CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

7.11 Định lý. Nếu p là số nguyên tố lẻ thì

$$\left[\frac{2}{p}\right] \equiv (-1)^{(p^2-1)/8}.$$

Chứng minh. Đặt $A = \{a.2 \mid 1 \le a \le (p-1)/2\}$. Để áp dụng Bổ đề Gauss ta đi tính t là số thặng dư nhỏ nhất trong tập A lớn hơn $p/2$. Ta có

$$2a > \frac{p}{2} \Rightarrow \frac{p}{4} < a \le \frac{p-1}{2}.$$

Suy ra $$t = \frac{p-1}{2} - \left[\frac{p}{4}\right] \Rightarrow \left[\frac{2}{p}\right] = (-1)^{(p-1)/2-[p/4]},$$

Với $\left[\frac{p}{4}\right]$ là phần nguyên của $p/4$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

$$p = 4k+1 \Rightarrow \frac{p^2-1}{8} = 2k^2 + k; \frac{p-1}{2} - \left[\frac{p}{4}\right] = k.$$

$$p = 4k+3 \Rightarrow \frac{p^2-1}{8} = 2k^2 + 3k + 1; \frac{p-1}{2} - \left[\frac{p}{4}\right] = k+1$$

$$\Rightarrow \frac{p-1}{2} - \left[\frac{p}{4}\right] \equiv \frac{(p^2-1)}{8} \pmod 2.$$

Do đó

$$\left[\frac{2}{p}\right] \equiv (-1)^{(p^2-1)/8} \pmod 2 \Rightarrow \left[\frac{2}{p}\right] \equiv (-1)^{(p^2-1)/8}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

§8 Luật thuận nghịch bình phương.

8.1 Bổ đề Cho p là số nguyên tố lẻ và a là số lẻ không chia hết cho p. Khi đó

$$\left[\frac{a}{p}\right] = (-1)^{\sum_{j=1}^{(p-1)/2} [ja/p]}$$

Chứng minh. Xét các thặng dư dương nhỏ nhất của dãy số

$$a, 2, \dots, ((p-1)/2)\,a.$$

Gọi $u_1, u_2, \dots, u_s$; $v_1, v_2, \dots, v_t$ lần lượt là các thặng dư bé hơn và lớn hơn $p/2$. Với mọi $j = 1, \dots, (p-1)/2$, $ja = p[ja/p]$ + phần dư. Trong đó phần dư là một trong các u_r hoặc v_l.

Cộng $(p-1)/2$ đẳng thức lại ta có

$$\sum_{j=1}^{(p-1)/2} ja = p\sum_{j=1}^{(p-1)/2} [ja/p] + \sum_{r=1}^{s} u_r + \sum_{l=1}^{t} v_l \quad (1)$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Trong chứng minh Bổ đề Gauss, ta đã chứng minh

$$\{u_1, \dots, u_s, p-v_1, \dots p-v_t\} = \{1, 2, \dots, (p-1)/2\}$$

$$\Rightarrow \sum_{j=1}^{(p-1)/2} j = \sum_{r=1}^{s} u_r + \sum_{l=1}^{t}(p-v_l) = \sum_{r=1}^{s} u_r + pt - \sum_{l=1}^{t} v_l \quad (2)$$

$$(1)-(2) \Rightarrow (a-1)\sum_{j=1}^{(p-1)/2} j = p\sum_{j=1}^{(p-1)/2}[ja/p] - pt + 2\sum_{l=1}^{t} v_l$$

Do a lẻ nên $p\sum_{j=1}^{(p-1)/2}[ja/p] \equiv pt \pmod 2$.

Từ $(p, 2) = 1$, $\bar{p}$ khả nghịch trong $\mathbb{Z}_2$. Suy ra $\sum_{j=1}^{(p-1)/2}[ja/p] \equiv t \pmod 2$.

Áp dụng Bổ đề Gauss $$\left[\frac{a}{p}\right] = (-1)^t = (-1)^{\sum_{j=1}^{(p-1)/2}[ja/p]}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

8.2 Định lý. Cho p, q là hai số nguyên tố lẻ phân biệt. Khi đó

$$\left[\frac{p}{q}\right]\left[\frac{q}{p}\right] = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Chứng minh.

