**HẠ TẦNG KHÓA CÔNG KHAI**

1. Mật mã/mã hóa và các loại mã hóa.
   1. Mật mã:
      * là một phương pháp bất kỳ của người quản trị hay người dùng thực hiện với mục đích làm mã hóa văn bản (che giấu người dùng trái phép đọc được).
      * là kỹ thuật áp dụng toán học phức tạp để có thể tăng độ an toàn cho các giao dịch điện tử
      * một mật mã khối là một mật khẩu chia nhỏ thông điệp thành các khối và kết hợp một khóa với mỗi đoạn.
      * Một mật mã dòng là một thuật toán áp dụng một khóa cho từng bit.
      * Hầu hết hiện nay, các mật mã thường được sử dụng là mật mã khối.
      * Quá trình mật mã học còn được biết đến là sự kết hợp giữa quá trình mã hóa và quá trình giải mã.
      * Tính quan trọng của mật mã nhằm đảm bảo:
        + Bảo mật: đảm bảo chỉ có người gửi và người nhận mới có khả năng biết được đoạn giải mã
        + Tính toàn vẹn: Bảo đảm được sự toàn vẹn của nội dung gửi đi
        + Tính xác thực: Chỉ người nhận và người gửi mới có khả năng xác thực thông tin và giải mã đoạn mật mã
        + An toàn: đảm bảo thông tin gửi đi và thông tin lúc nhận là không bị xem trộm hoặc sửa đổi bởi ai đó.
        + Kiếm soát truy cập: chỉ có người gửi và người nhận mới có khả năng mở đoạn đoạn mật mã, tránh sự truy cập trái phép hoặc đọc trộm bởi người khác.
   2. Mật mã đối xứng/bất đối xứng và kết hợp
      * Mật mã đối xứng:
        + Là một thành phần quan trọng của thuật toán mật mã
        + Là một chuỗi các bit có chiều dài xác định được sắp xếp ngẫu nhiên
        + Thuật toán mật mã đối xứng sử dụng 1 khóa cho cả 2 quá trình mã hóa và giải mã.
        + Một chuỗi n bit sẽ cho ra 2 ^ n mã khóa với n = 40,60 hoặc 80.
        + Chia thành 2 hình thức chính là block cipher và stream cipher.
          - Block cipher: Chia thông tin cần mã hóa thành từng đoạn ngắn có chiều dài cố định và thực hiện mã hóa từng đoạn này.Một số thuật toán phổ biến của block cipher: DES,

3-DES, RC2, RC5, RC6, AES(là thuật toán mã hóa đối xứng ưu việt nhất).

* + - * + Stream cipher: là phương pháp mã hóa từng bit thông tin của đoạn cần mã hóa. Có tốc độ nhanh hơn nhiều so với loại block cipher.
* Quá trình mã hóa và giải mã của thuật toán đối xứng.

Nội dung đã mã hóa

khóa đối xứng

Nội dung mã hóa

Nội dung ban đầu

Nội dung đã mã hóa

khóa đối xứng

* Ưu điểm
  + Tốc độ thực hiện nhanh
  + Độ bảo mật cao
  + Dung lượng bản mã tương đương với dung lượng nội dung ban đầu
* Nhược điểm.
  + Sử dụng 1 khóa cho cả 2 quá trình mã hóa và giải mã, điều này có thể gây nguy hiểm khi để lọt khóa đó ra ngoài.
  + 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.
* Mật mã bất đối xứng
  + Đây là loại mã hóa khá khác biệt so với mật mã đối xứng.
  + Sử dụng 1 cặp khóa (private key và public key) để thực hiện mã hóa và giải mã .
    - Private key (khóa cá nhân) và public key là 1 bộ khóa sẽ được tạo cùng nhau và sẽ có sự liên quan toán học với nhau.
    - Private Key (khóa cá nhân) sẽ được sử dụng để thực hiện quá trình giải mã đoạn mã hóa và chỉ có người giải mã mới được biết.
    - Public key (khóa công khai) đây là khóa được sử dụng để thực hiện mã hóa thông tin và ai cũng có thể được biết.
  + Mật mã bất đối xứng giải quyết được vấn đề bảo mật còn có ở mật mã đối xứng đó là việc chỉ sử dụng 1 khóa cho cả 2 quá tình mã hóa và giải mã
  + Một số thuật toán tiêu biểu có thể được kể đến như: RSA (thuật toán thành công nhất và được sử dụng phổ biến nhất), ECC, NTRU,…
  + Quá trình thực hiện mã hóa và giải mã trong mật mã bất đối xứng như sau:

