CRYPTOGRAPHY

I, Khái niệm về mật mã/mã hóa và các loại mã hóa

* Mật mã là kỹ thuật áp dụng toán học phức tạp để tăng sự an toàn của các giao dịch điện tử.

1, Mã hóa đối xứng

* + Mã khóa : là thành phần quan trọng trong thuật toán mật mã. Mã khóa như 1 chiếc chìa của 1 ổ khóa. Nó thực chất là một chuỗi các bit có chiều dài xác định được sắp xếp ngẫu nhiên.
  + Thuật toán mật mã đối xứng dùng một mã khóa cho cả quá trình mã hóa và giải mã
  + Một chuỗi n bit cho 2 ^ n mã khóa | n={40; 60; 128}
  + Chia thành 2 hình thức: block cipher và stream cipher :
    - Block cipher: Chia thông tin thành những đoạn ngắn và có chiều dài cố định và mã hóa từng đoạn này.
      * DES: là thuật toán tiêu biểu cho mật mã đối xứng. DES chia thông tin thành chuỗi 64 bit và mã hóa bằng mã khóa 56 bit
      * Rijindael: Là thuật toán AES mạnh nhất do 2 người Bỉ đề xướng: Daemen và Rijmen. (Thế hệ kế tiếp của các chuẩn mã đối xứng được gọi chung là AES - Advanced Encryption Standard - dùng mã khóa 128 bit có ưu thế vượt trội so với RC6)
    - Stream cipher: là phương pháp mã hóa từng bit của thông tin.
      * Stream cipher thông dụng nhất là RC4. RC4 rất nhanh, nhanh hơn nhiều so với block cipher và hỗ trợ khóa có độ dài thay đổi.
  + Ưu điểm :
    - Tốc độ thực hiện nhanh
    - Độ bảo mật cao
    - Dung lượng bản mã hóa tương đương bản gốc
  + Nhược điểm:
    - Dùng chung 1 mã khóa cho cả việc mã hóa và giải mã có thể sẽ rất nguy hiểm nếu người khác biết được mã khóa.
    - Số lượng mã khóa phải quản lý gần bằng bình phương số đối tượng tham gia trao đổi thông tin, vì thế không phù hợp với giao dịch trên quy mô lớn.
    - Việc quản lý mã khóa phức tạp, tốn nhiều công sức.

2, Mã hóa bất đối xứng

* + Tổng quan :
    - Thuật toán mật mã bất đối xứng thành công nhất là RSA. RSA được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT - Massachusetts Institute of Technology)
    - RSA thường dùng mã khóa 1024 bit và là thuật toán mật mã bất đối xứng được dùng phổ biến nhất trong công nghệ máy tính hiện nay.
  + Khóa công khai và khóa cá nhân(public key & private key) :
    - Sự khác biệt giữa mật mã đối xứng và bất đối xứng là mật mã bất đối xứng sử dụng 2 khóa là khóa công khai và khóa cá nhân, còn mật mã đối xứng chỉ sử dụng 1 khóa duy nhất để mã hóa và giải mã.
    - Khóa công khai và khóa cá nhân là 2 khóa độc lập luôn được tạo ra cùng nhau và có liên quan toán học với nhau.
    - Khóa công khai: tất cả mọi người đều có thể được biết.
    - Khóa cá nhân: khóa này chỉ người cần giải mã thông tin được biết, hoặc trong 1 số trường hợp đặc biệt có thể là không được biết.
  + Ưu điểm :
    - Độ bảo mật cao
    - Quá trình trao đổi mã khóa không ảnh hưởng đến việc bảo mật thông tin.
    - Số lượng mã khóa phải quản lý bằng với số đối tượng tham gia trao đổi thông tin, do đó phù hợp với giao dịch trên mọi quy mô.
  + Nhược điểm :
    - Tốc độ thực hiện khá chậm.
    - Bản mã có dung lượng lớn hơn nhiều so với bản gốc.

3, Kết hợp bất đối xứng + đối xứng :

* + Mục đích : Nhằm giải quyết các nhược điểm của cả 2 loại mật mã và để đạt được các yêu cầu:
    - Độ bảo mật cao.
    - Tốc độ thực hiện nhanh.
    - Bản mã có dung lượng tương đương bản gốc.
    - Quá trình trao đổi mã khóa không ảnh hưởng đến việc bảo mật thông tin.
    - Phù hợp với giao dịch trên mọi quy mô.

