TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

AN TOÀN HỆ THỐNG THÔNG TIN

Chương 1

TỔNG QUAN VỀ AN TOÀN HỆ THỐNG THÔNG TIN

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

Nội dung

- An toàn thông tin
- Mối đe dọa & ngăn chặn
- Mục tiêu an toàn hệ thống thông tin
- Chiến lược an toàn hệ thống và bảo vệ mạng
- An toàn thông tin & mật mã
- Các hệ mật mã

3

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

1.1 Tại sao phải bảo vệ thông tin

- Thông tin là một bộ phận quan trọng và là tài sản thuộc quyền sở hữu của các tổ chức

- Sự thiệt hại và lạm dụng thông tin không chỉ ảnh hưởng đến người sử dụng hoặc các ứng dụng mà nó còn gây ra các hậu quả tai hại cho toàn bộ tổ chức đó

- Thêm vào đó sự ra đời của Internet đã giúp cho việc truy cập, xử lý thông tin ngày càng trở nên dễ dàng hơn

4

Hệ thống và tài sản của hệ thống

Khái niệm hệ thống : Hệ thống là một tập hợp các máy tính bao gồm các thành phần, phần cứng, phần mềm và dữ liệu làm việc được tích lũy qua thời gian.

Tài sản của hệ thống bao gồm:

- ✓Phần cứng
- ✓ Phần mềm
- ✓ Dữ liệu
- ✓ Các truyền thông giữa các máy tính của hệ thống
- ✓ Môi trường làm việc
- ✓ Con người

5

1.2 Các mối đe doạ & các biện pháp ngăn chặn

Có 3 hình thức chủ yếu đe dọa đối với hệ thống:

✓Phá hoại: Kẻ tấn công phá hỏng thiết bị phần cứng hoặc phần mềm hoạt động trên hệ thống.

✓Sửa đổi: Tài sản của hệ thống bị sửa đổi trái phép. Điều này thường làm cho hệ thống không làm đúng chức năng của nó. Chẳng hạn như việc thay đổi mật khẩu, thay đổi quyền người dùng trong hệ thống làm họ không thể truy cập vào hệ thống để làm việc.

✓Can thiệp: Tài sản bị truy cập bởi những người không có thẩm quyền. Các truyền thông thực hiện trên hệ thống bị theo dõi, ngăn chặn, sửa đổi.

6

Các mối đe doạ & các biện pháp ngăn chặn

Các đe dọa đối với một hệ thống thông tin có thể đến từ ba loại đối tượng như sau:

- ✓Các đối tượng từ ngay bên trong hệ thống (insider), đây là những người có quyền sử dụng và truy cập hợp pháp đối với hệ thống thông tin
- ✓Những đối tượng ở bên ngoài hệ thống (hacker, attacker, cracker), thông thường các đối tượng này tấn công qua những kết nối với hệ thống như mạng, Internet
- ✓Các phần mềm (spyware, adware …) chạy trên hệ thống.

7

Các mối đe doạ & các biện pháp ngăn chặn

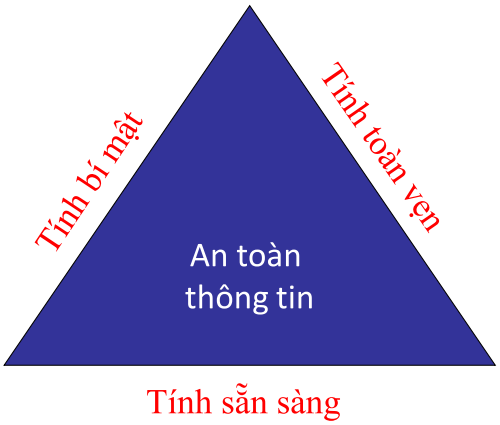
Các biện pháp ngăn chặn:

- ✓**Điều khiển thông qua phần mềm**: dựa vào các cơ chế an toàn bảo mật của hệ thống nền (hệ điều hành), sử dụng các thuật toán mật mã học
- ✓**Điều khiển thông qua phần cứng**: các cơ chế bảo mật, các thuật toán mật mã học được cứng hóa để sử dụng
- ✓**Điều khiển thông qua các chính sách của tổ chức:** ban hành các qui định của tổ chức nhằm đảm bảo tính an toàn bảo mật của hệ thống thông tin.