Xét các cặp số (x, y) với $1 \le x \le (p-1)/2$, $1 \le y \le (q-1)/2$. Có tất cả $(p-1)/2$. $(q-1)/2$ cặp số trên. Nếu $qx = py$ thì $q|py$ do $(p, q) = 1$ nên $q|y$ (vô lý) vậy $qx \ne py$ với mọi cặp.

Chia các cặp số trên làm 2 tập

$$A_2 = \left\{(x,y) \,\middle|\, 1 \le x \le \frac{p-1}{2}; 1 \le y \le \frac{q-1}{2}; qx < py\right\} =$$

$$\left\{(x,y) \,\middle|\, 1 \le y \le \frac{p-1}{2}; 1 \le x \le \frac{py}{q}\right\}$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

$$A_1 = \left\{(x,y) \,\middle|\, 1 \le x \le \frac{p-1}{2}; 1 \le y \le \frac{q-1}{2}; py < qx\right\} =$$

$$\left\{(x,y) \,\middle|\, 1 \le x \le \frac{p-1}{2}; 1 \le y \le \frac{qx}{p}\right\}$$

Với mỗi $1 \le x \le (p-1)/2$, có đúng $[qx/p]$ phần tử y xuất hiện trong tất cả các cặp (x, y) thuộc A_1. Suy ra số phần tử

$$|A_1| = \sum_{x=1}^{(p-1)/2}\left[\frac{qx}{p}\right]$$

Tương Tự

$$|A_2| = \sum_{y=1}^{(p-1)/2}\left[\frac{py}{q}\right]$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

$$\Rightarrow \frac{p-1}{2}.\frac{q-1}{2} = |A_1| + |A_2| = \sum_{x=1}^{(p-1)/2}\left[\frac{qx}{p}\right] + \sum_{y=1}^{(p-1)/2}\left[\frac{py}{q}\right]$$

Áp dụng Bổ đề 8.1

$$\begin{bmatrix} p \\ q \end{bmatrix}\begin{bmatrix} q \\ p \end{bmatrix} = (-1)^{\left(\sum_{y=1}^{(p-1)/2}\left[\frac{py}{q}\right] + \sum_{x=1}^{(p-1)/2}\left[\frac{qx}{p}\right]\right)} = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

8.3 Thí dụ. Tính $\begin{bmatrix} 713 \\ 1009 \end{bmatrix}$

Giải. ta có 1009 là số nguyên tố và 1009 ≡1(mod 4).

$$\begin{bmatrix} 713 \\ 1009 \end{bmatrix} = \begin{bmatrix} 23\times 31 \\ 1009 \end{bmatrix} = \begin{bmatrix} 23 \\ 1009 \end{bmatrix}\begin{bmatrix} 31 \\ 1009 \end{bmatrix}(7.8(b))$$

Áp dụng Định lý 8.2 ta có

$$\begin{bmatrix} 23 \\ 1009 \end{bmatrix} = \begin{bmatrix} 1009 \\ 23 \end{bmatrix}(-1)^{\frac{23-1}{2}\times\frac{1009-1}{2}}\begin{bmatrix} 1009 \\ 23 \end{bmatrix} = \begin{bmatrix} 1009 \\ 23 \end{bmatrix} = \begin{bmatrix} 20 \\ 23 \end{bmatrix} = \begin{bmatrix} 2^2 \\ 23 \end{bmatrix}\begin{bmatrix} 5 \\ 23 \end{bmatrix} =$$

$$\begin{bmatrix} 5 \\ 23 \end{bmatrix} = \begin{bmatrix} 23 \\ 5 \end{bmatrix} = \begin{bmatrix} 3 \\ 5 \end{bmatrix} = \begin{bmatrix} 5 \\ 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \end{bmatrix} = -1(7.11)$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

$$\begin{bmatrix} 31 \\ 1009 \end{bmatrix} = \begin{bmatrix} 1009 \\ 31 \end{bmatrix} = \begin{bmatrix} 17 \\ 31 \end{bmatrix} = \begin{bmatrix} 31 \\ 17 \end{bmatrix} = \begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} 2 \\ 17 \end{bmatrix}\begin{bmatrix} 7 \\ 17 \end{bmatrix} = \begin{bmatrix} 7 \\ 17 \end{bmatrix}$$

$$= \begin{bmatrix} 17 \\ 7 \end{bmatrix} = \begin{bmatrix} 3 \\ 7 \end{bmatrix} = -\begin{bmatrix} 7 \\ 3 \end{bmatrix} = -\begin{bmatrix} 1 \\ 3 \end{bmatrix} = -1$$

$$\Rightarrow \begin{bmatrix} 713 \\ 1009 \end{bmatrix} = -1.$$

Thực hành. Cho biết 703 = 37.19. Tính $\begin{bmatrix} 703 \\ 1231 \end{bmatrix}$

