Chương I: Tổng quan về chữ ký số

2.1. Chữ ký số.

2.1.1. Giới thiệu về chữ số

Trong cuộc sống hàng ngày, ta cần dùng chữ ký để xác nhận các văn bản tài liệu nào đó và có thể dùng con dấu với giá trị pháp lý cao hơn đi kèm với chữ ký.

Cùng với sự phát triển nhanh chóng của công nghệ thông tin, các văn bản tài liệu dưới dạng số, dễ dàng được sao chép, sửa đổi. Nếu ta sử dụng hình thức chữ ký truền thống như trên sẽ rất dễ dàng bị giả mạo chữ ký. Vậy làm sao để có thể ký vào văn bản, tài liệu số như vậy?

Câu trả lời đó là sử dụng chữ lý điện tử. Chữ ký điện tử đi kèm với các thông tin chủ sở hữu và một số thông tin cần thiết khác sẽ trở thành chứng chỉ điện tử. Chữ ký điện tử hoạt động dựa trên hệ thống mã hóa công khai. Mỗi chủ thể có một cặp khóa như vậy, chủ thể đó sẽ giữ khóa bí mật, còn khóa công khai sẽ được đưa ra công cộng để bất kỳ ai cũng có thể biết. Nguyên tắc của hệ thống mã khóa công khai đó là, nếu ta mã hóa bằng khóa bí mật thì chỉ có khóa công khai mới giải mã được, và ngược lại thì nếu mã hóa bằng khóa công khai thì khóa bí mật mới giải mã được.

**2.1.2. Định nghĩa chữ ký số**

Chữ ký số (digital signature) là đoạn dữ liệu ngắn đính kèm với văn bản gốc để chứng thực tác giả (người ký văn bản) của văn bản và giúp người nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc.

**2.1.3. Các ưu điểm của chữ ký số**

Việc sử dụng chữ ký số mang lại một số lợi điểm sau:

**Khả năng nhận thực:**

Các hệ thống mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa biết. Để sử dụng chữ ký số thì văn bản không cần phải được mã hóa mà chỉ cần mã hóa hàm băm của văn bản đó (thường có độ dài cố định và ngắn hơn văn bản). Khi cần kiểm tra, bên nhận giải mã (với khóa công khai) để lấy lại hàm băm và kiểm tra với hàm băm của văn bản nhận được. Nếu 2 giá trị này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản xuất phát từ người sở hữu khóa bí mật. Tất nhiên là chúng ta không thể đảm bảo 100% là văn bản không bị giả mạo vì hệ thống vẫn có thể bị phá vỡ.

Vấn đề nhận thực đặc biệt quan trọng đối với các giao dịch tài chính. Chẳng hạn một chi nhánh ngân hàng gửi một gói tin về trung tâm dưới dạng (a,b), trong đó a là số tài khoản và b là số tiền chuyển vào tài khoản đó. Một kẻ lừa đảo có thể gửi một số tiền nào đó để lấy nội dung gói tin và truyền lại gói tin thu được nhiều lần để thu lợi (tấn công truyền lại gói tin).

**Tính toàn vẹn**

Cả hai bên tham gia vào quá trình thông tin đều có thể tin tưởng là văn bản không bị sửa đổi trong khi truyền vì nếu văn bản bị thay đổi thì hàm băm cũng sẽ thay đổi và lập tức bị phát hiện. Quá trình mã hóa sẽ ẩn nội dung của gói tin đối với bên thứ 3 nhưng không ngăn cản được việc thay đổi nội dung của nó. Một ví dụ cho trường hợp này là tấn công đồng hình (homomorphism attack): tiếp tục ví dụ như ở trên, một kẻ lừa đảo gửi 1.000.000 đồng vào tài khoản của a, chặn gói tin (a,b) mà chi nhánh gửi về trung tâm rồi gửi gói tin (a,b3 ) thay thế để lập tức trở thành triệu phú!

