\ n)$ là yếu tố quan trọng đảm bảo sự mã hóa $m^e \equiv c(mod\ n)$ và giải mã $c^d \equiv m(mod\ n)$. Nói tổng quát, một khi có được phương trình $m^{ed} = m$, chúng ta có thể thiết lập được một biến thể của RSA.

Do đó, trong mục tiếp theo đây, chúng tôi chỉ đưa ra các điều kiện đảm bảo cho phương trình $m^{ed} = m$. Một biến thể của RSA sẽ được ngầm nói đến đằng sau phương trình này.

3. PHƯƠNG PHÁP CHUNG XÂY DỰNG BIẾN THỂ CHO RSA

Như đã nói ở trên, trong một biến thể của RSA, các bước tính toán trong các quá trình mã hóa và giải mã đều được thực hiện bằng cách tính lũy thừa. Điều này dẫn đến việc không gian văn bản có thể được khảo sát như một nhóm hoặc thậm chí là nửa nhóm nhân. Chúng tôi sẽ dùng tính chất sau đây trong một nhóm, tính chất này có thể bắt gặp trong hầu hết các giáo trình viết về nhóm.

Mệnh đề 3.1. *Giả sử G là một nhóm nhân cấp* n *và* 1_G *là phần tử đơn vị của nó. Khi đó phương trình*

$$a^n = 1_G$$

xẽ xảy ra với mọi phần tử $a \in G$.

Kết quả chính của chúng tôi là như sau.

Mệnh đề 3.2. *Cho* G, U *và* V *là các nửa nhóm nhân. Giả sử rằng*

a) Tồn tại các đồng cấu $\mu: G \longrightarrow U$ *và* $\eta: G \longrightarrow V$.

b) Tồn tại các nhóm $U_1 \subset U, U_2 \subset U$ *và* $V_1 \subset V, V_2 \subset V$ *sao cho* $\mu(G) \subset (U_1 \cup U_2)$ *và* $\eta(G) \subset (V_1 \cup V_2)$

c) Ánh xạ $\theta: G \longrightarrow U \times V$ *xác định bởi* $\theta(x) = (\mu(x), \eta(x))$ *là một đơn ánh.*

Kí hiệu $n_i = |U_i|, m_i = |V_i|$ $(i = 1,2)$. *Khi đó nếu* e, d *là các số nguyên thỏa mãn* $ed \equiv 1(mod\ n_i)$ *và* $ed \equiv 1(mod\ m_i)$ *với* $i = 1,2$ *thì* $x^{ed} = x$ *với mọi* $x \in G$.

Chứng minh. Lấy x là một phần tử tùy ý trong G. Trước hết ta sẽ chứng minh rằng $\mu(x^{ed}) = \mu(x)$. Do $\mu(x) \in (U_1 \cup U_2)$ nên hoặc $\mu(x) \in U_1$ hoặc $\mu(x) \in U_2$. Không mất tính tổng quát có thể giả sử rằng $\mu(x) \in U_1$.

Vì $ed \equiv 1(mod\ n_1)$ nên $ed = kn_1 + 1$ với $k \in \mathbb{Z}$ nào đó. Mệnh đề 3.1. suy ra rằng $(\mu(x))^{n_1} = 1_{U_1}$. Do đó,

$$\mu(x)^{ed} = (\mu(x))^{kn_1}.\mu(x) = ((\mu(x))^{n_1})^k.\mu(x) = \mu(x).$$

Do μ là một đồng cấu, ta có $\mu(x^{ed}) = \mu(x)^{ed}$. Vì vậy, $\mu(x^{ed}) = \mu(x)$.

Tương tự, ta cũng có $\eta(x^{ed}) = \eta(x)$.

Suy ra $\theta(x^{ed}) = (\mu(x^{ed}), \eta(x^{ed})) = (\mu(x), \eta(x)) = \theta(x)$.

Điều này dẫn đến $x^{ed} = x$ do θ là một đơn ánh.■

Phần còn lại của mục này dành cho việc điểm lại các biến thể của RSA dưới góc nhìn của Mệnh đề 3.2.