8

1.3 Mục tiêu của an toàn hệ thống thông tin

Ba mục tiêu chính của an toàn hệ thống thông tin:



9

Mục tiêu của an toàn hệ thống thông tin

Tính bí mật *(Confidentiality)*: - Đảm bảo rằng thông tin không bị truy cập bất hợp pháp. Thuật ngữ *privacy* thường được sử dụng khi dữ liệu được bảo vệ có liên quan tới các thông tin mang tính chất cá nhân.

Tính toàn vẹn *(Integrity)*: Đảm bảo rằng thông tin không bị sửa đổi bất hợp pháp.

Tính sẵn dùng *(availability)*: Tài sản luôn sẵn sàng được sử dụng bởi nhưng người có thẩm quyền.

10

Mục tiêu của an toàn hệ thống thông tin

Tính xác thực *(Authentication):*

- Đảm bảo rằng dữ liệu nhận được chắc chắn là dữ liệu gốc ban đầu

Tính không thể chối từ*(Non-repudiation):*

- Đảm bảo rằng người gửi hay người nhận dữ liệu không thể chối bỏ trách nhiệm sau khi đã gửi và nhận thông tin.

11

1.4 Các chiến lược an toàn hệ thống

Giới hạn quyền hạn tối thiểu *(Last Privilege)*: theo nguyên tắc này bất kỳ một đối tượng nào cũng chỉ được cấp và có những quyền hạn nhất định đối với tài nguyên mạng trong hệ thống thông tin.

Bảo vệ theo chiều sâu *(Defence In Depth):*Không nên dựa vào một cơ chế an toàn nào dù cho chúng có thể rất mạnh, mà nên tạo nhiều cơ chế an toàn khác nhau để tương hỗ lẫn nhau.

Nút thắt *(Choke Point):* Tạo ra "cửa khẩu" hẹp và chỉ cho phép thông tin đi vào, ra hệ thống bằng con đường duy nhất chính là "cửa khẩu" này.

12

Các chiến lược an toàn hệ thống

Điểm nối yếu nhất *(Weakest Link):*Chiến lược này dựa trên nguyên tắc: " Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất".

Tính toàn cục*:* Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ, đảm bảo cho mạng hoạt động tốt.

Tính đa dạng bảo vệ*:* Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau, nếu không khi kẻ tấn công xâm nhập vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

13

Các mức bảo vệ trên mạng

Quyền truy nhập: Là lớp bảo vệ trong cùng nhằm kiểm soát các tài nguyên của mạng và quyền hạn trên tài nguyên đó.

Đăng ký tên /mật khẩu: Thực ra đây cũng là kiểm soát quyền truy nhập, nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống.

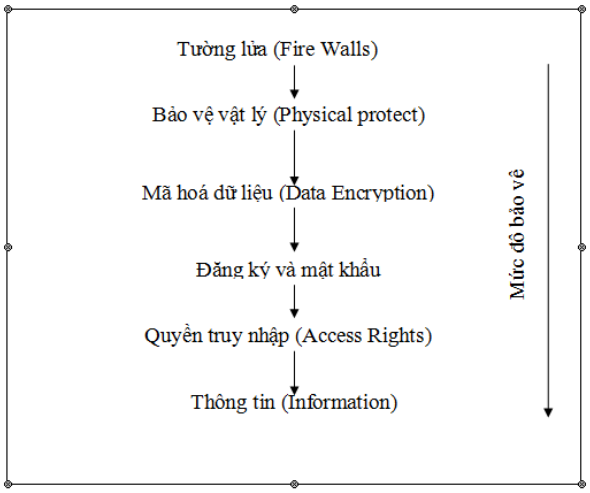
Mã hoá dữ liệu*:* Dữ liệu bị biến đổi từ dạng đọc được sang dạng không đọc được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở nơi nhận (giải mã).

Bảo vệ vật lý*:* Ngăn cản các truy nhập vật lý vào hệ thống.

14

Các mức bảo vệ trên mạng

Tường lửa: Ngăn chặn thâm nhập trái phép và lọc bỏ các gói tin không muốn gửi hoặc nhận vì các lý do nào đó để bảo vệ một máy tính hoặc cả mạng nội bộ (intranet).



