Tạp chí Tin học và Điều khiển học, T.25, S.2 (2009), 159–165

MỘT SỐ TÍNH CHẤT CỦA TẬP $T(e)$ MỘT TẬP CON ĐẶC BIỆT CỦA Z_e^*

VŨ HUY HOÀNG[1], ĐẶNG VĂN CHUYẾT[2]

[1] *Cục Cơ yếu 893 - Ban Cơ yếu Chính phủ*
[2] *Đại học Bách khoa Hà Nội*

Abstract. In [1, 2] we have proposed an algorithm to construct secure RSA Cryptography System with large decryption exponent. The algorithm has been installed and run in several practical tests. In this article some interesting properties of the set $T(e)$, a subset of $\boldsymbol{Z_e^*}$ are presented and applied to prove the correctness of the proposed algorithm.

Tóm tắt. Trong [1, 2], tác giả đã đề xuất một thuật toán xây dựng hệ mật RSA an toàn với số mũ giải mã lớn. Thuật toán đã được cài đặt và chạy thử nghiệm. Trong bài báo này, một số tính chất lý thú của tập $T(e)$, một tập con của $\boldsymbol{Z_e^*}$ sẽ được giới thiệu và dùng để chứng minh tính đúng đắn thuật toán nói ở trên.

1. ĐẶT VẤN ĐỀ

Các lược đồ hệ mật khóa công khai và chữ ký số RSA hiện nay đang được sử dụng rộng rãi trên thế giới và ở Việt Nam. Nhưng bên cạnh đó cũng có nhiều mối nguy hiểm khi sử dụng hệ mật RSA không đúng cách ([3, 4, 5]). Wiener [6] đã chứng minh rằng, các số mũ bí mật nhỏ có thể được khôi phục hiệu quả nếu $d < \frac{n^{0,25}}{3}$. Kết quả này được cải tiến bởi Boneh và Durfee [7], cho kết quả tương tự với $d < n^{0,292}$. Hơn nữa hai tác giả này còn phỏng đoán rằng hệ mật RSA không an toàn với $d < \sqrt{n}$. Vì vậy, việc xây dựng hệ mật RSA với số mũ giải mã d lớn đã trình bày trong [2] cho phép tránh được kiểu tấn công do việc dùng số mũ giải mã d nhỏ, có ý nghĩa thực tế, đáp ứng được nhu cầu trong giai đoạn hiện nay.

Để chứng minh tính đúng đắn và khả thi của thuật toán xây dựng hệ RSA với số mũ giải mã lớn sau khi đã chọn trước số mũ lập mã $e \geq 3$, ta cần xem xét và giải quyết những vấn đề sau.

Cho e là một số nguyên dương, $e \geq 3$. Khi đó:

$Z_e = \{0, 1, 2, ..., e-1\}$ là tập các số dư modulo e;

$Z_e^* = \{r \in Z_e | gcd(r, e) = 1\}$ là nhóm nhân của Z_e, trong đó mọi phần tử của Z_e^* đều có nghịch đảo nhân.

Gọi $T(e)$ là tập con của Z_e^*, được xác định như sau:

$$T(e) = \{r \in Z_e^* | (r-1) \in Z_e^*\}.$$

Ta cần nghiên cứu các tính chất của tập $T(e)$ và công thức tính lực lượng (số phần tử)

của tập đó. Và sau đây là một số ví dụ.

Ví dụ 1. Với $e = 9$, ta có

$$Z_9^* = \{1, 2, 4, 5, 7, 8\},\ |Z_9^*| = \Phi(9) = 6,$$

và $T(9) = \{2, 5, 8\},\ |T(9)| = 3.$

Ví dụ 2. Với $e = 10 = 2 \times 5$, ta có

$$Z_{10}^* = \{1, 3, 7, 9\},\ |Z_{10}^*| = \Phi(10) = 4,$$

và $T(10) = \phi,\ |T(10)| = 0.$

Ví dụ 3. Với $e = 15 = 3 \times 5$, ta có

$$Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\},\ |Z_{15}^*| = \Phi(15) = 8,$$

và $T(15) = \{2, 8, 14\},\ |T(15)| = 3.$

Ví dụ 4. Với $e = 8 = 2^3$, ta có

$$Z_8^* = \{1, 3, 5, 7\},\ |Z_8^*| = \Phi(8) = 4,$$

và $T(8) = \phi,\ |T(8)| = 0.$

Ví dụ 5. Với $e = 27 = 3^3$, ta có

$$Z_{27}^* = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\},$$
$$|Z_{27}^*| = \Phi(27) = 18,$$

