Bài 3.2 Hệ mật mã khoá công khai ElGamal.

1. Mô tả hệ mật mã ElGamal.

Hệ mật mã ElGamal được T. ElGamal đề xuất năm 1985, dựa vào độ phức tạp của bài toán tính lôgarit rời rạc, và sau đó đã nhanh chóng được sử dụng rộng rãi không những trong vấn đề bảo mật truyền tin mà còn trong các vấn đề xác nhận và chữ ký điện tử.

Sơ đồ hệ mật mã khoá công khai ElGamal được cho bởi

$$S = (P, C, K, E, D),$$

trong đó: $P = Z_p^*$, $C = Z_p^* \times Z_p^*$, với p là một số nguyên tố;

$$K = \{K = (K', K'') : K' = (p, \alpha, \beta),\ K'' = a,\ \beta \equiv \alpha^a \bmod p\},$$

ở đây α là một phần tử nguyên thuỷ theo mod$p$, tức của Z_p^*.

Các thuật toán lập mã $e_{K'} = E(K',.)$ và giải mã $d_{K''} = D(K'',.)$ được xác định như sau: Với mỗi $x \in P = Z_p^*$, để lập mật mã cho x trước hết ta chọn thêm một số ngẫu nhiên $k \in Z_{p-1}$ rồi tính:

$$e_{K'}(x,k) = (y_1, y_2), \quad \text{với} \quad \begin{cases} y_1 = \alpha^k \bmod p, \\ y_2 = x.\beta^k \bmod p. \end{cases}$$

Với mọi số ngẫu nhiên k bất kỳ, ta đều xem $e_{K'}(x,k)$ là mật mã của x. Và thuật toán giải mã được xác định bởi

$$d_{K''}(y_1, y_2) = y_2.(y_1^a)^{-1} \bmod p.$$

Các phép lập mật mã và giải mã được xác định như vậy là hợp thức, vì ta có với mọi $x \in P = Z_p^*$ và mọi $k \in Z_{p-1}$:

$$d_{K''}(e_{K'}(x,k)) = x.\beta^k.(\alpha^{k.a})^{-1} \bmod p = x.\beta^k.\beta^{-k} \bmod p = x.$$

Ta chú ý rằng trong một mạng truyền thông bảo mật với việc dùng sơ đồ mật mã ElGamal, mỗi người tham gia tự chọn cho mình các tham số p, α, a, rồi tính β, sau đó lập và công bố khoá công khai $K' = (p, \alpha, \beta)$, nhưng phải giữ tuyệt mật khoá bí mật $K'' = a$. Bài toán biết khoá công khai tìm ra khoá bí mật chính là bài toán tính lôgarit rời rạc được kể đến trong mục 4.1.2, một bài toán khó cho đến nay chưa có một thuật toán nào làm việc trong thời gian đa thức giải được nó.

Thí dụ : Chọn $p = 2579$, $\alpha = 2$, $a = 765$, ta tính được $\beta = 2^{765} = 949 \bmod 2579$. Ta có khoá công khai (2579, 2, 949) và khoá bí mật 765. Giả sử để lập mật mã cho $x = 1299$, ta chọn ngẫu nhiên $k = 853$, sẽ có

$$e_{K'}(1299, 853) = (2^{853}, 1299.949^{853}) \bmod 2579$$
$$= (453, 2396).$$

Và giải mã ta được lại

$$d_{K''}(453, 2396) = 2396.(453^{765})^{-1} \bmod 2579 = 1299.$$

2. Tính an toàn của hệ mật mã ElGamal.

Như đã trình bày ở trên, nếu ta xem tính an toàn của hệ mật mã ElGamal là ở việc giữ tuyệt mật khoá bí mật K'', thì ta có thể yên tâm vì bài toán phát hiện khoá bí mật có độ khó tương đương

với bài toán tính lôgarit rời rạc, mà bài toán này thì như ở các mục 4.1.2 và 2.4.3 đã chứng tỏ, cho đến nay chưa có một thuật toán nào làm việc trong thời gian đa thức giải được nó. Có một điều cảnh báo là nên chú ý chọn môđuyn p là số nguyên tố sao cho p -1 có ít nhất một ước số nguyên tố lớn (xem 2.4.3). Điều đó là thực hiện được nếu số nguuyên tố p được chọn là số nguyên tố Sophie Germain (tức có dạng $2q+1$, với q cũng là số nguyên tố lớn).

Ngoài ra, còn có khả năng khoá bí mật $K'' = a$ bị lộ do cẩu thả trong việc sử dụng số ngẫu nhiên k, đặc biệt là khi *để lộ số k được dùng*. Thực vậy, nếu để lộ số k, thì khoá bí mật a được tính ra ngay theo công thức sau đây:

$$a = (x - ky_2)y_1^{-1} \bmod (p-1).$$

Như vậy,một người thám mã có khả năng tấn công theo kiểu "biết cả bản rõ" (xem 1.5.1) có thể phát hiện ra khoá a nếu biết k .

Một trường hợp khác làm mất tính an toàn của hệ mật mã ElGamal là việc *dùng cùng một số k cho nhiều lần lập mật mã*. Thực vậy, giả sử dùng cùng một số ngẫu nhiên k cho hai lần lập mã, một lần cho x_1 , một lần cho x_2 , và được các bản mã tương ứng (y_1,y_2) và (z_1,z_2). Vì cùng dùng một số k nên $y_1=z_1$. Và do đó theo công thức lập mã ta có $z_2/y_2 = x_2/x_1$, tức là $x_2 = x_1.z_2/y_2$. Như vậy, một người thám mã, một lần "biết cả bản rõ" dễ dàng phát hiện được bản rõ trong các lần sau.

