CHƯƠNG 8 - SƠ ĐỒ CHỮ KÝ

Ngày 13 tháng 10 năm 2023

Trong chương này, ta sẽ tìm hiểu về các sơ đồ chữ ký, hay còn được gọi là các chữ ký số. Ta sẽ bao hàm các sơ đồ chữ ký dựa trên các vấn đề về phân tích nhân tử và giải thuật rời rạc, bao gồm cả tiêu chuẩn về chữ ký số (Digital Signature Standard)

8.1 Giới thiệu

Chữ ký viết tay "thông thường" đính kèm vào tài liệu được sử dụng để chỉ định người chịu trách nhiệm về nó. Chữ ký được sử dụng trong các tình huống hàng ngày như viết thư, rút tiền ngân hàng, ký hợp đồng, v.v.

Sơ đồ chữ ký là phương pháp ký một thông điệp được lưu trữ dưới dạng điện tử. Như vậy, một tin nhắn đã ký có thể được truyền qua mạng máy tính. Trong chương này, chúng ta sẽ nghiên cứu một số các sơ đồ chữ ký phổ biến, tuy nhiên trước đó ta sẽ thảo luận về một số khác biệt cơ bản giữa chữ ký thông thường và chữ ký số.

Đầu tiên là vấn đề ký một văn bản. Với chữ ký thông thường, chữ ký là một phần của tài liệu vật lý được ký. Tuy nhiên, chữ ký điện tử không được gắn vật lý vào tin nhắn được ký, vì vậy thuật toán được sử dụng phải bằng cách nào đó "che giấu" chữ ký với bản tin.

Thứ hai là vấn đề xác minh. Chữ ký thông thường được xác minh bằng cách so sánh nó với các chữ ký xác thực khác. Ví dụ: nếu ai đó ký để mua hàng bằng thẻ tín dụng (ngày nay không còn phổ biến do sự phổ biến của công nghệ chip-pin), nhân viên bán hàng phải so sánh chữ ký trên phiếu bán hàng với chữ ký ở mặt sau của thẻ tín dụng để xác minh chữ ký. Tất nhiên, đây không phải là một phương pháp an toàn vì việc giả mạo chữ ký của người khác là không khó. Mặt khác, chữ ký số có thể được xác minh bằng thuật toán xác minh được biết đến rộng rãi. Vì vậy, "bất kỳ ai" cũng có thể xác minh chữ ký số. Việc sử dụng sơ đồ chữ ký vì thế sẽ ngăn ngừa khả năng giả mạo.

Một điểm khác biệt cơ bản giữa chữ ký thông thường và chữ ký số là "bản sao" của tin nhắn kỹ thuật số được ký giống hệt với bản gốc. Trong khi đó, bản sao của tài liệu giấy đã được ký thường có thể được phân biệt với bản gốc. Tính năng này có nghĩa rằng, chúng ta sẽ phải cẩn thận để tránh việc sử dụng lại bản tin kỹ thuật số đã ký. Ví dụ: nếu Alice ký một tin nhắn kỹ thuật số cho phép Bob rút 100 đô la từ tài khoản ngân hàng của cô ấy, cô ấy muốn Bob chỉ có thể làm như vậy một lần. Vì vậy, bản thân tin nhắn phải chứa thông tin, chẳng hạn như ngày tháng, để ngăn không cho nó được sử dụng lại.

Một sơ đồ chữ ký bao gồm hai thành phần: thuật toán mã hoá và thuật toán giải mã. Alice có thể mã hoá một bản tin x bằng thuật toán ký (riêng tư) sig_K phụ thuộc vào khóa riêng K. Chữ ký kết quả $sig_K(x)$ sau đó có thể được xác minh bằng thuật toán giải mã công khai verK. Cho một cặp (x, y), trong đó x là một bản tin và y là chữ ký có mục đích trên x, thuật toán xác minh trả về câu trả lời đúng hay sai tùy thuộc vào việc y có phải là chữ ký hợp lệ cho thông báo x hay không.