3.1. RSA trên vành thương của vành Euclide

Chúng tôi nhắc lại ngay sau đây khái niệm vành Euclide, có thể tìm thấy các tính chất sâu hơn của vành Euclide trong các giáo trình đại số đại cương như [5-6].

3.1.1. Định nghĩa. *Giả sử X là một vành giao hoán có đơn vị. X được gọi là một vành Eudlide nếu tồn tại một ánh xạ*

$$\delta: X \setminus \{0\} \longrightarrow \mathbb{N}$$

từ $X \setminus \{0\}$ *vào tập số tự nhiên* $\mathbb{N}$ *thỏa mãn:*

(i) Nếu a, b *là các phần tử khác* 0 *của* X *thì* $\delta(ab) \geq \delta(a)$.

(ii) Với 2 phần tử $a, b \in X$ *trong đó* b *khác 0 sẽ tồn tại các phần tử* $q, r \in X$ *sao cho*

$$a = bq + r$$

trong đó hoặc $r = 0$ *hoặc* $\delta(r) < \delta(b)$.

δ được gọi là *ánh xạ Euclide* hay là một chuẩn trên X. Phép chia trên một vành Euclide X sinh ra trên đó một loạt các khái niệm quen thuộc như bội, ước, ước chung của hai phần tử, hệ thức Bezout, phần tử nguyên tố, ...

Bây giờ, giả sử X là một vành Euclide và với mỗi $x \in X$, vành thương $X / \langle x \rangle$ là hữu hạn; trong đó $\langle x \rangle$ kí hiệu là ideal trong X sinh bởi x.

3.1.2. Mệnh đề. *Nếu* p, q *là các phần tử nguyên tố cùng nhau trong* X *và* $n = pq$ *thì chúng ta có đẳng cấu*

$$X / \langle pq \rangle \cong (X / \langle p \rangle \times (X / \langle q \rangle.$$

Chứng minh. Để làm gọn kí hiệu, chúng ta viết I và J tương ứng thay cho $\langle p \rangle$ cho $\langle q \rangle$.

Xét ánh xạ

$$\phi: X \longrightarrow (X / I) \times (X / J)$$
$$x \longmapsto (x + I, x + J).$$

Có thể dễ dàng kiểm tra ϕ là một đồng cấu vành.

Do p, q là các phần tử nguyên tố phân biệt, ta có $gcd(p, q) = 1$. Áp dụng hệ thức Bezout, sẽ tồn tại $u, v \in X$ sao cho $up + vq = 1$. Kí hiệu $a = up, b = vq$ thì $a \in I, b \in J$ và $a + b = 1$.

Chúng ta sẽ chỉ ra rằng ϕ là một toàn ánh. Thật vậy, giả sử $(s + I, t + J)$ là một phần tử bất kỳ trong $(X / I) \times (X / J)$. Đặt $x = sb + ta$, thế thì

$$x - s = (sb + ta) - (a + b)s = (t - s)a \in I$$

và

$$x - t = (sb + ta) - (a + b)t = (s - t)b \in J.$$

Khi đó $\phi(x) = (x + I, x + J) = (s + I, t + J)$. Vì vậy, ϕ là một toàn ánh và cảm sinh ra đẳng cấu

$$X / Ker(\phi) \cong (X / I) \times (X / J).$$

Rõ ràng $Ker(\phi) = I \cap J$. Chú ý rằng do $IJ \subset I$ và $IJ \subset J$ nên $IJ \subset (I \cap J)$. Ngược lại, với $x \in I \cap J$, ta có $x = x(a + b) = xa + xb \in IJ$. Như vậy $Ker(\phi) = I \cap J = IJ$.

Do $IJ = \langle pq \rangle$ nên $X / \langle pq \rangle \cong (X / I) \times (X / J)$.■

Với $x \in X$, ta sẽ kí hiệu $\varphi(x)$ là số phần tử khả nghịch trong vành thương $X / \langle x \rangle$. Đây là một mở rộng của hàm Phi-Euler cho số nguyên.

