BG ChV Bài 2 Sơ đồ chữ ký ElGamal

2.1. Sơ đồ chữ ký ElGamal.

Sơ đồ chữ ký ElGamal được đề xuất năm 1985, gần như đồng thời với sơ đồ hệ mật mã ElGamal, cũng dựa trên độ khó của bài toán lôgarit rời rạc.

Sơ đồ được thiết kế đặc biệt cho mục đích ký trên các văn bản điện tử, được mô tả như một hệ

$$S = (\Pi, A, K, \Sigma, \varsigma),$$

trong đó $\Pi = Z_p^*$, $A = Z_p^* \times Z_{p-1}$, với p là một số nguyên tố sao cho bài toán tính lôgarit rời rạc trong Z_p^* là rất khó. Tập hợp K gồm các cặp khoá $K = (K', K'')$, với $K' = a$ là một số thuộc Z_p^*, $K'' = (p, \alpha, \beta)$, α là một phần tử nguyên thuỷ của Z_p^*, và $\beta = \alpha^a \bmod p$. K' là khoá bí mật dùng để ký, và K'' là khoá công khai dùng để kiểm thử chữ ký. Các thuật toán ký và kiểm thử chữ ký được xác định như sau:

Với mỗi thông báo x, để tạo chữ ký trên x ta chọn thêm môt số ngẫu nhiên $k \in Z_{p-1}^*$, rồi tính

$$sig_{K'}(\mathrm{h}(x),k) = (\gamma,\delta), \quad \text{với}$$

$$\gamma = \alpha^k \bmod p,$$

$$\delta = (h(x) - a\gamma).k^{-1} \bmod (p\text{ -1}).$$

Thuật toán kiểm thử được định nghĩa bởi:

$ver_{K''}(x,(\gamma,\delta)) =$ đúng $\Leftrightarrow \beta^{\gamma}.\gamma^{\delta} \equiv \alpha^{h(x)} (\bmod p)$.

Dễ thấy rằng sơ đồ chữ ký được định nghĩa như trên là hợp thức.

Thực vậy, nếu

$sig_{K'}(x,k) = (\gamma,\delta)$,

thì ta có :

$$\beta^{\gamma}.\gamma^{\delta} \equiv \alpha^{a\gamma}.\alpha^{k\delta} \bmod p$$

$$\equiv \alpha^{h(x)} \bmod p,$$

vì $k\delta + a\gamma \equiv h(x) \bmod(p-1)$. Do đó, $ver_{K''}(x,(\gamma,\delta)) =$ đúng.

Thí dụ: Giả sử $p = 467$, $\alpha = 2$, $a = 127$. Khi đó $\beta = 2^{127} \bmod 467 = 132$. Cho $x = 100$; ta chọn ngẫu nhiên $k = 213$ ($\in Z^*_{466}$) và được $k^{-1} \bmod 466 = 431$. Chữ ký trên văn bản $x = 100$ với số ngẫu nhiên $k = 213$ là (γ, δ), trong đó $\gamma = 2^{213} \bmod 467 = 29$ và $\delta = (100 - 127.29).431 \bmod 466 = 51$.

Để kiểm thử ta tính :

$$\beta^{\gamma}.\gamma^{\delta} = 132^{29}.29^{51} \equiv 189 \pmod{467},$$

$$\alpha^{x} = 2^{100} \equiv 189 \pmod{467},$$

hai giá trị đó đồng dư với nhau theo mod467, chữ ký(γ, δ)=(29,51) được xác nhận là đúng.

Bài tập

Lấy p và q đã cho trong hệ mật RSA.

ALICE : p_1 =127, tìm α_1 , chọn a=61, Tính β_1=. Công bố khóa công khai.

BOB : p_2 =149, tìm α_2, chọn a_2=97, Tính β_2= . Công bố khóa công khai.

Bước 1. ALICE gửi bản tin x=101, và ký trên x.

Số ngẫu nhiên k_1=22 để mã hóa và số k_2=83 để ký.