3. Các hệ mật mã tương tự ElGamal.

Hệ mật mã ElGamal được xây dựng dựa trên các yếu tố : một nhóm hữu hạn cyclic (Z_p^*), một phần tử nguyên thuỷ ($\alpha \in Z_p^*$) sao cho bài toán tính lôgarit rời rạc (tính $a = \log_\alpha \beta$, tức cho β tìm a sao cho $\beta = \alpha^a \bmod p$) là rất khó thực hiện. Vì vậy, nếu có đủ các yếu tố đó thì ta có thể xây dựng các hệ mật mã tương tự ElGamal. Như vậy, sơ đồ của một hệ mật mã tương tự ElGamal được cho bởi

$$S = (P, C, K, E, D),$$

trong đó: $P = G$, $C = G \times G$, với G là một nhóm cyclic hữu hạn;

$$K = \{K = (K', K'') : K' = (G, \alpha, \beta),\ K'' = a,\ \beta = \alpha^a\},$$

ở đây α là một phần tử nguyên thuỷ của nhóm G.

Các thuật toán lập mã $e_{K'} = E(K',.)$ và giải mã $d_{K''} = D(K'',.)$ được xác định như sau: Với mỗi $x \in P = G$, để lập mật mã cho x trước hết ta chọn thêm một số ngẫu nhiên k $(0 \le k \le |G|)$ rồi tính:

$$e_{K'}(x,k) = (y_1, y_2), \quad \text{với} \quad \begin{cases} y_1 = \alpha^k \\ y_2 = x.\beta^k \end{cases}$$

Với mọi số ngẫu nhiên k bất kỳ, ta đều xem $e_{K'}(x,k)$ là mật mã của x. Và thuật toán giải mã được xác định bởi

$$d_{K''}(y_1, y_2) = y_2.(y_1^a)^{-1} \bmod p.$$

Phép nhân trong các biểu thức nói trên đều là phép nhân của G.

Có hai lớp nhóm thường được sử dụng để xây dựng các hệ mật mã tương tự ElGamal là nhóm nhân của trường Galois GF(p^n) và nhóm cộng của một đường cong elliptic xác định trên một trường hữu hạn.

1. <u>*Nhóm nhân của trường Galois GF(p^n)*</u> : Trường Galois GF(p^n) là trường của các đa thức với hệ số trong Z_p lấy theo môđuyn là một đa thức bậc n bất khả qui; với phép cộng và phép nhân

là phép cộng và phép nhân đa thức theo môđuyn đó. Trường có p^n phần tử, có thể xem mỗi phần tử là một đa thức bậc n -1 với hệ số thuộc Z_p = {0,1,2,...,p -1}, thậm chí là một vectơ n chiều mà các thành phần là các hệ số của đa thức đó. Tập tất cả các đa thức khác 0 lập thành nhóm nhân của trường GF (p^n),và người ta chứng minh được rằng nhóm nhân đó là cyclic.

Như vậy, nhóm $G = GF(p^n)\setminus\{0\}$ là nhóm cyclic cấp p^n-1. ta có thể chọn một phần tử nguyên thuỷ của nhóm đó, và thiết lập bài toán lôgarit rời rạc tương ứng, từ đó xây dựng được hệ mật mã tương tự ElGamal.

2. <u>*Nhóm cộng của đường cong elliptic*</u> : Giả sử p là một số nguyên tố > 3. *Đường cong elliptic* $y^2=x^3+a.x+b$ *trên* Z_p **,** trong đó $a,b \in Z_p$ là các hằng số thoả mãn $4a^3+27b^2 \not\equiv 0 \pmod p$, được định nghĩa là tập hợp tất cả các điểm $(x,y)\in Z_p \times Z_p$ thoả mãn phương trình

$$y^2 \equiv x^3+a.x+b \pmod p,$$

cùng với một phần tử đặc biệt mà ta ký hiệu là $\mathcal{O}$. Tập hợp đó được ký hiệu là E. Trên tập E ta xác định một phép cộng như sau : Giả sử $P =(x_1, y_1)$ và $Q = (x_2, y_2)$ là hai điểm của E. Nếu $x_1=x_2$ và $y_1= -y_2$ thì ta định nghĩa $P +Q =\mathcal{O}$; nếu không thì $P +Q = (x_3, y_3)$, trong đó

$$x_3 = \lambda^2-x_1-x_2 , \quad y_3 = \lambda (x_1-x_3) - y_1 ,$$

với

$$\lambda=\begin{cases}(y_2-y_1)/(x_2-x_1), & khi\ P\neq Q;\\ (3x_1^2+a)/2y_1, & khi\ P=Q.\end{cases}$$

Ngoài ra, ta định nghĩa thêm : $P +\mathcal{O} = \mathcal{O}+P = P$.

Tập E với phép toán cộng đó lập thành một nhóm. Nếu $|E| =q$ là số nguyên tố thì nhóm cộng đó là nhóm cyclic, và mọi phần tử khác không ($\neq\mathcal{O}$) đều là phần tử nguyên thuỷ. Ta nhớ rằng trong trường hợp này, phần tử nghịch đảo là phần tử đối, phép nâng lên luỹ thừa n là phép nhân với số n , phép lôgarit tương ứng với một kiểu phép chia. Ta có thể xuất phát từ nhóm E này để xây dựng hệ mật mã tương tự ElGamal.