Đẳng cấu trong mệnh đề trên sẽ cảm sinh một đồng cấu nửa nhóm nếu ta xem các vành thương là các nửa nhóm nhân. Nếu ta viết $G = X / \langle pq \rangle$; U, V thay cho các nửa nhóm nhân $X / \langle p \rangle$ và $X / \langle q \rangle$; U_1, V_1 thay cho nhóm nhân các phần tử khả nghịch trong $X / \langle p \rangle$ và $X / \langle q \rangle$; $U_2 = \{0\}, V_2 = \{0\}$ trong $X / \langle p \rangle$ và $X / \langle q \rangle$. Khi đó theo Mệnh đề 3.2., ta có

$$x^{ed} = x$$

với mọi $x \in X$; trong đó e, d là các số nguyên thỏa mãn $ed \equiv 1 (mod\ l)$ với

$$l = lcm(n_1, n_2, m_1, m_2),$$

$$n_1 = |U_1| = \varphi(p),$$

$$n_2 = |U_2| = 1,$$

$$m_1 = |V_1| = \varphi(q),$$

và

$$m_2 = |V_2| = 1.$$

Do đó, chúng ta có thể thiết lập một hệ mã RSA trên $X / \langle pq \rangle$. Các vành sau đây là các vành Euclide và chúng ta có thể theo sơ đồ trên đây thiết lập một hệ mã RSA trên vành thương của chúng:

- Vành các số nguyên thông thường $\mathbb{Z}$.

- Vành các số nguyên Gauss $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ với phép cộng và nhân các số phức thông thường.

- Vành các đa thức theo một biến x hệ số trong vành $\mathbb{Z}_p$, với p là một số nguyên tố.

3.2. Biến thể của RSA trên nhóm các ma trận khả nghịch

Giả sử p, q là hai số nguyên tố phân biệt, $n = pq$ và m là một số nguyên dương. Kí hiệu $GL(m, p), GL(m, q)$ và $GL(m, n)$ là các nhóm nhân các ma trận khả nghịch cấp m hệ số tương ứng trong $\mathbb{Z}_p, \mathbb{Z}_q$ và $\mathbb{Z}_n$. Bậc của các nhóm $GL(m, p)$ và $GL(m, q)$ lần lượt là

$$N_p = (p^m - 1)(p^m - p) \dots (p^m - p^{m-1})$$

và

$$N_q = (q^m - 1)(q^m - q) \dots (q^m - q^{m-1}),$$

(xem [3]).

Từ đẳng cấu vành

$$\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q,$$

một phần tử trong $GL(m,n)$ sẽ tương ứng với một phần tử trong $\mathbb{Z}_p \times \mathbb{Z}_q$. Do đó, bậc của $GL(m,n)$ sẽ là

$$N_n = N_P N_q.$$

Đẳng cấu vành $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q$ cũng cảm sinh các đồng cấu μ, η từ $GL(m,n)$ vào $GL(m,p)$ và $GL(m,q)$.

Đặt

$$G = GL(m,n),$$

$$U = U_1 = U_2 = GL(m,p),$$

và

$$V = V_1 = V_2 = GL(m,q).$$

Mệnh đề 3.2 suy ra rằng $x^{ed} = x$ với mọi $x \in GL(m,n)$, trong đó e, d là các số nguyên thỏa mãn $ed \equiv 1(mod\ l)$ với $l = lcm(N_p, N_q)$. Do đó, chúng ta có thể thiết lập một hệ mã RSA trên $G = GL(m,n)$. Biến thể này của RSA dược công bố bởi Varadharajan V. và Odoni R. vào 1985 [3].

3.3. Biến thể của RSA trên nhóm đường cong elliptic

Giả sử p, q là các số nguyên tố phân biệt và $n = pq$. Các số nguyên A, B thỏa mãn điều kiện $\gcd(4A^3 + 27B^2, n) = 1$.