và $T(27) = \{2, 5, 8, 11, 14, 17, 20, 23, 26\},\ |T(27)| = 9.$

Ví dụ 6. Với $e = 5$ là một số nguyên tố, ta có

$$Z_5^* = \{1, 2, 3, 4\},\ |Z_5^*| = \Phi(5) = 4,$$

và $T(5) = \{2, 3, 4\},\ |T(5)| = 3.$

Ví dụ 7. Với $e = 25 = 5^2$, ta có

$$Z_{25}^* = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\},$$
$$|Z_{25}^*| = \Phi(25) = 20,$$

và $T(25) = \{2, 3, 4, 7, 8, 9, 12, 13, 14, 17, 18, 19, 22, 23, 24\},\ |T(25)| = 15.$

2. MỘT SỐ TÍNH CHẤT CỦA TẬP $T(e)$

Tính chất 1. *Nếu e là một số nguyên tố (tức e nguyên tố và lớn hơn 2) thì $T(e) \neq \phi$ và $|T(e)| = e - 2$.*

Chứng minh.

Vì e là số nguyên tố nên $Z_e^* = \{1, 2, 3, ..., e - 1\}$.

Suy ra $T(e) = \{2, 3, 4, ..., e - 1\}$ và $|T(e)| = e - 2.$ ■

Tính chất 2. *Nếu e là một hợp số chẵn thì $T(e) = \phi$.*

Chứng minh.

Giả sử $T(e) \neq \phi$ và $r \in T(e)$. Vì $r \in Z_e^*$ và e là số chẵn nên r là một số lẻ. Theo định nghĩa của $T(e)$, có $r - 1 \in Z_e^*$ và rõ ràng $(r - 1)$ là một số chẵn. Mâu thuẫn. Vậy $T(e) = \phi$.

Trở lại với ví dụ $e = 10$. Ta có $Z_{10}^* = \{1, 3, 7, 9\}$ và $T(10) = \phi$. ■

Tính chất 3. *Nếu m và n là hai số nguyên dương nguyên tố cùng nhau thì $T(m.n) = T(m).T(n)$.*

Chứng minh.

Trước hết, ta nhắc lại một tính chất quen thuộc tương tự đối với hàm Φ Euler:

$$\Phi(n.m) = \Phi(n).\Phi(m),$$

với n, m là hai số nguyên dương nguyên tố cùng nhau.

Thật vậy, giá trị của $\Phi(n.m)$ tương ứng với số các số nguyên tố cùng $n.m$ trong $n.m$ số nguyên dương đầu tiên. Ta biểu diễn $n.m$ số nguyên dương đầu tiên dưới dạng một bảng chữ nhật ($n \times m$, n hàng, m cột), mỗi hàng gồm m số như sau:

1	2	3	. . .	m
m+1	m+2	m+3	. . .	m+m
2m+1	2m+2	2m+3	. . .	2m+m
. . .	. . .	. . .	. . .	. . .
(n-1)m+1	(n-1)m+2	(n-1)m+3	. . .	(n-1)m+m

Bảng trên chứa $\Phi(n.m)$ số nguyên tố cùng $n.m$, có thể tìm được bằng cách xóa đi tất cả các số có một ước nguyên tố chung với m hay n.

Các số có ước nguyên tố chung với m là các số thuộc các cột mà số hiệu i (số đầu tiên trên đầu cột) có một ước chung với m (vì ước chung đó chia hết tất cả các số $k.m + i$ của cột).

Bằng cách lấy đi tất cả các cột có số hiệu không nguyên tố cùng m, ta đã xóa đi (loại bỏ đi) tất cả các số không nguyên tố cùng m.

Trong mỗi một cột gồm n số của $\Phi(m)$ cột còn lại, có đúng một số bằng 0 (mod n), một số bằng 1 (mod n), ... , một số bằng $n-1$ (mod n), và như vậy chứa n giá trị phân biệt modulo n. Thực vậy, giả sử ngược lại, có hai phần tử thuộc cùng một cột $(b.m + a)$ và $(b'm + a)$ mà bằng nhau theo modulo n. Nếu $b.m + a = b'm + a(\text{mod } n)$ thì $bm = b'm(\text{mod } n)$. Nhân hai vế với nghịch đảo của m theo modulo n (nghịch đảo này tồn tại vì n và m nguyên tố cùng nhau), có $b = b'(\text{mod } n)$, có nghĩa $b = b'$ vì b và b' đều nằm giữa 0 và $n - 1$.