Dưới đây là định nghĩa đầy đủ về một sơ đồ chữ ký

Định nghĩa 8.1: Một số đồ chữ ký là một bộ năm (P, C, K, E, D), với các điều kiện sau:

- P là không gian bản tin
- C là không gian các chữ ký
- K là không gian khoá, gồm danh sách các khoá có thể sử dụng
- Với mỗi khoá $k \in K$, sẽ có một hàm mã hoá $sig_K \in E$, tương ứng với đó là một hàm giải mã $ver_K \in D$. Mọi bản tin x và mọi chữ ký y đều phải thoả mãn:

$$ver_K(x, y) = \begin{cases} true & \text{if } \ y = sig_K(x) \\ false & \text{if } \ y \neq sig_K(x) \end{cases}$$

Một cặp (x, y) với $x \in P$ và $y \in C$ được gọi là một bản tin được mã hoá (signed message)

Với mọi $k \in K$, các hàm sig_K và ver_K phải là các hàm thời gian đa thức (polynomial-time functions). Thuật toán xác minh ver_K sẽ được công khai và thuật toán ký sig_K sẽ ở chế độ riêng tư. Với một thông báo x, không ai khác ngoài Alice có thể tính toán chữ ký y sao cho $ver_K(x, y) = true$ (và lưu ý rằng có thể có nhiều hơn một y như vậy cho một x cho trước, tùy thuộc vào cách thức chức năng ver được xác định). Nếu Oscar có thể tính toán một cặp (x, y) sao cho $ver_K(x, y) = true$ và x chưa được ký bởi Alice trước đó thì chữ ký y được gọi là giả mạo. Một cách không chính thức, chữ ký giả mạo là chữ ký hợp lệ được tạo bởi người khác không phải Alice.

8.1.1 Sơ đồ chữ ký RSA

Đây là ví dụ đầu tiên mà ta sẽ tìm hiểu, quan sát xem hệ mật RSA được sử dụng để cung cấp chữ ký số như thế nào. Dưới đây là định nghĩa của hệ mật RSA

Cho $n = pq$, với p và q là hai số nguyên tố đủ lớn. Xét $P = A = Z_n$, ta có định nghĩa

$$K = \{(n, p, q, a, b) : n = pq, ab \equiv 1(mod\phi(n))\} \quad (1)$$

Ta có n và b là khoá công khai, còn p, q, và a là khoá bí mật

Với $K = (n, p, q, a, b)$, ta định nghĩa hàm mã hoá như sau

$$sig_K(x) = x^a mod n \quad (2)$$

và hàm giải mã có dạng như sau

$$ver_K(x, y) = true \Leftrightarrow x \equiv y^b(mod n) \quad (3)$$

Với $x, y \in Z_n$

Lấy ví dụ, Alice tiến hành mã hoá một tin nhắn x bằng cách sử dụng hàm giải mã RSA e_K. Alice là người duy nhất có thể tạo chữ ký vì $e_K = sig_K$ là khoá bí mật. Thuật toán giả mã sử dụng quy tắc giải hóa RSA d_K. Bất kỳ ai cũng có thể giải mã được chữ ký vì d_K được công khai.

Lưu ý rằng bất kỳ ai cũng có thể giả mạo chữ ký RSA của Alice bằng cách chọn ngẫu nhiên y và tính $x = e_K(y)$; thì $y = sig_K(x)$ là chữ ký hợp lệ trên thông điệp x. (Tuy nhiên, lưu ý rằng dường như không có cách rõ ràng nào để chọn x trước rồi tính chữ ký y tương ứng; nếu điều này có thể thực hiện được thì Hệ thống mật mã RSA sẽ không an toàn.) Một cách để ngăn chặn những cuộc tấn công này là yêu cầu các tin nhắn chứa đủ độ dư thừa để chữ ký giả mạo này không tương ứng với tin nhắn x "có ý nghĩa", ngoại trừ với một xác suất rất nhỏ. Ngoài ra, việc sử dụng hàm băm kết hợp với sơ đồ chữ ký sẽ loại bỏ phương pháp giả mạo này (hàm băm mật mã đã được thảo luận trong Chương 5). Ta sẽ tìm hiểu kĩ về cách tiếp cận này trong phần tiếp theo.