Bản mã:

Chữ ký :

Bước 2. BOB nhận được bản mã và chữ ký, tiến hành giải mã và xác thực chữ ký.

Bài kiểm tra

Với p đã cho, hãy :

1. Xác định phần tử nguyên thủy α của Z_p^*;
2. Xây dựng hệ mật ElGamal với a = 1010.
3. Hai sv ghép thành 1 cặp để nhận và gửi bản mã, ký trên bản tin x=số hóa 3 chữ cái đầu tên của sinh viên.
   Với $k_{mã\ hóa}$=853, $k_{ký}$ = 467.
   Mỗi sinh viên vừa mã hóa, gửi tin, ký trên bản tin và nhận tin, giải mã, xác thực chữ ký.

4.2.2. Tính an toàn của sơ đồ chữ ký ElGamal.

Sơ đồ chữ ký ElGamal được xem là an toàn, nếu việc ký trên một văn bản là không thể giả mạo được, nói cách khác, không thể có một người nào ngoài chủ thể hợp pháp có thể giả mạo chữ ký của chủ thể hợp pháp đó trên một văn bản bất kỳ. Vì vậy, việc giữ bí mật khoá $K' = a$ dùng để tạo chữ ký là có ý nghĩa quyết định đối với việc bảo đảm tính an toàn của chữ ký. Có thể để lộ khoá bí mật $K' = a$ trong những trường hợp nào, và có thể không để lộ $K' = a$

mà vẫn giả mạo chữ ký được không? Ta sẽ xét sau đây một vài trường hợp đơn giản :

1) *Khả năng để lộ khoá* $K' = a$: Cũng như đối với sơ đồ hệ mật mã ElGamal, khoá bí mật a có thể bị phát hiện trong trường hợp để lộ số ngẫu nhiên k ở một lần ký nào đó, hoặc sử dụng cùng một số ngẫu nhiên k ở hai lần ký khác nhau.

Nếu số ngẫu nhiên k được sử dụng khi ký trên văn bản x bị lộ, thì khoá bí mật $K' = a$ được tính theo công thức sau đây:

$$a = (x - k\delta).\ \gamma^{-1} \bmod (p - 1).$$

Bây giờ ta xét trường hợp dùng cùng một số ngẫu nhiên k cho hai lần ký khác nhau, chẳng hạn cho x_1 và x_2. Khi đó ta có chữ ký trên x_1 là (γ, δ_1), trên x_2 là (γ, δ_2), với thành phần thứ nhất bằng nhau (và bằng $\gamma = \alpha^k \bmod p$), và các chữ ký đó thoả mãn

$$\beta^{\gamma}.\gamma^{\delta_1} \equiv \alpha^{x_1} (\bmod p),$$

$$\beta^{\gamma}.\gamma^{\delta_2} \equiv \alpha^{x_2} (\bmod p).$$

Từ đó ta có

$$\alpha^{x_1 - x_2} \equiv \gamma^{\delta_1 - \delta_2} \equiv \alpha^{k(\delta_1 - \delta_2)} (\bmod p),$$

điều đó tương đương với

$x_1 - x_2 \equiv k(\delta_1 - \delta_2) \pmod{(p-1)}$.

Đặt $d = \gcd(\delta_1 - \delta_2, p - 1)$. Cả ba số $\delta_1 - \delta_2$, $p - 1$ và $x_1 - x_2$ đều chia hết cho d, ta đặt

$$x' = \frac{x_1 - x_2}{d}\ ,\ \delta' = \frac{\delta_1 - \delta_2}{d}\ ,\ p' = \frac{p-1}{d}.$$

Khi đó đồng dư thức ở trên trở thành

$$x' \equiv k.\delta' \pmod{p'}.$$

Vì $\gcd(\delta', p') = 1$, nên có thể tính $\varepsilon = \delta'^{-1} \bmod p'$, và sau đó giá trị k theo mod p':

$k = x'.\varepsilon \bmod p'$, tức là

$k = x'.\varepsilon + i.p' \bmod (p - 1)$

với i là một giá trị nào đó, $0 \leq i \leq d - 1$. Thử lần lượt điều kiện

$$\gamma = \alpha^k \bmod p$$

với các giá trị đó của i , ta sẽ tìm được k ;sau đó từ k tính được a cần tìm.