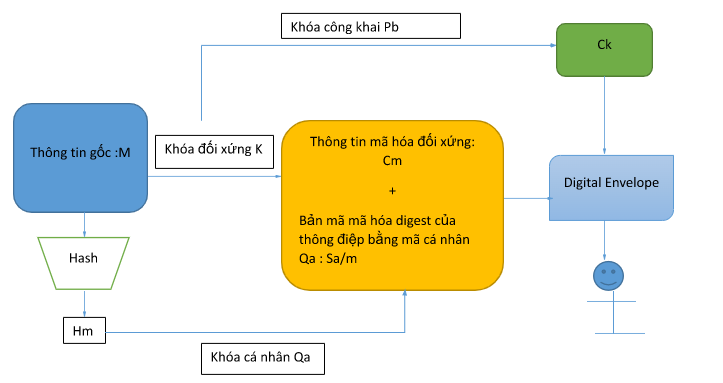
4, Hashes

* + Là một hàm khá phổ biến trong khoa học máy tính, thường được dùng nhất để tăng tốc quá trình xử lý chỉ mục của một mảng hoặc một cơ sở dữ liệu có dung lượng lớn.
  + Hàm băm nhận dữ liệu đầu vào là chuỗi ký tự có độ dài bất kỳ trong một thông điệp để kết xuất một chuỗi ký tự có độ dài xác định. Chuỗi kết quả thường có dung lượng nhỏ hơn rất nhiều lần so với thông điệp gốc.
  + Thông điệp gốc thường được gọi là message. Chuỗi kết quả được gọi là digest hoặc digital fingerprint (dấu tay số) của thông điệp.
  + MD2 là 1 hàm băm từ RSA, tạo ra digest có dung lượng 128 bit.
  + MD5 cũng tạo ra digest có dung lượng 128 bit, nhưng được tối ưu cho bộ vi xử lý 32 bit.
  + SHA-1 cũng được tối ưu cho bộ vi xử lý cao cấp, tạo ra digest có dung lượng 160 bit.
  + Mục đích của hàm băm: khiến cho kẻ tấn công không thể thay đổi thông điệp (cho dù là thay đổi cực nhỏ) mà không làm thay đổi digest.

II. Chữ ký số/Chứng thư số

1, Chữ kí số :

* + Tổng quan : Chữ ký số (Digital Signature) hay chữ ký điện tử (Electronic Signature) là thông tin đi kèm theo dữ liệu nhằm mục đích xác nhận người chủ của dữ liệu đó.
    - Quy trình mã hóa :



1,Phát sinh ngẫu nhiên mã khóa đối xứng: K

2,Hash thông điệp M: Hash(M) -> Hm

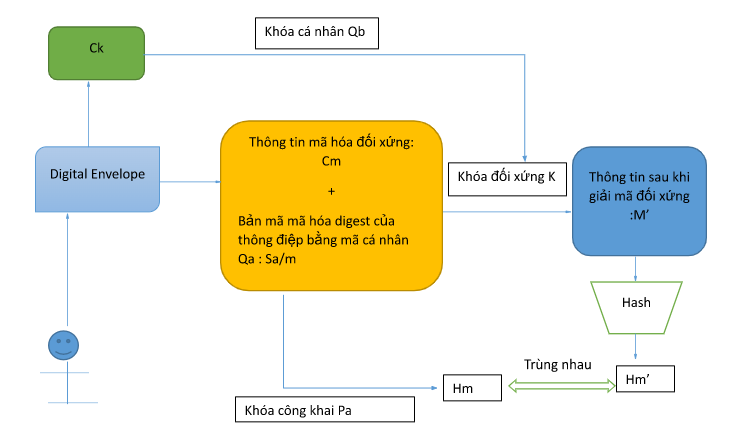
3,Mã hóa đối xứng thông điệp M: M+K = Cm

4,Mã hóa bất đối xứng mã khóa K bằng mã khóa Công khai Pb: K+Pb=Ck

5,Mã hóa Hm bằng mã khóa cá nhân Qa: Hm+Qa=Sa/m

6,Gửi Digital Envelope cho người nhận: Ck & Cm& Sa/m

* + - Quy trình giải mã :



1,Người nhận nhận Digital Envelope: Ck & Cm & Sa/m

2,Giải mã chữ ký số Sa/m bằng mã khóa công khai Pb: Sa/m –Pa=Hm

3,Nếu giải mã thành công => Khóa Qa mã hóa đúng => xuất xứ được xác thực

4,Giải mã gói Ck bằng mã khóa cá nhân Qb: Ck-Qb=K

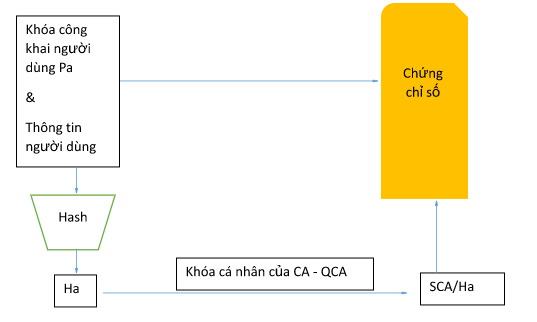
5,Giải mã thông điệp: Cm – K = M’