Trước hết, chúng tôi nhắc lại nhóm đường cong elliptic trên $\mathbb{Z}_p$, xét tập hợp

$$E_p(A,B) = \{\infty\} \cup \{(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p : y^2 = x^3 + Ax + B\}$$

và phép toán cộng "+" định nghĩa trên $E_p(A,B)$ thỏa mãn các điều kiện sau:

(a) ∞ là phần tử đơn vị của phép cộng, tức là $P + \infty = \infty + P = P$ với mọi $P \in E_p(A,B)$.

(b) Với $P_1 = (x_1, y_1)$ và $P_2 = (x_2, y_2)$ là các điểm trong $E_p(A,B)$. Phép cộng $P_1 + P_2 = P_3 = (x_3, y_3)$ được định nghĩa:

.Nếu $x_1 \neq x_2$ thì $x_3 = m^2 - x_1 - x_2$, $y_3 = m(x_1 - x_3) - y_1$, trong đó $m = \frac{y_2 - y_1}{x_2 - x_1}$.

.Nếu $x_1 = x_2$ nhưng $y_1 \neq y_2$ thì $P_1 + P_2 = \infty$.

.Nếu $P_1 = P_2$ và $y_1 \neq 0$ thì $x_3 = m^2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$, trong đó $m = \frac{3x_1^2 + A}{2y_1}$.

.Nếu $P_1 = P_2$ và $y_1 = 0$ thì $P_1 + P_2 = \infty$.

Khi đó $(E_p(A,B), +)$ là một nhóm và được gọi là nhóm đường cong elliptic trên $\mathbb{Z}_p$.

Nhóm bù với nhóm elliptic là nhóm kí hiệu bởi $\overline{E_p(A,B)}$, được định nghĩa ngay sau đây. Với $a \in \mathbb{Z}_p$, chúng ta dùng kí hiệu Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{nếu a là một bình phương theo modulo p và a} \neq 0(\text{mod p}) \\ -1, \text{nếu a không là một bình phương theo modulo p} \\ 0, \quad \text{nếu a} = 0(\text{mod p}) . \end{cases}$$

Kí hiệu g_p là phần tử sinh của nhóm nhân $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\}$. Với $y \in \mathbb{Z}_p$ mà $\left(\frac{y}{p}\right) = -1$ thì y sẽ có dạng $y = u\sqrt{g_p}$, trong đó $u \in \mathbb{Z}_p$. Kí hiệu

$$\overline{E_p(A,B)} = \{\infty\} \cup \{(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p : y = u\sqrt{g_p}, u \in \mathbb{Z}_p, y^2 = x^3 + Ax + B\}.$$

Tương tự như trên $E_p(A,B)$ chúng ta có thể định nghĩa một phép toán cộng trên $\overline{E_p(A,B)}$ thỏa mãn các tính chất sau.

(a) ∞ là phần tử đơn vị của phép cộng, tức $M + \infty = \infty + M = M$ với mọi $M \in \overline{E_p(A,B)}$.

(b) Với $M_1 = (x_1, y_1) = (x_1, u_1\sqrt{w_p})$ và $M_2 = (x_2, y_2) = (x_2, u_2\sqrt{w_p})$ là các điểm thuộc $\overline{E_p(A,B)}$. Định nghĩa $M_1 + M_2 = M_3 = (x_3, y_3) = (x_3, u_3\sqrt{w_p})$ như sau:

.Nếu $x_1 \neq x_2$ thì $x_3 = m^2 w_p - x_1 - x_2$, $y_3 = (m(x_1 - x_3) - u_1)\sqrt{w_p}$, trong đó $m = \frac{u_2 - u_1}{x_2 - x_1}$.

.Nếu $x_1 = x_2$ nhưng $y_1 \neq y_2$ thì $M_1 + M_2 = \infty$.

.Nếu $M_1 = M_2$ và $y_1 \neq 0$ thì $x_3 = m^2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$, trong đó $m = \frac{3x_1^2 + A}{2y_1}$.