2) *Khả năng giả mạo chữ ký trên một văn bản cho trước* :

Giả sử chủ thể A chọn sơ đồ chữ ký ElGamal với cặp khoá K =(K’,K''), trrong đó $K' = a$ là khoá bí mật. Một người ngoài O không biết khoá bí mật $K' = a$ mà muốn giả mạo chữ ký của A trên một văn bản x thì phải có khả năng tạo ra được chữ ký (γ,δ) mà không cần biết a. Có hai cách : hoặc chọn trước γ rồi tìm δ tương ứng, hoặc ngược

lại, chọn trước δ rồi tìm γ tương ứng.

Nếu chọn trước γ rồi tìm δ, thì δ phải là

$$\delta = (x - a\gamma)k^{-1} \bmod (p-1)$$

$$= ((x - a\gamma)\log_{\gamma} \alpha \bmod (p-1)$$

$$= \log_{\alpha}(\alpha^{x}\beta^{-\gamma}).\log_{\gamma}\alpha = \log_{\gamma}\alpha^{x}\beta^{-\gamma} \bmod (p-1);$$

đó là một bài toán tính lôgarit rời rạc, mà ta biết rằng rất khó.

Nếu chọn trước δ rồi tìm γ thì phải giải phương trình

$$\beta^{\gamma}.\gamma^{\delta} \equiv \alpha^{x} \bmod p$$

với ẩn số γ. Ta chưa biết có cách giải hữu hiệu nào không,

nhưng chắc là không dễ hơn bài toán tính lôgarit rời rạc.

Như vậy, ta có thể tin rằng khả năng giả mạo chữ ký trên một văn bản cho trước khi không biết khoá bí mật $K' = a$ là rất ít, do đó không có ảnh hưởng đáng kể đến tính an toàn của sơ đồ chữ ký.

3)*Giả mạo chữ ký cùng với văn bản được ký* :

Có một khả năng giả mạo khác là giả mạo cả văn bản gửi đi *x* cùng với chữ ký (γ,δ) trên *x*. Khả năng đó xẩy ra khi kẻ giả mạo chọn được *x* và (γ,δ) thoả mãn điều kiện kiểm thử, cụ thể

khi chọn được x, γ, δ có dạng sau đây :

$$\gamma = \alpha^i . \beta^j \bmod p,$$

$$\delta = -\gamma . j^{-1} \bmod (p-1),$$

$$x = -\gamma . i . j^{-1} \bmod (p-1),$$

trong đó i, j là các số nguyên sao cho $0 \le i, j \le p-2$, $\gcd(j, p-1) = 1$, và j^{-1} được tính theo $\bmod(p-1)$. Thực vậy, khi đó ta có

$$\begin{aligned} \beta^\gamma . \gamma^\delta &\equiv \beta^\gamma (\alpha^i \beta^j)^{-\gamma . j^{-1}} \bmod p \\ &\equiv \beta^\gamma . \alpha^{-i\gamma j^{-1}} . \beta^{-\gamma} \bmod p \\ &\equiv \alpha^x \bmod p , \end{aligned}$$

tức điều kiện kiểm thử được thoả mãn, (γ, δ) có thể được xác nhận hợp thức là chữ ký trên x.

Có thể có một cách giả mạo khác nữa, nếu kẻ giả mạo sử dụng chữ ký đúng (γ,δ) trên một văn bản *x* có từ trước để tạo ra một chữ ký (λ,μ) mới cho một văn bản "mới" x' như sau:

$$\lambda=\gamma^h.\alpha^i.\beta^j \bmod p,$$

$$\mu=\delta\lambda(h\gamma-j\delta)^{-1} \bmod(p-1),$$

$$x'=\lambda(hx+i\delta)(h\gamma-j\delta)^{-1} \bmod(p-1).$$

Có thể thử lại rằng điều kiện kiểm thử đúng đối với "chữ ký" (λ,μ) và "văn bản" x' , tức là

$$\beta^{\lambda}.\lambda^{\mu}\equiv\alpha^{x'} \bmod p.$$

Cả hai cách giả mạo nói trên đều cho chữ ký thoả mãn điều kiện kiểm thử đối với văn bản tương ứng, tuy nhiên văn bản