Đáp án. $\begin{bmatrix} 37 \\ 1231 \end{bmatrix} = -1; \begin{bmatrix} 19 \\ 1231 \end{bmatrix} = -1.$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

§9 Kí hiệu Jacobi.

9.1 Định nghĩa. Cho $n = p_1^{t_1}p_2^{t_2}...p_k^{t_k}$ và $(a, n) = 1$. Kí hiệu Jacobi được định nghĩa là

$$\begin{bmatrix} a \\ n \end{bmatrix} = \begin{bmatrix} a \\ p_1 \end{bmatrix}^{t_1}\begin{bmatrix} a \\ p_2 \end{bmatrix}^{t_2}...\begin{bmatrix} a \\ p_k \end{bmatrix}^{t_k}.$$

Trong đó các kí hiệu $\begin{bmatrix} a \\ p_i \end{bmatrix}$ ở vế phải là kí hiệu Legendre.

9.2 Chú ý. Khái niệm Jacobi là một mở rộng của khái niệm Legendre.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

9.3 Mệnh đề. Cho n là số nguyên dương lẻ, a và b là các số nguyên tố cùng nhau với n. Khi đó.

a) Nếu $a \equiv b(mod\ p)$ thì $\begin{bmatrix} a \\ n \end{bmatrix} = \begin{bmatrix} b \\ n \end{bmatrix}$.

b) $\begin{bmatrix} a \\ n \end{bmatrix}\begin{bmatrix} b \\ n \end{bmatrix} = \begin{bmatrix} ab \\ n \end{bmatrix}$

c) $\begin{bmatrix} a^2 \\ n \end{bmatrix} = 1$.

d) $\begin{bmatrix} -1 \\ n \end{bmatrix} = (-1)^{\frac{n-1}{2}}$.

e) $\begin{bmatrix} 2 \\ n \end{bmatrix} = (-1)^{\frac{p^2-1}{2}}$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Chứng minh. (a), (b), (c) suy trực tiếp từ định nghĩa Jacobi và tính chất của Legendre.

d) Viết $n = p_1^{t_1}p_2^{t_2}...p_k^{t_k}$. Do p_i -1 chẵn nên

$$p_i^{t_i} = (1+(p_i-1))^{t_i} = \sum_{u=0}^{t_i} C_{t_i}^u (p_i-1)^{t_i} \equiv 1 + t_i(p_i-1)(\text{mod } 4).$$

$$(1+t_i(p_i-1))(1+t_j(p_j-1)) \equiv 1 + t_i(p_i-1) + t_j(p_j-1)(\text{mod } 4)$$

$$\Rightarrow n \equiv \prod_{i=1}^{k} t_i(p_i-1)(\text{mod } 4) = 1 + \sum_{i=1}^{k} t_i(p_i-1)(\text{mod } 4)$$

$$\Rightarrow \frac{n-1}{2} \equiv \sum_{i=1}^{k} t_i\frac{(p_i-1)}{2}(\text{mod } 2).$$ Theo tiêu chuẩn Euler

$$\begin{bmatrix} -1 \\ n \end{bmatrix} = \prod_{i=1}^{k}\begin{bmatrix} -1 \\ p_i \end{bmatrix}^{t_i} = \prod_{i=1}^{k}(-1)^{t_i\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^{k} t_i\frac{p_i-1}{2}} = (-1)^{\frac{n-1}{2}}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

e) Ta có $p_i^2 - 1 \vdots 4$

$$p_i^{2t_i} = \left(1 + \left(p_i^2 - 1\right)\right)^{t_i} = \sum_{u=0}^{t_i} C_{t_i}^u \left(p_i^2 - 1\right)^{t_i} \equiv 1 + t_i\left(p_i^2 - 1\right) \pmod{16}.$$