Như vậy, với một giá trị cho trước tương ứng chỉ cùng một phần tử của cột, ta đã chứng minh được rằng các số của mỗi cột còn lại đều phân biệt modulo n.

Do đó trong mỗi cột, thuộc $\Phi(m)$ cột còn lại, chứa các số không có một ước chung nào với m, việc loại bỏ các số có một ước chung với n sẽ để lại đúng $\Phi(n)$ số.

Tóm lại, trong bảng còn lại đúng $\Phi(n).\Phi(m)$ số, chứng tỏ điều phải chứng minh. ■

Ví dụ 8. Xét một ví dụ với $m = 25$ và $n = 9$. Ta lập Bảng 1.

Bảng 1. $m = 25$ và $n = 9$ (trong đó các ô sẫm màu bị loại bỏ)

1	2	3	4	5	6	7	8	9	10	11	12	13
26	27	28	29	30	31	32	33	34	35	36	37	38
51	52	53	54	55	56	57	58	59	60	61	62	63
76	77	78	79	80	81	82	83	84	85	86	87	88
101	102	103	104	105	106	107	108	109	110	111	112	113
126	127	128	129	130	131	132	133	134	135	136	137	138
151	152	153	154	155	156	157	158	159	160	161	162	163
176	177	178	179	180	181	182	183	184	185	186	187	188
201	202	203	204	205	206	207	208	209	210	211	212	213

14	15	16	17	18	19	20	21	22	23	24	25
39	40	41	42	43	44	45	46	47	48	49	50
64	65	66	67	68	69	70	71	72	73	74	75
89	90	91	92	93	94	95	96	97	98	99	100
114	115	116	117	118	119	120	121	122	123	124	125
139	140	141	142	143	144	145	146	147	148	149	150
164	165	166	167	168	169	170	171	172	173	174	175
189	190	191	192	193	194	195	196	197	198	199	200
214	215	216	217	218	219	220	221	222	223	224	225

Các cột 5, 10, 15, 20, 25 bị loại bỏ. Còn lại $\Phi(25) = \Phi(5^2) = 5 \times \Phi(5) = 5 \times 4 = 20$ cột.

Trong 20 cột còn lại, mỗi cột gồm các số không có ước chung với 25 và việc loại bỏ các số có ước chung với 9, còn lại $\Phi(9) = \Phi(3^2) = 3 \times 2 = 6$ số.

Điều đó chứng tỏ $\Phi(25 \times 9) = \Phi(25) \times \Phi(9) = 20 \times 6 = 120$.

Với lập luận tương tự, ta cũng chứng minh được $T(m \times n) = T(m) \times T(n)$, với m, n là ước số dương nguyên tố cùng nhau.

Với $m = 25, n = 9$, tính được

$$T(25 \times 9) = T(225) = 45,\ T(25) = 15,\ T(9) = 3,$$

và như vậy $T(25 \times 9) = T(25) \times T(9) = 45$.

Tính chất 4. *Nếu e là một luỹ thừa bậc k của một số nguyên tố p, $e = p^k$, thì*

$$|T(e)| = (p-2) \times p^{k-1} = p^k(1 - \frac{2}{p}).$$

Chứng minh. Trước hết ta tìm giá trị của hàm Euler Φ, áp dụng cho số p^k. Muốn vậy, cần loại bỏ những số giữa 0 và $p^k - 1$ mà có một ước chung với p^k, những số đó là các bội số của p, tức các số $0, p, 2p, ..., p^k - p$. Có đúng p^{k-1} số như vậy.

Từ đó $\Phi(e) = p^k - p^{k-1} = p^{k-1}(p-1)$.

Theo định nghĩa của tập $T(e)$, suy ra $|T(e)| = p^{k-1} \times (p-2)$.

Từ các tính chất đã xét của tập $T(e)$, có thể chứng minh các mệnh đề sau.

Mệnh đề 1. *Nếu $e = p_1^{e_1}, p_2^{e_2}, ..., p_t^{e_t}$ là phân tích ra thừa số nguyên tố của e, trong đó $1 < p_1 < p_2 < ... < p_t$ là các số nguyên tố, còn $e_i \geq 1,\ \forall i = 1, 2, ..., t$, thì*

$$|T(e)| = \prod_{i=1}^{t}(p_i - 2) \times p_i^{e_i - 1}. \quad (1)$$

Chứng minh.