đó không phải là văn bản được chọn theo ý muốn của người giả mạo, cho nên khả năng sử dụng các cách giả mạo đó trong thực tế cũng không có giá trị , do đó không thể gây nguy hại đáng kể cho tính an toàn của sơ đồ chữ ký nói chung.

4.2.3. Chuẩn chữ ký số (Digital Signature Standard).

Chuẩn chữ ký số (DSS) được đề xuất từ năm 1991 và được chấp nhận vào cuối năm 1994 để sử dụng trong một số lĩnh vực giao dịch điện tử tại Hoa kỳ. DSS dựa vào sơ đồ chữ ký

ElGamal, với một vài sửa đổi. Để bảo đảm an toàn , số nguyên tố p cần phải đủ lớn, biểu diễn nhị phân của p phải có từ 512 bit trở lên (cụ thể từ 512 đến 1024 bit, số bit là một bội của 64). Tuy nhiên, độ dài chữ ký theo sơ đồ ElGamal là gấp đôi số bit của p, mà trong nhiều ứng dụng người ta lại mong muốn có chữ ký độ dài ngắn, nên giải pháp sửa đổi được đề xuất là: trong khi vẫn dùng p lớn với độ dài biểu diễn 512 bit trở lên, thì sẽ hạn chế độ dài của γ và δ trong chữ ký (γ,δ) vào khoảng 160 bit (như vậy cả chữ ký sẽ có

độ dài khoảng 320 bit); điều này được thực hiện bằng cách dùng một nhóm con cyclic Z_q^* của Z_p^* thay cho chính bản thân Z_p^*, do đó mọi tính toán vẫn được thực hiện như trong Z_p^* nhưng các dữ liệu và thành phần chữ ký lại thuộc Z_q^*. Ta được *sơ đồ chuẩn chữ ký số DSS* như mô tả sau đây:

Chọn p là một số nguyên tố lớn có độ dài biểu diễn ≥ 512 bit sao cho bài toán tính logarit rời rạc trong Z_p là khó, q là một ước số nguyên tố của p -1, có độ dài biểu diễn cỡ 160 bit. Gọi $\alpha \in Z_p^*$

là một căn bậc q của 1 theo mod$p$.

Đặt $\Pi = Z_p^*$, A $= Z_q^* \times Z_q^*$. Chọn $a \in Z_q^*$ và tính $\beta \equiv \alpha^a \bmod p$. Xác định khoá K =(K’,K''), trong đó khoá bí mật K’ = a, và khoá công khai K'' = (p,q,α,β). Thuật toán ký và thuật toán kiểm thử được định nghĩa như sau: Với $x \in \Pi = Z_p^*$, ta chọn thêm một số ngẫu nhiên k (0≤k ≤ q -1), và định nghĩa chữ ký

$sig_{K'}(x,k) = (\gamma,\delta)$, trong đó $\gamma = (\alpha^k \bmod p) \bmod q$,

$\delta = (x + a\gamma).k^{-1} \bmod q$.

Thuật toán kiểm thử được định nghĩa bởi:

$ver_{K''}(x,(\gamma,\delta)) =$ đúng $\Leftrightarrow (\alpha^{e_1}.\beta^{e_2} \bmod p) \bmod q = \gamma$,
trong đó $e_1 = x.\delta^{-1} \bmod q$ và $e_2 = \gamma.\delta^{-1} \bmod q$.
Chú ý rằng ta phải có $\delta \neq 0 \bmod q$ để có thể tính được $\delta^{-1} \bmod q$ dùng trong thuật toán kiểm thử, vì vậy nếu chọn k mà được $\delta \equiv 0 \bmod q$ thì phải chọn lại số k khác để có được $\delta \neq 0 \bmod q$.