$$\left(1 + t_i\left(p_i^2 - 1\right)\right)\left(1 + t_j\left(p_j^2 - 1\right)\right) \equiv 1 + t_i\left(p_i^2 - 1\right) + t_j\left(p_j^2 - 1\right) \pmod{16}$$

$$\Rightarrow n^2 \equiv \prod_{i=1}^{k} t_i\left(p_i^2 - 1\right) \pmod{16} = 1 + \sum_{i=1}^{k} t_i\left(p_i^2 - 1\right) \pmod{16}$$

$$\Rightarrow \frac{n-1}{2} \equiv \sum_{i=1}^{k} t_i \frac{\left(p_i^2 - 1\right)}{2} \pmod{8}.$$

$$\begin{bmatrix} 2 \\ n \end{bmatrix} = \prod_{i=1}^{k} \begin{bmatrix} 2 \\ p_i \end{bmatrix}^{t_i} = \prod_{i=1}^{k} (-1)^{t_i \frac{p_i^2 - 1}{8}} = (-1)^{\sum_{i=1}^{k} t_i \frac{p_i^2 - 1}{8}} = (-1)^{\frac{n^2 - 1}{2}}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

9.4 Định lý (luật thuận nghịch bình phương của Jacobi). Cho *m, n* là hai số nguyên dương lẻ nguyên tố cùng nhau. Khi đó

$$\begin{bmatrix} m \\ n \end{bmatrix}\begin{bmatrix} n \\ m \end{bmatrix} = (-1)^{\frac{m-1}{2} \times \frac{n-1}{2}}.$$

Chứng minh. Viết $m = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}, n = q_1^{s_1} q_2^{s_2} \ldots q_t^{s_t}; p_i, q_j$ nguyên tố. Áp dụng luật thuận nghịch Legendre, ta có

$$\begin{bmatrix} m \\ n \end{bmatrix}\begin{bmatrix} n \\ m \end{bmatrix} = \prod_{i=1}^{k}\prod_{j=1}^{t} (-1)^{r_i \frac{p_i - 1}{2} \times s_j \frac{p_j - 1}{2}} = (-1)^{\sum_{i=1}^{k}\sum_{j=1}^{t} r_i \frac{p_i - 1}{2} \times s_j \frac{p_j - 1}{2}} = (-1)^{\sum_{i=1}^{k} r_i \frac{p_i - 1}{2} \sum_{i=1}^{k} s_j \frac{p_j - 1}{2}}$$

Trong chứng minh 9.3, ta có

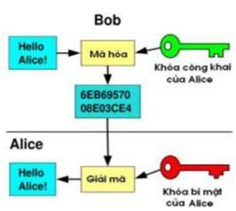
$$\frac{m-1}{2} \equiv \sum_{i=1}^{k} r_i \frac{\left(p_i - 1\right)}{2} \pmod{2}; \frac{n-1}{2} \equiv \sum_{i=1}^{k} s_j \frac{\left(p_i - 1\right)}{2} \pmod{2}$$

$$\Rightarrow \begin{bmatrix} m \\ n \end{bmatrix}\begin{bmatrix} n \\ m \end{bmatrix} = (-1)^{\frac{m-1}{2} \times \frac{n-1}{2}}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

§10 Sơ lược mật mã khóa công khai.

10.1 Tổng quan về mật mã công khai



Sơ đồ mã hóa công khai

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Hệ mã công khai sử dụng hai khóa có quan hệ toán học với nhau, tức là một khóa này được hình thành từ khóa kia.

Người muốn nhận bản mã (Alice) tạo ra một khóa mật (private key) và từ khóa mật, tính ra khóa công khai (public key) với một thủ tục không phức tạp, còn việc tìm khóa mật khi biết khóa công khai là bài toán khó giải được.