15

Các mức bảo vệ trên mạng

Quản trị mạng: Công tác quản trị mạng máy tính phải được thực hiện một cách khoa học đảm bảo các yêu cầu sau :

- ➔ Toàn bộ hệ thống hoạt động bình thường trong giờ làm việc.
- ➔ Có hệ thống dự phòng khi có sự cố về phần cứng hoặc phần mềm xảy ra.
- ➔ Backup dữ liệu quan trọng theo định kỳ.
- ➔ Bảo dưỡng mạng theo định kỳ.
- ➔ Bảo mật dữ liệu, phân quyền truy cập, tổ chức nhóm làm việc trên mạng.

16

Các phương pháp bảo mật

Các phương pháp quan trọng

Mã hóa thông điệp : đảm bảo tính bí mật của thông tin truyền thông

Xác thực quyền : được sử dụng để xác minh, nhận dạng quyền hạn của các thành viên tham gia.

17

1.5 An toàn thông tin bằng mật mã

- Mật mã là một ngành khoa học chuyên nghiên cứu các phương pháp thực hiện truyền tin an toàn, bí mật
- Mật mã bao gồm hai quá trình : Mã hóa và giải mã

Mã hóa: Các sản phẩm của lĩnh vực này là các hệ mật mã , các hàm băm, các hệ chữ ký điện tử, các cơ chế phân phối, quản lý khóa và giao thức mật mã

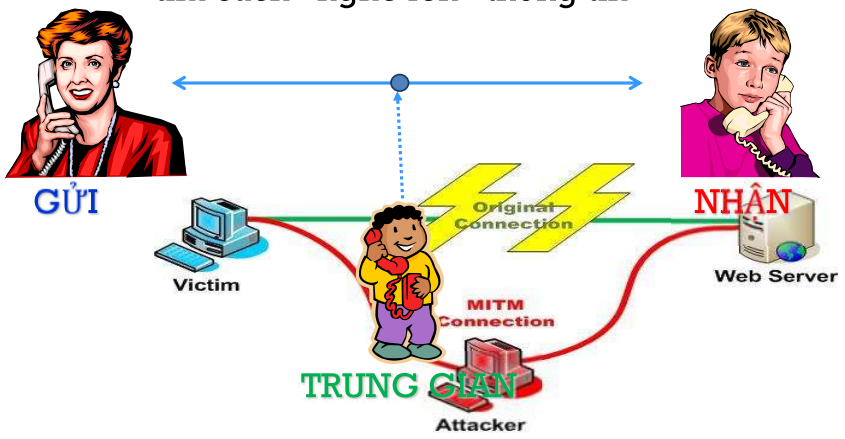
Giải mã: Nghiên cứu các phương pháp phá mã hoặc tạo mã giả. Sản phẩm của lĩnh vực này là các phương pháp phá mã , các phương pháp giả mạo chữ ký, các phương pháp tấn công các hàm băm và các giao thức mật mã

18

An toàn thông tin bằng mật mã

Cách hiểu truyền thống: giữ bí mật nội dung trao đổi

GỬI và NHẬN trao đổi với nhau trong khi có TRUNG GIAN tìm cách "nghe lén" thông tin



19

An toàn thông tin bằng mật mã

- Một trong những phương pháp để bảo vệ thông tin là biến đổi nó thành một định dạng mới khó có thể đọc được

- Mật mã có liên quan đến việc mã hoá các thông báo trước khi gửi chúng đi và tiến hành giải mã chúng lúc nhận được

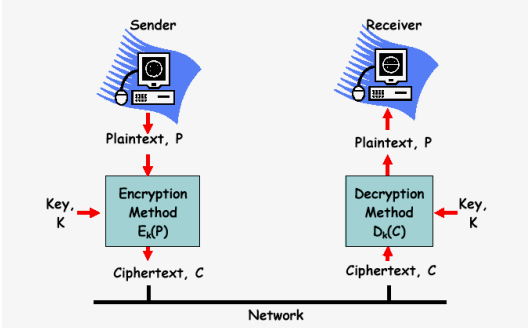


Figure 2: The basic cryptographic techniques

20

An toàn thông tin bằng mật mã

Có 2 phương thức mã hoá cơ bản: thay thế và hoán vị:

✓**Phương thức mã hoá thay thế**: là phương thức mã hoá mà từng ký tự gốc hay một nhóm ký tự gốc của bản rõ được thay thế bởi các từ, các ký hiệu khác hay kết hợp với nhau cho phù hợp với một phương thức nhất định và khoá.