.Nếu $P_1 = P_2$ và $y_1 = 0$ thì $P_1 + P_2 = \infty$.

Khi đó $\overline{E_p(A,B)}$ là một nhóm, được gọi là nhóm bù của nhóm $\mathrm{E_p(A,B)}$.

Các nhóm $E_q(A,B)$ và $\overline{E_q(A,B)}$ được xây dựng một cách hoàn toàn tương tự. Chi tiết về các nhóm này có thể tìm thấy ở [4] và [7].

Bây giờ giả sử $N_1 = \left|\mathrm{E_p(A,B)}\right|$, $N_2 = \left|\overline{\mathrm{E_p(A,B)}}\right|$, $M_1 = \left|\mathrm{E_q(A,B)}\right|$ và $M_2 = \left|\overline{\mathrm{E_q(A,B)}}\right|$. Kí hiệu $L = lcm(N_1, N_2, M_1, M_2)$.

Do đẳng cấu vành $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q$, một phần tử x trong $\mathbb{Z}_n$ có thể xem là một cặp $(x_p, x_q) \in \mathbb{Z}_p \times \mathbb{Z}_q$. Kí hiệu w_1, w_2, w_3 lần lượt là các phần tử trong $\mathbb{Z}_n$ mà

$$w_1 \equiv 1(mod\ p), w_1 \equiv g_q(mod\ q),$$

$$w_2 \equiv g_p(mod\ p), w_1 \equiv 1(mod\ q),$$

và

$$w_3 \equiv g_p(mod\ p), w_1 \equiv g_q(mod\ q).$$

Khi đó với mỗi $x \in \mathbb{Z}_n$, có và chỉ có một trong các trường hợp sau xảy ra:

$.x^3 + Ax + B = t^2$,

$. x^3 + Ax + B = t^2 w_1$,

. $x^3 + Ax + B = t^2 w_2$,

. $x^3 + Ax + B = t^2 w_3$.

Do đó nếu kí hiệu

$$E_n^{11} = \{(x, y): x, y \in \mathbb{Z}_n, x^3 + Ax + B = y^2\},$$
$$E_n^{12} = \{(x, y): x \in \mathbb{Z}_n, y = t\sqrt{w_1}, t \in \mathbb{Z}_n, x^3 + Ax + B = y^2\},$$
$$E_n^{21} = \{(x, y): x \in \mathbb{Z}_n, y = t\sqrt{w_2}, t \in \mathbb{Z}_n, x^3 + Ax + B = y^2\},$$

và

$$E_n^{22} = \{(x, y): x \in \mathbb{Z}_n, y = t\sqrt{w_3}, t \in \mathbb{Z}_n, x^3 + Ax + B = y^2\},$$

thì với mỗi $x \in \mathbb{Z}_n$, tồn tại duy nhất một trong các tập hợp trên có chứa một phần tử mà tọa độ đầu là x .

Chúng ta đều biết rằng có thể định nghĩa một phép cộng "+" trên E_n^{11} sao cho $(E_n^{11}, +)$ là một nhóm và $E_n^{11} \cong E_p \times E_q$ ([7]). Các phép chiếu μ và η từ E_n^{11} lần lượt lên E_p và E_q là các đồng cấu nhóm. Mệnh đề 3.2. suy ra rằng $(ed)(x, y) = (x, y)$ với mọi $(x, y) \in E_n^{11}$, trong đó e, d là các số nguyên thỏa $ed \equiv 1(mod\ L)$.

Lập luận tương tự cũng chỉ ra rằng $(ed)(x, y) = (x, y)$ với mọi $(x, y) \in E_n^{12} \cup E_n^{21} \cup E_n^{22}$.

Hệ thức $(ed)(x, y) = (x, y)$ với mọi $(x, y) \in E_n^{11} \cup E_n^{12} \cup E_n^{21} \cup E_n^{22}$ cho phép chúng ta xây dựng một hệ mã RSA trên $E_n^{11} \cup E_n^{12} \cup E_n^{21} \cup E_n^{22}$. Do các phép cộng trên các nhóm này được thực hiện theo cách tương tự như nhau, chúng ta không cần quan tâm đến việc (x, y) thuộc cụ thể nhóm nào to. Biến thể này của RSA được công bố bởi N. Demytko vào 1993 [4].