**Tính không thể phủ nhận**

Trong giao dịch, một bên có thể từ chối nhận một văn bản nào đó là do mình gửi. Để ngăn ngừa khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số với văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết. Tuy nhiên, khóa bí mật vẫn có thể bị lộ và tính không thể phủ nhận cũng không thể đạt được hoàn toàn

**2.1.4 Tình trạng hiện tại - luật pháp và thực tế**

Tất cả các mô hình chữ ký số cần phải đạt được một số yêu cầu để có thể được chấp nhận trong thực tế: Chất lượng của thuật toán: một số thuật toán không đảm bảo an toàn; Chất lượng của phần mềm/phần cứng thực hiện thuật toán; Khóa bí mật phải được giữ an toàn; Quá trình phân phối khóa công cộng phải đảm bảo mối liên hệ giữa khóa và thực thể sở hữu khóa là chính xác. Việc này thường được thực hiện bởi hạ tầng khóa công cộng (PKI) và mối liên hệ khóa người sở hữu được chứng thực bởi những người điều hành PKI. Đối với hệ thống PKI mở, nơi mà tất cả mọi người đều có thể yêu cầu sự chứng thực trên thì khả năng sai sót là rất thấp. Tuy nhiên các PKI thường mại cũng đã gặp phải nhiều vấn đề có thể dẫn đến những văn bản bị ký sai.

Những người sử dụng (và phần mềm) phải thực hiện các quá trình đúng thủ tục (giao thức). Chỉ khi tất cả các điều kiện trên được thỏa mãn thì chữ ký số mới là bằng chứng xác định người chủ (hoặc người có thẩm quyền) của văn bản. Một số cơ quan lập pháp, dưới sự tác động của các doanh nghiệp hy vọng thu lợi từ PKI hoặc với mong muốn là người đi tiên phong trong lĩnh vực mới, đã ban hành các điều luật cho phép, xác nhận hay khuyến khích việc sử dụng chữ ký số. Nơi đầu tiên thực hiện việc này là bang Utah (Hoa kỳ). Tiếp theo sau là các bang Massachusetts và California. Các nước khác cũng thông qua những đạo luật và quy định và cả Liên hợp quốc cũng có những dự án đưa ra những bộ luật mẫu trong vấn đề này. Tuy nhiên, các quy định này lại thay đổi theo từng nớc tùy theo điều kiện về trình độ khoa học (mật mã học). Chính sự khác nhau này làm bối rối những người sử dụng tiềm năng, gây khó khăn cho việc kết nối giữa các quốc gia và do đó làm chậm lại tiến trình phổ biến chữ ký số.

2.1.5.Quy trình tạo ra và kiểm tra chữ ký điện tử:

**Quy trình tạo**

Dùng giải thuật băm để thay đổi thông điệp cần truyền đi,kết quả ta được một message diget,dùng giải thuật md5 ta được digest có chiều dài 128 bit,dùng giải thuật sha ta có chiều dài 160bit.

Sử dụng khóa private key của người để mã hóa message digest thu được ở bước 1,thông thường ở bước này ta dùng giải thuật RSA,kết quả thu được