Nội dung đã mã hóa

Public key

Nội dung mã hóa

Nội dung ban đầu

Nội dung đã mã hóa

Private key

* Ưu điểm :
  + - Độ bảo mật cao (cao hơn loại mật mã đối xứng).
    - 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
    - Dung lượng bản mã lớn hơn nhiều so với bản gốc.
* Mật mã kết hợp.
  + Được tạo ra nhằm khắc phục được các nhược điểm của cả 2 loại mật mã trên nhưng vẫn giữ được các ưu điểm như.
    - Khắc phục việc chỉ sự dụng 1 khóa cho cả 2 quá trình trên mật mã đối xứng.
    - Khắc phục được tình trạng tốc độ thực hiện chậm ở mật mã bất đối xứng.
    - Độ bảo mật cao
    - Dung lượng bản mã tương đương bản gốc.
    - Quá trình trao đổi mã khóa không bản hưởng đến bảo mật thông tin.
    - Phù hợp với giao dịch quy mô lớn.
  + Quy trình thực hiện mã hóa và giải mã ở mật mã kết hợp
    - Mã hóa :
      1. Bản mã lúc đầu sẽ được thực hiện mã hóa bằng khóa đối xứng K, sẽ nhận được bản mã (A’).
      2. Tạo ra 1 cặp private key và public key
      3. Sử dụng public key để mã hóa khóa đối xứng K , thu được khóa đối xứng K’ đã mã hóa qua kỹ thuật key wrapping
      4. Từ bản mã A’ ta thực hiện mã hóa từ đầu và khóa K’ ta sẽ thu được 1 bộ gồm thông tin cần mã hóa và khóa cần để giải mã (được gọi là phong bì số - digital envelope) và thực hiện gửi đi.
    - Giải mã:
      1. Từ phong bì số được nhận, ta có bản mã A’ và khóa đối xứng mã hóa K’
      2. Thực hiện sử dụng private key để giải mã K’ ra khóa K đối xứng ban đầu ra kĩ thuật key wrapping.
      3. Từ khóa K được giải mã, ta có thể thực hiện giải mã được bản mã A’ và sẽ thu được nội dung ban đầu.
  + Ưu điểm: Thực hiện giải quyết được các vấn đề tồn đọng mà 2 mật mã đối xứng và bất đối xứng còn có.
  + Nhược điểm: có thể gây sai lệch thông tin nếu có người sử dụng public key để giải mạo thông tin gửi đi.
* Hashes.
  + Là một kỹ thuật cho phép biến nội dung đầu vào với 1 độ dài bất kì thành đầu ra có độ dài nhất định.
  + Đầu ra thường có dung lượng bé hơn nhiều so với đầu vào.
  + Một thuật toán được sử dụng để thực hiện kĩ thuật hashing như MD2, MD5, SHA-1,…
  + Ưu điểm :
    - Rút gọn được nội dung đầu vào, giảm được dung lượng đầu vào,…
    - Bảo mật cao do không thể giải mã được đầu ra của hash để xem được bản gốc. (chỉ có thể thực hiện 1 chiều).
    - Nhược điểm:
* Luôn cho đầu ra có độ dài cố định nên đôi khi có thể gây lãng phí do đầu vào có độ dài nhỏ hơn nhiều.