4. KẾT LUẬN

Kết quả chính của chúng tôi là Mệnh đề 3.2., nó cho phép thiết lập hệ thức xây dựng nên hệ mã RSA. Bằng cách này, chúng ta có thể thiết lập biến thể của RSA trên các cấu trúc đại số phức tạp hơn $\mathbb{Z}_n$. Chẳng hạn, chúng tôi đã xây dựng được một biến thể của RSA trên vành các tự đồng cấu $End(\mathbb{Z}_n \times \mathbb{Z}_{n^2} \times ... \times \mathbb{Z}_{n^k})$, đây sẽ là nội dung chính của bài báo tiếp theo của chúng tôi.

TÀI LIỆU THAM KHẢO

[1]. R.L. Rivest, A. Shamir and L.M. Adleman (1978). A method for obtaining digital signatutes and public key cryptosystems, *Communication of the ACM*, Vol. 21, no. 2, pp. 120-126

[2]. El-Kassar A.N., R. Hatary and Y. Awad (2004). Modified RSA in the domains of Gaussian integers and polynomials over finite fields, *Proc. Intl. Conf. CSITeA'04*, Cairo, Egypt.

[3]. Varadharajan V. and Odoni R. (1985). Extension of RSA cryptosystems to matrix rings, *Cryptologia*, Vol 9:2, pp. 140-153.

[4]. N. Demytko (1993). A new elliptic curve based analogue of RSA, *Eurocrypt'93*, LNCS 765, pp. 40-49.

[5]. J. B. Fraleigh, V. J. Katz (1967). *A first course in abstract algebra*, Addison-Wesley Publishing Company, 5th ed.

[6]. R. S. Irving. Integers (2004). *Polynomials and Rings, A course in Algebra*, Springer.

[7]. K.H.Rosen (2008). *Elliptic curves – Number theory and cryptofraphy*, Taylor and Francis Group, LLC, Second Edition.

TOWARD A UNIFORM ESTABLISHING RSA CRYPTOSYSTEMS

Long T. D[1*], Duy V. A.[2]

[1] Faculty of Mathematics, University of Sciences, Hue University

[2] Ton Duc Thang Secondary School, Dong Hoa City, Phu Yen District

* Email: tdlong@husc.edu.vn

ABSTRACT

There have been many RSA cryptosystems which firstly came into existence since 1978. These RSA cryptosystems rely on different algebraic structures, therefore they were constructed in various ways. We show that, by group based tools, such cryptosystems can be established uniformly.

Keywords: group, homomorphism, RSA cryptosystem.

Trần Đình Long sinh ngày 18/01/1963 tại Thừa Thiên Huế. Năm 1984, ông tốt nghiệp cử nhân ngành Toán tại Trường Đại học Tổng hợp Huế. Năm 1997 tốt nghiệp thạc sỹ ngành Công nghệ thông tin tại trường QUT (Queensland University of Technology). Ông bào vệ tiến sĩ ngành Khoa học Máy tính năm 2015 tại trường Đại học Khoa học Tự nhiên thành phố Hồ Chí Minh.

Lĩnh vực nghiên cứu: Mã hóa thông tin, Đại số.

Võ Anh Duy sinh ngày 02/05/1990 tại Phú Yên. Năm 2012, ông tốt nghiệp ngành Sư phạm Tin học tại Trường Đại học Phú Yên. Năm 2016, ông tốt nghiệp Thạc sĩ ngành Khoa học máy tính tại trường Đại học Khoa học, ĐH Huế. Từ năm 2019, ông theo học lớp Cao học ngành Toán ứng dụng của trường Đại học Khoa học, ĐH Huế.

Lĩnh vực nghiên cứu: Toán ứng dụng.