✓**Phương thức mã hoá hoán vị:** là phương thức mã hoá mà các từ mã của bản rõ được sắp xếp lại theo một phương thức nhất định.

21

TRƯỜNG ĐẠI HỌC MỞ TP. HCM
Cơ hội học tập cho mọi người

1.6 Hệ mật mã

Vai trò của hệ mật mã:

✓Hệ mật mã phải che dấu được nội dung của văn bản rõ (PlainText).

✓Tạo các yếu tố xác thực thông tin, đảm bảo thông tin lưu hành trong hệ thống đến người nhận hợp pháp là xác thực (Authenticity).

✓Tổ chức các sơ đồ chữ ký điện tử, đảm bảo không có hiện tượng giả mạo, mạo danh để gửi thông tin trên mạng.

22

Hệ mật mã

Khái niệm cơ bản

✓**Bản rõ** X được gọi là là bản tin gốc. Bản rõ có thể được chia nhỏ có kích thước phù hợp.

✓**Bản mã** Y là bản tin gốc đã được mã hoá. Ở đây ta thường xét phương pháp mã hóa mà không làm thay đổi kích thước của bản rõ, tức là chúng có cùng độ dài.

✓**Mã** là thuật toán E chuyển bản rõ thành bản mã. Thông thường chúng ta cần thuật toán mã hóa mạnh, cho dù kẻ thù biết được thuật toán, nhưng không biết thông tin về khóa cũng không tìm được bản rõ.

23

Hệ mật mã

Khái niệm cơ bản

✓**Khoá** K là thông tin tham số dùng để mã hoá, chỉ có người gửi và người nhận biết. Khóa là độc lập với bản rõ và có độ dài phù hợp với yêu cầu bảo mật.

✓**Mã hoá** là quá trình chuyển bản rõ thành bản mã, thông thường bao gồm việc áp dụng thuật toán mã hóa và một số quá trình xử lý thông tin kèm theo.

✓**Giải mã** chuyển bản mã thành bản rõ, đây là quá trình ngược lại của mã hóa.

24

Hệ mật mã

Các thành phần của một hệ mật mã *:*

Một hệ mật mã là bộ gồm 5 (P, C, K, E, D) thoả mãn các điều kiện sau:

- **P** không gian bản rõ : tập hữu hạn các bản rõ có thể có.
- **C** không gian bản mã : tập hữu hạn các bản mã có thể có.
- **K** là không gian khoá : tập hữu hạn các khoá có thể có.

Đối với mỗi k $\in$ K có một quy tắc mã $e_K: P \rightarrow C$ và một quy tắc giải mã tương ứng $d_K \in D$.

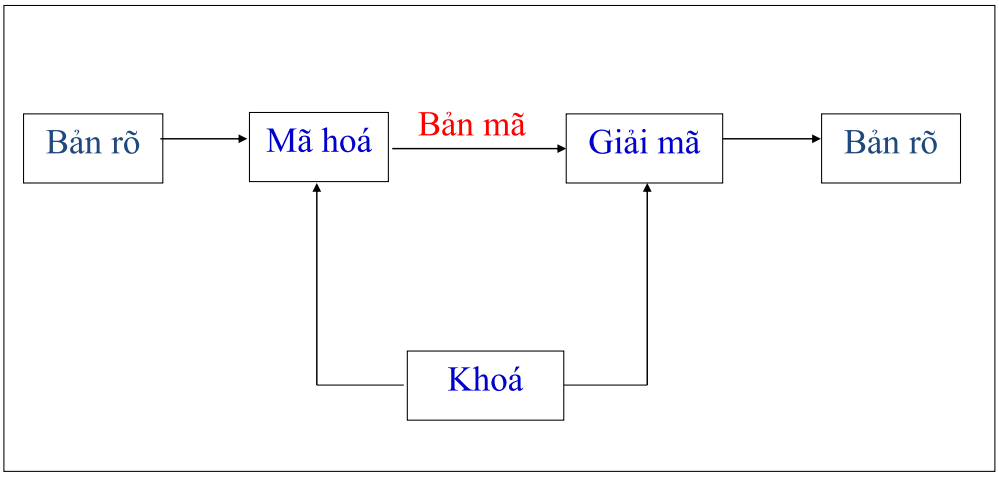
Với mỗi $e_K: P \rightarrow C$ và $d_K: C \rightarrow P$ là những hàm mà