6,Hash thông điệp: Hash(M’) -> Hm’

7,Nếu Hm và Hm’ trùng khớp nhau => thông điệp toàn vẹn

2, Chứng thư số

* + Chứng chỉ số là một tài liệu khẳng định khóa công khai nào đó thuộc về 1 chủ sở hữu nào đó.
  + Bao gồm :
    - Thông tin của người, tổ chức
    - Khóa công khai
    - Ngày hiệu lực của chứng chỉ
    - Chứng nhận thẩm quyền của chữ ký số
  + Quy trình tạo ra CTS :



1,Phát sinh cặp mã khóa bất đối xứng Pa, Qa

2,Gửi cho bên cấp chứng chỉ số CA Info và khóa công khai Pa.

3,CA phát sinh chứng chỉ số

+ Tạo ra digest của thông tin khách hàng Hash(Pa, Info) -> Ha

+ Dùng mã khóa cá nhân CA để triển khai chữ ký số: Ha + QCA -> SCA/Ha

+ Chứng chỉ số gồm: Mã khóa công khai, tên chủ sở hữu, thời gian hiệu lực, chữ ký số của CA

III, Cơ sở hạ tầng hóa công khai

1, Tại sao mã hóa khóa công khai là chưa đủ?

* + Tạo ra chữ ký số, đầu tiên yêu cầu mã hóa băm được tạo cho nội dung quan trong của tài liệu, để chắc chắn thông tin chưa bị sửa đổi.
  + Xác nhận của chữ ký số yêu cầu băm của nội dung tài liệu. Giá trị băm ban đầu được mã hóa bằng mã khóa cá nhân sau đó được giải mã bằng mã khóa công khai, và sau đó so sánh 2 giá trị băm với nhau. Nếu giá trị giống nhau, thì chữ ký được coi là xác thực.
  + Vấn đề ở đây là làm thế nào biết được cặp khóa được sử dụng để mã hóa và sau đó là giải mã giá trị băm thực sự là 1.

2, Sự cần thiết để định danh được xác thực

* + Vai trò chính của PKI là thiết lập định danh số, cái mà có thể được xác thực.
  + Các lượt nhận diện có thể được sử dụng cùng với cơ chế mã hóa để gửi dịch vụ bảo mật như việc xác thực, ủy quyền, và xác nhận của chữ ký số, nơi mà người sử dụng dịch vụ có thể tin tưởng.

3, Cơ quan cung cấp chứng thực số (Certification Authorities)

* + Cùng với PKI, CA là cơ quan tin cậy chịu trách nhiệm cho việc tạo và xác nhận định danh.
  + CA thực hiện thủ tục xác minh định danh của một người đăng ký cấp xác thực và đưa ra 1 bản chứng chỉ số có khả năng xác minh danh tính người đăng ký đó. Định danh được đưa ra cho 1 khoảng thời gian cụ thể, và CA có khả năng thu hồi chứng nhận đã quá hạn đó.
  + Cơ quan xác thực có thể là những tổ chức như ngân hàng, công ty thẻ tín dụng, bưu điện, các cơ quan khác của chính phủ như Cục thuế hoặc hộ chiếu văn phòng, hay các tập đoàn công nhận chuyên nghiệp như AMA.

4, Ứng dụng của chứng thực

* + Secure Sockets Layer: được lựa chọn để đảm bảo an toàn cho 1 phiên làm việc web khi người sử dụng trình duyệt để truy cập vào URL (https:). Đây là dạng URL dẫn trực tiếp trình duyệt web đến 1 cổng khác trên máy chủ web, và tất cả mọi thông tin được chuyển đi qua các phiên sẽ được mã hóa để đảm bảo sự riêng tư. Ngoài ra, chứng thực còn được sử dụng để thiết lập định danh của máy chủ Web và có thể là các khách hàng web.
  + Secure Electronick Mail: Thư điện tử được bảo vệ bằng các cơ chế khác nhau. Người gửi thư có thể thiết lập các định danh của mình bằng chữ ký số. Người gửi tạo chữ ký sử dụng khóa cá nhân và gửi các chứng thực đó cùng với thư của mình. Điều này cho phép người nhận có thể xác thực danh tính của người gửi và xác minh nội dung của bức thư không bị giả mạo.
  + Virtual Private Networks: (VPNs) cho phép sử dụng mạng Internet công cộng như là một mạng riêng. Để làm được điều này, thông tin phải được mã hóa trước khi nó được truyền giữa các mạng người dùng.