Vì các số $p_i^{e_i}$ và $p_j^{e_j}$ với $i \neq j$ từng đôi nguyên tố cùng nhau, áp dụng Tính chất 3, có

$$|T(e)| = |T(p_1^{e_1})|.|T(p_2^{e_2})|...|T(p_i^{e_i})|. \quad (2)$$

Đến đây, áp dụng Tính chất 4 cho vế phải của (2), ta có được kết quả cần chứng minh. ■

Áp dụng công thức (1), ta dễ dàng tính lại được một số kết quả đã có.

$|T(9)| = |T(3^2)| = (3-2) \times 3^{2-1} = 3,$

$|T(10)| = |T(2 \times 5)| = (2-2) \times [(5-2)] = 0,$

$|T(15)| = |T(3 \times 5)| = (3-2) \times [(5-2)] = 3,$

$|T(8)| = |T(2^3)| = (2-2) \times 2^{3-1} = 0,$

$|T(27)| = |T(3^3)| = (3-2) \times 3^2 = 9,$

$|T(25)| = |T(5^2)| = (5-2) \times 5 = 15.$

Mệnh đề 2. *Tỷ số giữa số phần tử của $T(e)$ với số phần tử của Z_e^* được tính theo công thức*

$$\frac{|T(e)|}{|Z_e^*|} = \frac{|T(e)|}{\Phi(e)} = \prod_{i=1}^{t}\frac{p_i - 2}{p_i - 1},$$

trong đó, $e = p_1^{e_1}.p_2^{e_2}...p_t^{e_t}$ là phân tích ra thừa số nguyên tố của e.

Nếu $e = 3^l$ thì $\frac{|T(e)|}{\Phi(e)} = \frac{1}{2}$.

Nếu $e = p^l$, với p là một số nguyên tố lớn hơn 3 thì $\frac{|T(e)|}{\Phi(e)} > \frac{1}{2}$.

Chứng minh.

Sử dụng hai công thức

$$\Phi(e) = p_1^{e_1}(1 - \frac{1}{p_1}).p_2^{e_2}(1 - \frac{1}{p_2})...p_t^{e_t}(1 - \frac{1}{p_t}) = \prod_{i=1}^{t}(p_i - 1)p_i^{e_i - 1}),$$

và $|T(e)| = \prod_{i=1}^{t}(p_i - 2).p_i^{e_i - 1})$.

Ta có kết quả

$$\frac{|T(e)|}{\Phi(e)} = \prod_{i=1}^{t}\frac{p_i - 2}{p_i - 1}.$$

(i) Trường hợp $e = 3^l$, ta có $\dfrac{|T(e)|}{\Phi(e)} = \dfrac{3-2}{3-1} = \dfrac{1}{2}$.

(ii) Trường hợp $e = p^l$ với p là một số nguyên tố lớn hơn 3, ta có

$$\frac{|T(e)|}{\Phi(e)} = \frac{p-2}{p-1}.$$

Vì $p > 3$, có $\dfrac{p-2}{p-1} - \dfrac{1}{2} = \dfrac{2p-5}{2(p-1)} > 0$. Suy ra $\dfrac{|T(e)|}{\Phi(e)} > \dfrac{1}{2}$.

3. ỨNG DỤNG

Để thấy được các kết quả đã trình bày ở trên, các bước của thuật toán xây dựng hệ mật RSA an toàn với số mũ giải mã lớn [1, 2] là đúng đắn và luôn khả thi, ta nhắc lại các bước của thuật toán.

Thuật toán xây dựng hệ mật RSA an toàn với số mũ giải mã lớn

Bước 1. Chọn số mũ lập mã $e \geq 3$ là số nguyên dương lẻ.
Bước 2. Chọn ngẫu nhiên $r_p \in T(e)$ với $T(e) = \{r_p \in Z_e^* | (r_p - 1) \in Z_e^*\}$. Tạo sinh số nguyên tố p đủ lớn sao cho $p = c_p.e + r_p$ (theo định lý Dirichlet).
Bước 3. Tính một số nguyên tố lớn $q = r_p(r_p - 1)^{-1} (\text{mod } e) + ke$, với k bất kỳ, thuộc N.
Bước 4. Tính $n = p.q$, $\varphi(n) = (p-1).(q-1)$ và kiểm tra xem đã có được $e < \varphi(n)$ và $gcd(e, \varphi(n)) = 1$. Nếu thỏa mãn, chuyển sang Bước 5, ngược lại quay về Bước 2.
Bước 5. Tính trực tiếp số mũ giải mã d theo công thức $d = \varphi(n) - \dfrac{\varphi(n) - 1}{e}$ là nghịch đảo nhân của e.