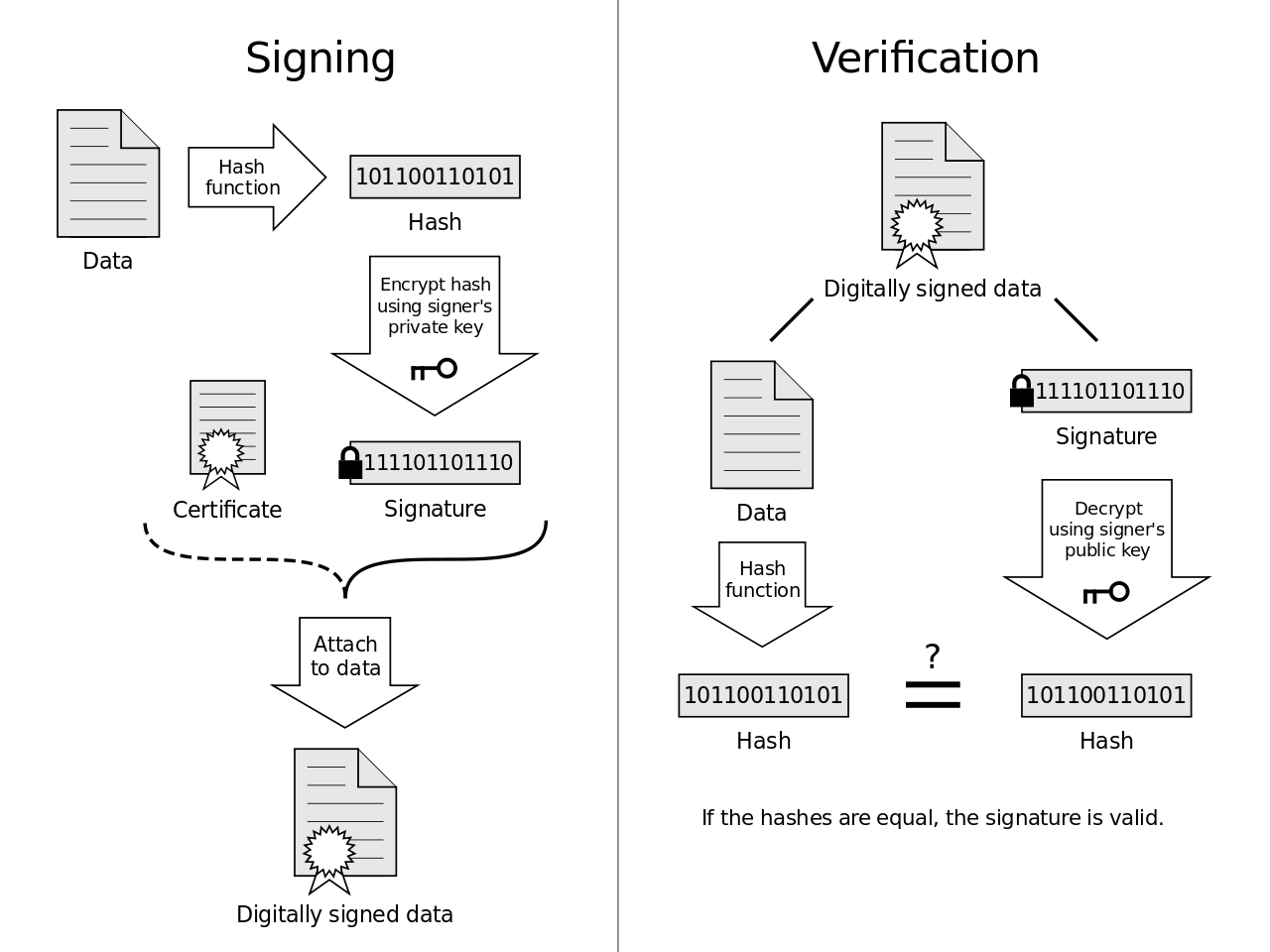
**Các bước kiểm tra**

Dùng public key của người gửi (khóa này được thông báo đến mọi người) để giải mã chữ ký số của message.

Dùng giải thuật md5 hoặc sha băm message đính kèm.

So sánh kết quả thu được ở các bước trên.Nếu trùng nhau,ta kết luận message này không bị thay đổi trong quá trình truyền và message này là của người gửi.

**Quy trình tạo và kiểm tra chữ ký số**



2.2. Sơ đồ chữ ký

2.2.1 Định nghĩa sơ đồ chữ ký

Một sơ đồ chữ ký số là bộ 5 (P, A, K, S, V) thoả mãn các điều kiện sau :

P: là tập hữu hạn các bức điện có thể.

A: là tập hữu hạn các chữ ký có thể.

K: không gian khoá¸ là tập hữu hạn các khoá có thể.

Với mỗi K K tồn tại một thuật toán ký S và một thuật toán xác minh V.

Mỗi Sigk: P->A và : P xA -> {TRUE, FALSE} là những hàm sao cho mỗi bức điện x thuộc P và mỗi bức điện y A thoả mãn phương trình sau đây :

Ver(x,y) =

Với mỗi K K hàm và là các hàm thời gian đa thức. sẽ là hàm công khai còn là hàm bí mật. Ta gọi Alice là người gửi còn Bob là người nhận. Không thể dễ dàng tính toán để giả mạo chữ ký của Bob trên bức điện x. Nghĩa là với x cho trước, chỉ có Bob mới có thể tính được chữ ký y để Ver(x,y) =True. Một sơ đồ chữ kí không thể an toàn vô điều kiện vì một người tò mò nào đó có thể kiểm tra tất cả các chữ số y có thể trên bức điện x nhờ dùng thuật toán Ver công khai cho đến khi anh ta có thể tìm thấy một chữ ký đúng. Vì thế, nếu có đủ thời gian anh ta luôn luôn có thể giả mạo chữ ký của Bob. Như vậy, giống như trường hợp hệ thống mã hoá công khai, mục đích của chúng ta là tìm các sơ đồ chữ ký số an toàn về mặt tính toán.