Phần còn lại của chương 8 bao gồm như sau: Phần 8.2 giới thiệu khái niệm về bảo mật cho sơ đồ chữ ký và cách sử dụng hàm băm cùng với sơ đồ chữ ký. Phần 8.3 trình bày về Sơ đồ chữ ký ElGamal và thảo luận về tính bảo mật của nó. Phần 8.4 sẽ đề cập đến ba sơ đồ chữ ký quan trọng được phát triển từ hệ mật ElGamal, cụ thể là sơ đồ chữ ký Schnorr, thuật toán chữ ký số và thuật toán chữ ký số đường cong Elliptic. Sơ đồ chữ ký có độ an toàn có thể chứng minh được gọi là Full Domain Hash là nội dung của Phần 8.5 và các chứng chỉ sẽ được thảo luận trong Phần 8.6. Cuối cùng, một số phương pháp kết hợp sơ đồ chữ ký với sơ đồ mã hóa sẽ được thảo luận và xem xét trong Phần 8.7.

8.2 Yêu cầu về bảo mật cho các sơ đồ chữ ký

Ở phần này, ta sẽ thảo luận về việc một hệ mật như thế nào thì được coi là bảo mật. Ta sẽ cần phải chị định mô hình tấn công, mục đích của kẻ tấn công, và dạng bảo mật được cung cấp bởi sơ đồ chữ ký.

Nhắc lại một chút ở phần 2.2, một mô hình tấn công sẽ được thực hiện dựa theo những thông tin công khai. Đối với trường hợp của sơ đồ chữ ký, các dạng tấn công phổ biến bao gồm:

Tấn công chỉ bằng khoá công khai

Ví dụ, Oscar có được khoá hay chữ ký công khai của Alice thông qua hàm giải mã e_K hay ver_K

Tấn công bằng bản tin đã biết

Ví dụ, Oscar đã có được danh sách một số bản tin trước đã được Alice mã hoá như là

$$(x_1, y_1), (x_2, y_2), ...,$$

Tấn công với các bản tin được chọn trước

Ví dụ, Oscar yêu cầu các chữ ký của Alice đối với danh sách một số bản tin nhất định. Từ đó, anh ấy sẽ chọn các bản tin $x_1, x_2, ...$, và Alice sẽ cung cấp các chữ ký của cô ấy lần lượt là $y_i = sig_K(x_i), i = 1, 2, ...$

Ta sẽ xem xét một vài mục đích của việc tấn công

Bẻ khoá toàn bộ (total broken)

Oscar có thể xác định được khoá bí mật của Alice hay là hàm mã hoá sig_K. Từ đó anh ấy có thể tạo ra các chữ ký khác với bất kì bản tin nào.

Giả mạo có chọn lọc (selective forgery)

Với một số xác suất không thể bỏ qua, Oscar có thể tạo một chữ ký hợp lệ trên một tin nhắn do người khác chọn. Nói cách khác, nếu Oscar nhận được một bản tin x thì anh ta có thể xác định (với xác suất nào đó) chữ ký y sao cho $ver_K(x, y) = true$. Tin nhắn x không được là tin nhắn đã được Alice ký trước đó.

Giả mạo hiện sinh (existential forgery)

Oscar có thể tạo chữ ký hợp lệ cho ít nhất một tin nhắn. Nói cách khác, Oscar có thể tạo một cặp (x, y), trong đó x là một thông điệp và $ver_K(x, y) =$

true, còn bản tin x không phải là bản tin đã được Alice ký trước đó.