1. Chữ ký số/chứng thư số

* Chữ ký số : còn được gọi là chữ ký điện tử là thông tin đi kèm dữ liệu nhằm mục đích xác nhận người chủ dữ liệu đó.
* Quy trình thực hiện kí số bao gồm :
  + Ký bằng file .p12:Tạo file CSR 🡪 xin cấp chứng chỉ .cert 🡪 tạo file .p12 🡪 ký
  + Ký bằng thiết bị HSM : tạo CSR 🡪 xin cấp chứng chỉ .cert 🡪 import file cert vào HSM 🡪 ký.
* Quy trình xử lý mã hóa:

1. Phát sinh ngẫu nhiên mã khóa đối xứng: K
2. Thực hiện hàm băm thông điệp M ban đầu: Hash(M) 🡪 Hm
3. Mã hóa đối xứng thông điệp M với khóa đối xứng K: M+K 🡪 Cm
4. Mã hóa bất đối xứng mã khóa K bằng mã khóa Công khai Public key (Pb) : K+Pb 🡪 Ck
5. Mã hóa Hm bằng mã khóa cá nhân Qa: Hm+Qa 🡪 Sa/m
6. Gửi phong bì số cho người nhận: Ck , Cm và Sa/m

* Quá trình xử lí giải mã (thực hiện verify):

1. Người nhận nhận phong bì số từ người gửi: Ck & Cm & Sa/m
2. Giải mã chữ ký số Sa/m bằng mã khóa công khai Public key (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. Kiểm tra thông tin Hm và thông Hm’. Nếu Hm và Hm’ trùng khớp nhau 🡪 thông điệp toàn vẹn

* Chứng thư số

|  |  |
| --- | --- |
| Chữ ký số | Chứng thư số |
| Tương tự với chữ ký truyền thông, xác nhận người kí,… | Là loại chứng thư điện tử, có vai trò như CMND hoặc hộ chiếu |
| Giúp nhận dạng được người gửi là ai | Giúp xác nhận chữ kí là đúng 🡺 xác nhận được cá nhận, tổ chức nào đó kí. |
| Được tạo ra sau khi nhà cung cấp chứng thư số. |  |
| Được tạo ra trong thời gian chứng thư số còn có hiệu lựa và có thể được kiếm tra bởi khóa công khai của chứng thư số. |  |

* Các loại chứng thư số :
  + File p12 hoặc pfx : định dạng nhị phân lưu chứng chỉ số máy chủ, bất kì chứn chỉ, khóa riêng tư, chứa cả private key và public key.
  + CRT hoặc CERT: sử dụng loại tệp X509 v3 khac nhau có chứa dữa liệu ASCII có tiền tố “ ------ Begin…”. Chỉ chứa khóa public key.
  + DER : định dạng nhị phân, không chứa BEGIN/END , hiện thị dãy nhị phân bị cắt xén, cả chứng chỉ số và khóa cá nhận đều có thể mã hóa ở dạng DER.
* Quy trình tạo chứng thư số:

1. Từ thông tin cá nhân, tổ chức nào đó thực hiện tạo ra file Certificate Signing Request (CSR).
2. Thực hiện gửi file CSR đến 1 tổ chức CA (EASYCA,…) để xin cấp chứng chỉ số CERT.
3. Nếu CA xác thực được thông tin từ CSR là đúng sẽ cấp file chứng chỉ số CERT.
4. Từ file CERT có thể thực hiện import vào thiết bị HSM để thiết bị thực hiện kí, hoặc có thể thực hiện tạo ra file p12 để kí.
5. Cơ sở hạ tầng khóa công khai – PKI

* Cho phép cho phép người dùng trong một mạng công cộng không bảo mật (như Internet), có thể trao đổi thông tin một cách an toàn thông qua việc sử dụng một cặp khóa bí mật và công khai được chứng nhận bởi một nhà cung cấp chứng nhận số CA (Certificate Authority) được tín nhiệm.
* Nền tảng khóa công khai cung cấp một chứng chỉ số, dùng để xác minh một cá nhân hoặc một tổ chức, và các dịch vụ danh mục có thể lưu trữ và khi cần có thể thu hồi các chứng chỉ số.
* Vai trò :
  + cung cấp khóa công khai và xác định mối liên hệ giữa khóa và định danh người dùng
  + Mã hóa, giải mã văn bản.
  + Xác thực người dùng ứng dụng
  + Mã hóa email hoặc xác thực người gửi email,
  + Tạo chữ kí số trên văn bản điện tử.
* Các thành phần chính của PKI:
  + Thực thể cuối : đối tượng được chứng nhận chứng thư số
  + Tổ chức chứng nhận: CA,…
  + Chứng nhận khóa công khai
  + Tổ chức đăng kí chứng nhận : RA
  + Kho lưu trữ chứng nhận