2.2.2 Chữ ký số RSA.

Lược đồ chữ ký RSA được định nghĩa như sau:

Tạo khóa:

Sơ đồ chữ ký cho bởi bộ năm (P,A,K,S,V) Cho n=p.q; với mỗi p,q là các số nguyên tố lớn khác nhau ϕ(n) = (p - 1)(q - 1)

Cho P = A = Zn và định nghĩa: K là tập các khóa, K=(K’,K’’); với K’=a; K’’=(n,b) a,b , thỏa mãn ab ≡ 1mod ϕ (n).

Các giá trị n,b là công khai, các giá trị p,q,a là các giá trị bí mật.

**Tạo chữ ký:**

Với mỗi K=(n.p,q,a,b) xác định:

= xa mod n Kiểm tra chữ ký: (x,y)= true x y b mod n; x, y Zn.

Giả sử A muốn gửi thông báo x, A sẽ tính chữ ký y bằng cách :

y== mod n (a là tham số bí mật của A)

A gửi cặp (x,y) cho B. Nhận được thông báo x, chữ ký số y, B bắt đầu tiến hành kiểm tra đẳng thức

x= mod(n) (b là khóa công khai A)

Nếu đúng, B công nhận y là chữ ký trên x của A. Ngược lại, B sẽ coi x không phải của A gửi cho mình (chữ ký không tin cậy).

Người ta có thể giả mạo chữ ký của A như sau: chọn y sau đó tính x=(y), khi đó y= . Một cách khắc phục khó khăn này là việc yêu cầu x phải có nghĩa. Do đó chữ ký giả mạo thành công với xác suất rất nhỏ. Ta có thể kết hợp chữ ký với mã hóa làm cho độ an toàn tăng thêm.

Giả sử trên mạng truyền tin công cộng, ta có hai hệ mật mã khóa công khai δ1 và hệ xác nhận chữ ký δ2. Giả sử B có bộ khóa mật mã K=(K’,K’’) với K’=(n,e) và K’’=d trong hệ δ1, và A có bộ khóa chữ ký Ks=(Ks’,Ks’’) với Ks’= a và Ks’’=(n,b) trong hệ δ2. A có thể gửi đến B một thông báo vừa bảo mật vừa có chữ ký xác nhận như sau: A tính chữ ký của mình là: y= ), và sau đó mã hóa cả x và y bằng cách sử dụng mật mã công khai của B, khi đó A nhận được z= (x,y), bản mã z sẽ được gửi tới B, khi nhận được z việc trước tiên B phải giải mã bằng hàm để nhận được (x,y). Sau đó B sử dụng hàm kiểm tra công khai của A để kiểm tra xem (x,y)= true? Tức là kiểm tra xem chữ ký đó có đúng là của A?

Ví dụ: A dùng lược đồ chữ ký số RSA với n=247,(p=13,q=19);

ϕ (n) = 12.18 = 216. Khóa công khai của A là b=7.

=> a = 7-1mod216 = 31.

A công khai (n,b) = (247,7)

A ký trên thông báo x=100 với chữ ký:

y = modn = mod247 = 74.

A gửi cặp (x,y) = (100,74) cho B, B kiểm tra bằng cách sử dụng khóa công khai của A như sau:

x = modn = mod247 = 100 = x.

B chấp nhận y=74 là chữ ký tin cậy.

**2.2.3 Chữ ký Elgamal.**

Lược đồ chữ ký ElGamal được giới thiệu năm 1985 và được Viện tiêu chuẩn và Công nghệ quốc gia Mỹ sửa đổi thành chuẩn chữ ký số. Lược đồ chữ ký ElGammal không tất định cũng giống như hệ mã hóa ElGamal. Điều này có nghĩa là có nhiều chữ ký hợp lệ cho một thông báo bất kỳ. Thuật toán kiểm tra phải có khả năng khả năng chấp nhận bất kỳ chữ ký hợp lệ nào khi xác minh. Lược đồ chữ ký ElGamal được định nghĩa như sau:

**Tạo khóa:**

Cho p là số nguyên tố sao cho bài toán logarit rời rạc trong là khó và giả sử Z \* p là phần tử nguyên thủy Cho P = Z \* p , A = Z \* p Zp-1 và định nghĩa ♣ K = {(p, a, , ): = a modp }. Các giá trị p, , là công khai, a là bí mật.

**Tạo chữ ký**

Với K = (p, a, , ) và với số ngẫu nhiên k Z \* p 1 ,