- Kỹ thuật để chọn cơ sở nhân tử chưa được chỉ ra.

- Phương pháp hiệu quả để chỉ ra một số quan hệ cần thiết cũng chưa được chỉ ra.

- Kỹ thuật này cũng không được áp dụng cho mọi nhóm.

### *3.4.2. Mã hóa, giải mã Elgamal*

#### *3.4.2.1. Thuật toán tạo khóa*

Tóm lược: Mỗi đầu liên lạc tạo một khoá công khai và một khoá bí mật tương ứng :

(1) Tạo 1 số nguyên tố p lớn và một phần tử sinh $\alpha$ của nhóm nhân $Z_p^*$ của các số nguyên $\bmod p$.

(2) Chọn một số nguyên ngẫu nhiên a, $1 \le a \le p-2$ và tính $\alpha^a \bmod p$.

(3) Khoá công khai là bộ 3 số $(p, \alpha, \alpha^a)$, khoá bí mật là a.



#### *3.4.2.2. Thuật toán mã hóa, giải mã*

*Tóm lược*: B mã hoá một thông tin báo m để gửi cho A bản mã cần gửi.

***Mã hoá:*** B phải thực hiện các bước sau:

(1) Nhận khoá công khai $(p, \alpha, \alpha^a)$ của A.

(2) Biểu thị bản tin dưới dạng một số nguyên m trong dải $\{0, 1, \ldots, p-1\}$.

(3) Chọn số nguyên ngẫu nhiên k, $1 \le k \le p-2$



(4) Tính $\gamma = \alpha^k \bmod p$ và $\delta = m(\alpha^a)^k \bmod p$.

(5) Gửi bản mã $c = (\gamma, \delta)$ cho A

***Giải mã:*** Để khôi phục bản rõ m từ c, A phải thực hiện các bước sau:

(1) Sử dụng khoá riêng a để tính $\gamma^{p-1-a} \bmod p$

(Chú ý $\gamma^{p-1-a} = \gamma^{-a} = \gamma^{-ak}$)

(2) Khôi phục bản rõ bằng cách tính $\left(\gamma^{-a}\right)\delta \bmod p$.

*Chứng minh hoạt động giải mã:*

Thuật toán trên cho phép A thu được bản rõ vì:

$$\gamma^{-a}\delta \equiv \alpha^{-ak}.m\alpha^{ak} \equiv m \bmod p$$

*3.4.2.3. Ví dụ*

***Tạo khoá.***

A chọn p = 2357 và một phần tử sinh $\alpha = 2$ của $Z_{2357}^{*}$. A chọn khoá bí mật a = 1751 và tính $\alpha^{a} \bmod p = 2^{1751} \bmod 2357 = 1185$. Khoá công khai của A là $\left(p = 2357, \alpha = 2, \alpha^{a} = 1185\right)$

***Mã hoá***

Để mã hoá bản tin m = 2035, B sẽ chọn một số nguyên ngẫu nhiên k = 1520 và tính:

$$\gamma = 2^{1520} \bmod 2357 = 1430$$

và $$\delta = 2035.1185^{1520} \bmod 2357 = 697$$

Sau đó B gửi $c = (1430, 697)$ cho A

***Giải mã***

Để giải mã A phải tính:

$$\gamma^{p-1-a} = 1430^{605} \bmod 2357 = 872$$

Sau đó khôi phục bản rõ m bằng cách tính:

$m = 872.697 \bmod 2357 = 2035$.

***3.4.3. Tham số của hệ mật***

Để chống lại các thuật toán tấn công P-Pollard, Pollig-Hellman, số nguyên tố p được chọn phải thỏa mãn một số điều kiện sau:

$$\begin{cases} p-1 \text{ có ước số nguyên tố lớn (cỡ 100 bit trở lên)} \\ p \text{ có độ lớn cỡ 1024 bit trở lên} \end{cases}$$