Khóa công khai sẽ đưa đến cho người gởi bản tin (Bob) qua kênh công cộng. Và bản tin được Bob mã hóa bằng khóa công cộng. Bản mã truyền đến Alice, và nó được giải mã bằng khóa mật.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

10.2 Hệ mật mã RSA

10.2.1 Quá trình tạo khóa cho hệ mật RSA.

Giả sử Alice và Bob cần trao đổi thông tin bí mật thông qua một kênh không an toàn (ví dụ như Internet). Với thuật toán RSA, Alice đầu tiên cần tạo ra cho mình cặp khóa gồm khóa công khai và khóa bí mật theo 6 bước sau:

a) Chọn 2 số nguyên tố lớn khác nhau *p*, *q* thỏa mãn điều kiện $|p| \approx |q|$

b)Tính tích $n = pq$.

c) Tính giá trị hàm Phi Euler của n: $\phi(n) = (p-1)(q-1)$.

d) Chọn số nguyên *d*, sao cho $d < \phi(n), (d, \phi(n)) = 1$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

e) Tính giá trị *e* thỏa mãn điều kiện: $ed \equiv 1\left(\bmod\ \phi(n)\right)$.

d) Khóa công khai bao gồm *n* và *e*. Khóa mật là *d*

(giá trị *p,q* bị xóa sau khi tính toán khóa)

10.2.2 Quá trình mã hóa. Giả sử Bob muốn gửi đoạn thông tin *m* nhỏ hơn *n* cho Alice, thì Bob tính bản mã như sau: $c = m^e \pmod{n}$ rồi gửi *c* cho Bob.

10.2.3 Quá trình giải mã. Alice nhận *c* từ Bob và khóa bí mật *d*. Alice có thể tìm được *m* từ *c* theo công thức sau:

$$m = c^d \pmod{n}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Quá trình giải mã hoạt động vì ta có

$$c^d = (m^e)d = m^{ed} \pmod n$$

Do $ed \equiv 1 \pmod{p-1}$ và $ed \equiv 1 \pmod{q-1}$ và Định lý Fermat nhỏ nên

$$m^{ed} \equiv m \pmod p, m^{ed} \equiv m \pmod q.$$

Do p và q là hai số nguyên tố cùng nhau, áp dụng định lý phần dư trung hoa, chúng ta có:

$$m^{ed} \equiv m \pmod{pq}.$$

Hay

$$c^d \equiv m \pmod n.$$

10.2.4 Thí dụ: $p = 70793$; $q = 707933$; $n = pq = 50116700869$;
$\phi(n) = (p-1)(q-1) = 50115922144$
$d = 30483041$; $e = 5851898625$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

m	$m' = c^d \pmod n$	$c = m^e \pmod n$
30483041	7523619714	**30483041**
7523619714	38101458113	**7523619714**
3487987	4469234330	**3487987**
754553	45262687896	**754553**
884545	48968540294	**884545**
46665533	10037623855	**46665533**
15657	29531681112	**15657**
95432	4648093185	**95432**
4545786	38326603863	**4545786**
777543	38921288996	**777543**
45673222	**21930948547**	**45673222**

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

10.2.5 Một số chú ý quan trọng về RSA

An ninh: Độ an toàn của hệ thống RSA dựa trên 2 vấn đề của toán học:

a) Bài toán phân tích ra thừa số nguyên tố các số nguyên lớn

b) Bài toán RSA.

Nếu 2 bài toán trên là khó (không tìm được thuật toán hiệu quả để giải chúng) thì không thể thực hiện được việc phá mã toàn bộ đối với RSA. Phá mã một phần phải được ngăn chặn bằng các phương pháp chuyển đổi bản rõ an toàn.

Bài toán RSA là bài toán tính căn bậc *e* môđun *n* (với *n* là hợp số): tìm số *m* sao cho $m^e = c$ mod n, trong đó (e, n) chính là khóa công khai và *c* là bản mã.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Hiện nay phương pháp triển vọng nhất giải bài toán này là phân tích *n* ra thừa số nguyên tố. Khi thực hiện được điều này, kẻ tấn công sẽ tìm ra số mũ bí mật *d* từ khóa công khai và có thể giải mã theo đúng quy trình của thuật toán.

Nếu kẻ tấn công tìm được 2 số nguyên tố *p* và *q* sao cho: $n = pq$ thì có thể dễ dàng tìm được giá trị $(p-1)(q-1)$ và qua đó xác định *d* từ *e*.

Hiện nay chưa có một phương pháp nào được tìm ra trên máy tính để giải bài toán này trong thời gian đa thức (*polynomial-time*). Tuy nhiên người ta cũng chưa chứng minh được điều ngược lại (sự không tồn tại của thuật toán).