Rõ ràng là các bước của thuật toán cũng như việc tìm các số nguyên tố p, q thỏa điều kiện đủ đưa ra trong thuật toán là luôn thực hiện được.

Ví dụ 9. Với $e = 27$, ta có tập $T(27) = \{2, 5, 8, 11, 14, 17, 20, 23, 26\}$ và lực lượng $(T(27)| = 9$. Áp dụng thuật toán trên chọn ngẫu nhiên $r_p = 2, c_p = 204463810153171834065$, số nguyên tố $p = c_p.e + r_p = 5520522874135639519757$.

Chọn ngẫu nhiên

$k = 597085208340567843261276397956937569875679136791758623908213495$.

Tính một số nguyên tố

$$q = r_p(r_p - 1)^{-1}(\text{ mod } e) + ke$$
$$= 161213006251953317680544627448373143866433366933774828455217643 67.$$

$$n = p.q$$
$$= 889980088622080152182232427159924125211242016499718475695792867883457086948311950988 19.$$

$$\varphi(n) = (p-1).(q-1)$$
$$= 889980088622080152182071214153672171893561471872270102551926434461318083378500338146 96.$$

Tính trực tiếp số mũ giải mã d theo công thức $d = \varphi(n) - \dfrac{\varphi(n) - 1}{e}$,

$$d = 857017863117558665064216724740573202564170306247371209864818047999787783994111436734 11.$$

Như vậy, với mỗi e và r_p đã chọn chỉ cần thay đổi c_p và k, ta có thể tìm được hai số nguyên tố p và q khác nhau.

4. KẾT LUẬN

Qua việc khảo sát tập $T(e) = \{r \in Z_e^* | (r-1) \in Z_e^*\}$, ta đã thấy nếu e không là một hợp số chẵn thì tập $T(e)$ là khác rỗng, có số phần tử lớn nếu e lớn và được tính theo công thức

$$|T(e)| = \prod_{i=1}^{t} (p_i - 2) p_i^{e_i - 1},$$

và tỷ số $\dfrac{T(e)}{|Z_e^*|}$ trong đa số trường hợp dao động quanh giá trị $\frac{1}{2}$.

Mặt khác, theo định lý Dirichlet: Nếu e và r_p nguyên tố cùng nhau thì khi đó cấp số cộng $r_p,\ e + r_p,\ 2e + r_p,\ 3e + r_p, ...$ chứa một số vô hạn các số nguyên tố.

(Chú ý là ở đây ta đã lấy $r_p \in T(e)$ để có được $(r_p - 1) \in Z_e^*$).

Lời cảm ơn. Chúng tôi xin chân thành cảm ơn PGS.TS Hồ Thuần đã đọc và có nhiều ý kiến đóng góp xác đáng, giúp chúng tôi hoàn thiện bài báo này.

TÀI LIỆU THAM KHẢO

[1] Vũ Huy Hoàng, Đặng Văn Chuyết, Phương pháp sinh khóa RSA an toàn, *Tạp chí Khoa học và Công nghệ các trường Đại học Kỹ thuật* (68) (2008) 22–27.

[2] Vũ Huy Hoàng, Lê Xuân Tuấn, Xây dựng hệ mật RSA an toàn với số mũ giải mã lớn, *Tạp chí Khoa học và Kỹ thuật, Học viện Kỹ thuật quân sự* (125) (2008) 31–36.

[3] Dan Boneh, Twenty years of attacks on the RSA cyptosystem, *Notices of the AMS* **46** (2) (1999) 203–213.

[4] Andrej Dujella, A variant of Wiener's attack on RSA, *Computing* **85** (2009) Springer Wien, 77–83.

[5] M. Ernst, E. Jochemsz, A. May, B. de Weger, Partial key exposure attacks on RSA up to full size exponents, *Advanced in Cryptology-EUROCRYPT 05*, Springer-Verlag, 2005, (371–385).

[6] M. Wiener, Cryptanalysis of short RSA secret exponents, *IEEE Transactions on Information Theory* **36** (1990) 553–558.

[7] Dan Boneh and G.Durfee, Cryptanalysis of RSA with private key d less than N0,292, *IEEE Trans. Inform. Theory* **46** (4) (2000) 1339–1349.

Nhận bài ngày 3 - 7 - 2009
Nhận lại sau sửa ngày 26 - 10 -2009