Một sơ đồ chữ ký sẽ không thể có đủ độ bảo mật, nếu như Oscar có thể kiểm tra một chữ ký khả dụng $y \in A$ với một bản tin x được cho trước bằng cách sử dụng hàm giải mà ver_K, cho đến khi anh ấy tìm ra một chữ ký có nghĩa. Vậy với khoảng thời gian đủ lâu thì Oscar sẽ luôn tìm ra được chữ ký của Alice cho mọi bản tin. Vì thế, với các hệ mật có khoá công khai, mục tiêu của chúng ta sẽ là tìm ra các sơ dồ chữ ký có khả năng tính toán lớn và đảm bảo về bảo mật.

Lưu ý rằng các định nghĩa trên có một số điểm tương đồng với các cuộc tấn công vào MAC mà chúng ta đã xem xét trong Phần 5.5. Trong cài đặt MAC, không có thứ gọi là khóa chung, vì vậy sẽ không có ý nghĩa gì khi nói về một cuộc tấn công chỉ bằng khóa (và tất nhiên, MAC không có chức năng ký và xác minh riêng biệt). Các cuộc tấn công trong Phần 5.5 là các cuộc tấn công giả mạo hiện hữu bằng cách sử dụng các cuộc tấn công tin nhắn đã chọn.

Ta minh họa các khái niệm được mô tả ở trên bằng một số cuộc tấn công vào Lược đồ Chữ ký RSA. Trong Phần 8.1, chúng ta đã quan sát thấy Oscar có thể xây dựng một thông điệp được ký hợp lệ bằng cách chọn chữ ký y và sau đó tính x sao cho $ver_K(x, y) = true$. Đây sẽ là một sự giả mạo bằng cách sử dụng một cuộc tấn công chỉ bằng khóa công khai. Một kiểu tấn công khác dựa trên đặc tính nhân của RSA mà ta đã đề cập trong Phần 6.9.1. Giả sử $y_1 = sig_K(x_1)$ và $y_2 = sig_K(x_2)$ là hai thông điệp bất kỳ được Alice ký trước đó. Sau đó

$$ver_K(x_1x_2 mod n, y_1y_2 mod n) = true,$$

và do đó Oscar có thể tạo chữ ký hợp lệ $y_1y_2 \ mod n$ trên bản tin $x_1x_2 \ mod n$. Đây là một ví dụ về sự giả mạo hiện hữu bằng cách sử dụng một cuộc tấn công tin nhắn đã biết.

Sau đây là một dạng khác. Giả sử Oscar muốn giả mạo chữ ký trên tin nhắn x, trong đó x có thể đã được người khác chọn. Việc tìm $x1, x2 \in Z_n$ sao cho

$$x \equiv x_1x_2 (mod n)$$

là một vấn đề đơn giản. Bây giờ, giả sử anh ta yêu cầu Alice cho chữ ký của cô trên bản tin x_1 và x_2, chúng ta ký hiệu lần lượt là y_1 và y_2. Sau đó, như trong cuộc tấn công trước, $y_1y_2 \ mod n$ là chữ ký cho bản tin $x = x_1x_2 mod n$. Đây là hành vi giả mạo có chọn lọc bằng cách sử dụng một cuộc tấn công bằng tin nhắn đã chọn.

8.2.1 Chữ ký và hàm băm

Sơ đồ chữ ký hầu như luôn được sử dụng cùng với hàm băm mật mã (công khai) an toàn. Hàm băm $h : \{0, 1\}^* \to Z$ sẽ nhận một thông báo có độ dài tùy ý và tạo ra một bản tóm tắt thông báo có kích thước xác định (224 bit là lựa chọn phổ biến). Sau đó, bản tóm tắt thông điệp sẽ được ký bằng sơ đồ chữ ký (P, C, K, S, V), trong đó $Z \subseteq P$. Việc sử dụng hàm băm và sơ đồ chữ ký này

được mô tả dưới dạng sơ đồ trong Hình 8.1.

