Bài 4.1 Sơ đồ chữ ký RSA

1. Định nghĩa sơ đồ chữ ký.

Định nghĩa 4.1. Một *sơ đồ chữ ký* S là một bộ năm

$$S = (\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V}),$$

trong đó: $\mathcal{P}$ là một tập hữu hạn các thông báo có thể có,

$\mathcal{A}$ là một tập hữu hạn các chữ ký có thể có,

$\mathcal{K}$ là một tập hữu hạn các khoá, mỗi khoá $K \in \mathcal{K}$ gồm có hai phần $K=(K',K'')$, K' là khoá bí mật dành cho việc ký, còn K''

là khoá công khai dành cho việc kiểm thử chữ ký.

Với mỗi $K=(K',K'')$, trong $\mathcal{S}$ có một *thuật toán ký*

$$sig_{K'}:\mathcal{P}\rightarrow\mathcal{A},$$

và trong $\mathcal{V}$ có một *thuật toán kiểm thử*

$$ver_{K''}:\mathcal{P}\times\mathcal{A}\rightarrow\{\text{đúng,sai}\}$$

thoả mãn điều kiện sau đây đối với mọi thông báo $x\in\mathcal{P}$ và mọi chữ ký $y\in\mathcal{A}$: $ver_{K''}(x,y)=$ đúng $\Leftrightarrow\ y=sig_{K'}(x)$.

Với sơ đồ trên, mỗi chủ thể sở hữu một bộ khoá $K=(K',K'')$, công bố công khai khoá K'' để

mọi người có thể kiểm thử chữ ký của mình, và giữ bí mật khoá K' để thực hiện chữ ký trên các thông báo mà mình muốn gửi đi. Các hàm $ver_{K''}$ và $sig_{K'}$ (khi biết K') phải tính được một cách dễ dàng (trong thời gian đa thức), tuy nhiên hàm $y = sig_{K'}(x)$ là khó tính được nếu không biết K' - điều đó bảo đảm bí mật cho việc ký, cũng tức là bảo đảm chống giả mạo chữ ký.

Bài toán xác nhận với chữ ký điện tử, theo một nghĩa nào đó, có thể xem là ô đối ngẫu với bài toán bảo mật bằng mật mã, như được minh hoạ bởi thí dụ sơ đồ

chữ ký RSA, đối ngẫu với sơ đồ mật mã RSA, dưới đây :

2. Sơ đồ chữ ký RSA.

Sơ đồ chữ ký RSA được cho bởi bộ năm

$$S = (\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V}),$$

trong đó $\mathcal{P} = \mathcal{A} = Z_n$, với $n = p.q$ là tích của hai số nguyên tố lớn p,q, $\mathcal{K}$ là tập các cặp khoá $K = (K', K'')$, với $K' = a$ và $K'' = (n,b)$, a và b là hai số thuộc Z_n^* thoả mãn $a.b \equiv 1 (\mathrm{mod}\, \phi(n))$. Các hàm $sig_{K'}$ và $ver_{K''}$ được xác định như sau:

$$sig_{K'}(x) = (\mathrm{h}(x))^a \,\mathrm{mod} n = \mathrm{y},$$

$ver_{K''}(x,y) = \text{đúng} \Leftrightarrow \text{h}(x) \equiv y^b \pmod{n}$.

Dễ chứng minh được rằng sơ đồ được định nghĩa như vậy là hợp thức, tức là với mọi $x \in \mathcal{P}$ và mọi chữ ký $y \in \mathcal{A}$: $ver_{K''}(x, y) =$ đúng $\Leftrightarrow$ $y = sig_{K'}(x)$.

Chú ý rằng tuy hai vấn đề xác nhận và bảo mật theo sơ đồ RSA là có bề ngoài giống nhau, nhưng nội dung của chúng là hoàn toàn khác nhau:

Khi A gửi thông báo x cho B, để B có căn cứ xác nhận đó đúng thực là thông báo do A gửi, A phải gửi kèm theo chữ ký $sig_{K'}(x)$, tức là A gửi cho B (x,

$sig_{K'}(x)$), trong các thông tin gửi đi đó, ***thông báo x được mã hóa bằng khóa công khai của người nhận, chữ ký được tạo bởi khóa bí mật của người gửi.***

Cũng tương tự như vậy, nếu dùng sơ đồ mật mã RSA, khi một chủ thể A nhận được một bản mật mã $e_{K'}(x)$ từ B thì A chỉ biết rằng thông báo *x* được bảo mật, chứ không có gì để xác nhận *x* là của B.

Nếu ta muốn hệ truyền tin của ta vừa có tính bảo mật vừa có tính xác thực, thì ta phải sử dụng đồng thời cả hai hệ mật

mã hóa và xác nhận (bằng chữ ký).

Giả sử trên mạng truyền tin công cộng, ta có cả hai hệ mật mã khoá công khai S_1 và hệ xác nhận bằng chữ ký S_2. Giả sử B có bộ khoá mật mã $K = (K', K'')$ với $K' = (n, e)$ và $K'' = d$ trong hệ S_1, và A có bộ khoá chữ ký $K_s = (K_s', K_s'')$ với $K_s' = a$ và $K_s'' = (n, b)$ trong hệ S_2. A có thể gửi đến B một thông báo vừa bảo mật vừa có chữ ký để xác nhận như sau: A ký trên thông báo x trước, rồi thay cho việc gửi đến B văn bản cùng chữ ký $(x, sig_{K_s'}(x))$ thì A sẽ gửi cho B bản mật mã của văn

bản đó được lập theo khoá công khai của B, tức là gửi cho B $e_{K'}$ $((x, sig_{K'_s}(x))$.

Nhận được văn bản mật mã đó B sẽ dùng thuật toán giải mã $d_{K''}$ của mình để thu được $(x, sig_{K'_s}(x))$, sau đó dùng thuật toán kiểm thử chữ ký công khai $ver_{K''_s}$ của A để xác nhận chữ ký $sig_{K'_s}(x)$ đúng là của A trên x.

Ví dụ :

ALICE : Người gửi tin

p_s= 23, q_s = 29, a= 127, b= ?

Bản tin : BINH=

BOB: p=19, q=37, e= 149, d= ?

Hệ mật 1. ALICE

n = 29*37, a_1 =467, tính b_1 = 395

Hệ mật 2. BOB

n = 23*43, a_2 = 583, tính b_2 = 835

Bước 1. ALICE mã hóa bản tin x = 20 bằng khóa công khai (n_2, b_2) của BOB và ký trên x bằng khóa bí mật (n_1, a_1) và gửi cho đối tác:

Bản mã : $x^{b2} \mod n_2$ =

Chữ ký : $x^{a1} \mod n_1$ =

Bước 2. BOB sau nhận được bản mã và chữ ký của ALICE

thì tiến hành giải mã và xác thực chữ ký.