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Chiều dài khóa: Số *n* cần phải có kích thước không nhỏ hơn 512 bít. Năm 2006 hệ mật RSA được cho là hiệu quả với kích thước n phải từ 1024 trở lên. Và họ khuyến cáo là tương lai thì chiều dài n phải từ 2024 bít.

Chọn tham số công khai:

Để nâng cao tốc độ mã hóa, thì chúng ta nên chọn *e* với giá trị không lớn, thường là 3, 7 hay 65537. Các số này khi biểu diễn ở dạng nhị phân chỉ có 2 chữ số 1, nên khi thực hiện lệnh lũy thừa sẽ giảm đi lệnh nhân.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Chọn tham số mật.

p và *q* còn cần được chọn không quá gần nhau để phòng trường hợp phân tích *n* bằng phương pháp phân tích Fermat. Ngoài ra, nếu $p - 1$ hoặc $q - 1$ có thừa số nguyên tố nhỏ thì *n* cũng có thể dễ dàng bị phân tích theo phương pháp $p - 1$ Pollaid và vì thế *p* và *q* cũng cần được thử để tránh khả năng này. Chúng ta có thể chọn như sau. Trước tiên tìm số nguyên tố p_1 sao cho $p = 2p_1+1$ cũng là số nguyên tố, tương tự chọn số nguyên tố lớn q_1 sao cho $q = 2q_1+1$ cũng là số nguyên tố.

Giá trị *d* cần phải đủ lớn. Năm 1990 Michael J. Wiener đã chứng minh rằng nếu $q < p < 2q$ và $d < n^{1/4}/3$, thì có phương pháp hiệu quả để tính *d* theo *n* và *e*.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

10.3 Hệ mật mã Elgama. Hệ mật Elgama hình thành trên cơ sở bài toán logarith rời rạc. Được đề xuất năm 1984. Sau đó chuẩn chữ ký điện tử của Mỹ và Nga hình thành trên cơ sở hệ mật này.

10.3.1 Hình thành khóa:

Giả sử Alice và Bob muốn trao đổi thông tin mật với nhau bằng hệ mật Elgamma. Trước tiên Alice thực hiện qúa trình hình thành khóa như sau:

1) Chọn số nguyên tố đủ lớn p có chiều dài đủ lớn sao cho bài toán logarithm trong là khó giải.

2) Chọn $\alpha \in \mathbb{Z}_p^*$, là nghiệm nguyên thủy. Chọn x là số ngẫu nhiên sao cho $1 < x < p$.

3) Tính giá trị y thỏa mãn công thức: $y \equiv \alpha^x \pmod{p}$.

Khóa mật là x, còn khóa mở là 3 số (α, p, y).

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

10.3.2 Quá trình mã hóa bản tin T < p:

1) Chọn số ngẫu nhiên $k < p$. Tính $C_1 = \alpha^k \pmod{p}$.

2) Tính $C_2 = y^k T \pmod{p}$.

Bob gởi khóa công khai (C_1, C_2, p) đến Alice, k sẽ bị hủy

10.3.3 Quá trình giải mã:

1) Tính giá trị: $Z \equiv C_1^x \pmod{p}$.

2) Tính nghịch đảo của Z: $Z^{-1} \equiv \left(C_1^x\right)^{-1} \pmod{p} \equiv \alpha^{-kx} \pmod{p}$

3) $T = C_2.Z^{-1} \pmod{p}$

Chúng ta kiểm chứng lại quá trình giải mã là đúng như sau:

$$C_2 Z^{-1} \equiv y^k T \alpha^{-kx} \pmod{p} \equiv \alpha^{kx} T \alpha^{-kx} \pmod{p} \equiv T \pmod{p}$$

10.3.4 Thí dụ. $p = 707933$; $\alpha = 203$; $x = 765$; $y = 371696$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

T	K	C_1	C_2	Z	Z^{-1}
455	457	381267	263892	181064	168667
2222	333	309977	295242	545579	313868
554	2224	114192	691348	394828	530064
6878	1175	413040	378587	351963	684082
34333	95453	77756	76073	698244	194793
332	545	417805	454024	231659	89120
978	9996	618551	421976	527400	247794
8656	778645	305246	144687	305321	329172
1233	7564	558848	379425	523937	419571
8965	3434	239368	626159	658412	701743