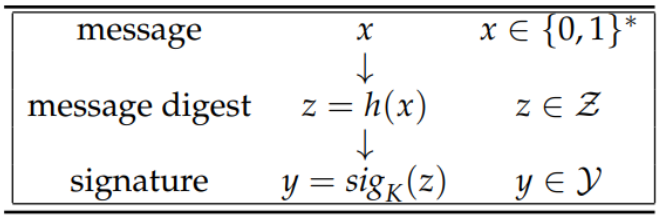

FIGURE 8.1: Signing a message digest

Giả sử Alice muốn ký một tin nhắn x, là một chuỗi bit có độ dài tùy ý. Đầu tiên cô ấy xây dựng bản tóm tắt thông điệp $z = h(x)$, sau đó tính chữ ký trên z, cụ thể là $y = sig_K(z)$. Sau đó cô ấy truyền cặp thứ tự (x, y) qua kênh. Bây giờ, việc xác minh có thể được thực hiện (bởi bất kỳ ai) bằng cách trước tiên xây dựng lại bản tóm tắt thông báo $z = h(x)$ bằng cách sử dụng hàm băm công khai h, sau đó kiểm tra xem $ver_K(z, y) = true$.

Ta sẽ phải cẩn thận rằng việc sử dụng hàm băm h không làm suy yếu tính bảo mật của sơ đồ chữ ký, vì đó là bản tóm tắt thông điệp được ký chứ không phải thông điệp. h sẽ cần phải đáp ứng một số đặc tính nhất định để ngăn chặn các cuộc tấn công khác nhau. Các thuộc tính mong muốn của hàm băm là những thuộc tính đã được thảo luận trong Phần 5.2.

Kiểu tấn công rõ ràng nhất là Oscar bắt đầu bằng một tin nhắn được ký hợp lệ (x, y), trong đó $y = sig_K(h(x))$ (Cặp (x, y) có thể là bất kỳ thông điệp nào được Alice ký trước đó.). Sau đó, anh ta tính $z = h(x)$ và cố gắng tìm $x' \neq x$ sao cho $h(x') = h(x)$. Nếu Oscar có thể làm điều này, (x', y) sẽ là một tin nhắn được ký hợp lệ, vì vậy y là chữ ký giả mạo cho tin nhắn x' . Đây là một sự giả mạo hiện hữu bằng cách sử dụng một cuộc tấn công tin nhắn đã biết. Để ngăn chặn kiểu tấn công này, ta yêu cầu h phải có khả năng chống lại hình ảnh thứ hai.

Một cuộc tấn công khác có thể xảy ra như sau: Đầu tiên Oscar tìm thấy hai tin nhắn $x \neq x'$ sao cho $h(x) = h(x')$. Sau đó, Oscar đưa x cho Alice và thuyết phục cô ký vào bản tóm tắt thông điệp $h(x)$, thu được y. Khi đó (x', y) là một tin nhắn được ký hợp lệ và y là chữ ký giả mạo cho tin nhắn x.

Đây là một hành vi giả mạo hiện sinh bằng cách sử dụng một cuộc tấn công tin nhắn đã chọn; nó có thể được ngăn chặn nếu h có khả năng chống va chạm. Đây là kiểu tấn công thứ ba. Thông thường, với một số lược đồ chữ ký nhất định, có thể giả mạo chữ ký trên các bản tóm tắt thông báo ngẫu nhiên z (ta đã quan sát thấy rằng điều này có thể được thực hiện với sơ đồ chữ ký RSA). Nghĩa là, giả định rằng sơ đồ chữ ký (không có hàm băm) có thể bị giả mạo

bằng cách sử dụng một cuộc tấn công chỉ bằng khóa công khai. Bây giờ, giả sử Oscar tính toán một chữ ký trên bản tóm tắt thông điệp z nào đó, và sau đó anh ta tìm thấy một thông điệp x sao cho $z = h(x)$. Nếu anh ta có thể làm điều này thì (x, y) là một thông điệp được ký hợp lệ và y là một chữ ký giả mạo cho thông điệp x. Đây là một sự giả mạo tồn tại trong sơ đồ chữ ký bằng cách sử dụng một cuộc tấn công chỉ bằng khóa. Để ngăn chặn cuộc tấn công này, chúng tôi mong muốn h là hàm băm kháng tiền ảnh.