$d_K(e_K(x))=x$ *với mọi bản rõ* $x \in P$.

Hàm giải mã d_k là ánh xạ ngược của hàm mã hóa e_k

25

Hệ mật mã



Quá trình mã hóa và giải mã thông tin

26

Phân loại hệ mật mã

- Hệ mật đối xứng (hay còn gọi là mật mã khóa bí mật): là những hệ mật dùng chung một khoá cả trong quá trình mã hoá dữ liệu và giải mã dữ liệu. Do đó khoá phải được giữ bí mật tuyệt đối. Một số thuật toán nổi tiếng trong mã hoá đối xứng là: DES, Triple DES(3DES), RC4, RC5, AES…

- Hệ mật mã bất đối xứng (hay còn gọi là mật mã khóa công khai): Các hệ mật này dùng một khoá để mã hoá sau đó dùng một khoá khác để giải mã, nghĩa là khoá để mã hoá và giải mã là khác nhau. Các khoá này tạo nên từng cặp chuyển đổi ngược nhau và không có khoá nào có thể suy được từ khoá kia. Khoá dùng để mã hoá có thể công khai nhưng khoá dùng để giải mã phải giữ bí mật. Khoá để mã hoá được gọi là khóa công khai-Public Key, khoá để giải mã được gọi là khóa bí mật - Private Key. Một số thuật toán mã hoá công khai nổi tiếng: Diffle-Hellman, RSA,…

27

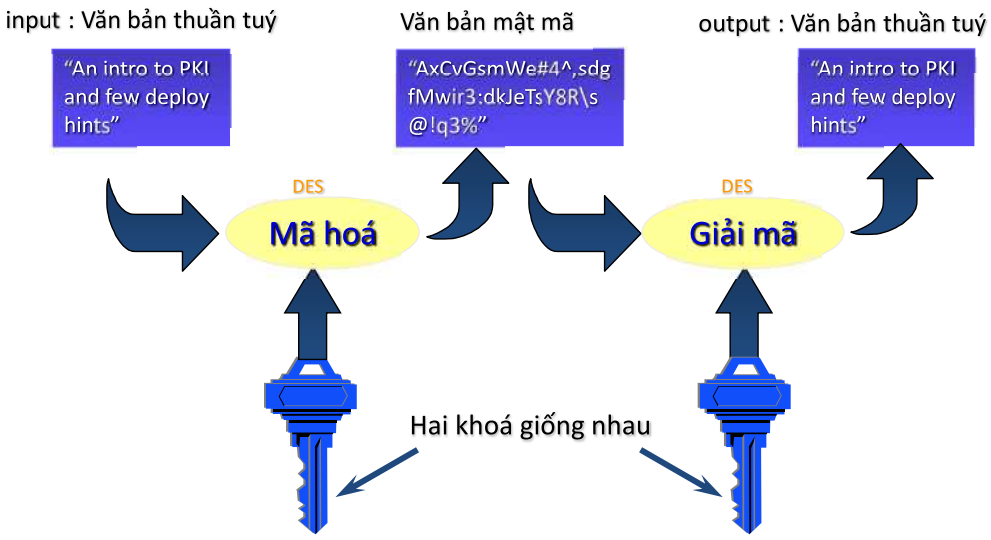
Các phương pháp mã hoá

Các phương pháp chính cho việc mã hoá và giải mã

- ❑ Sử dụng khoá đối xứng
- ❑ Sử dụng khoá bất đối xứng
- ❑ Sử dụng hàm băm một chiều

28

Mã hoá đối xứng



29

Mã hoá đối xứng

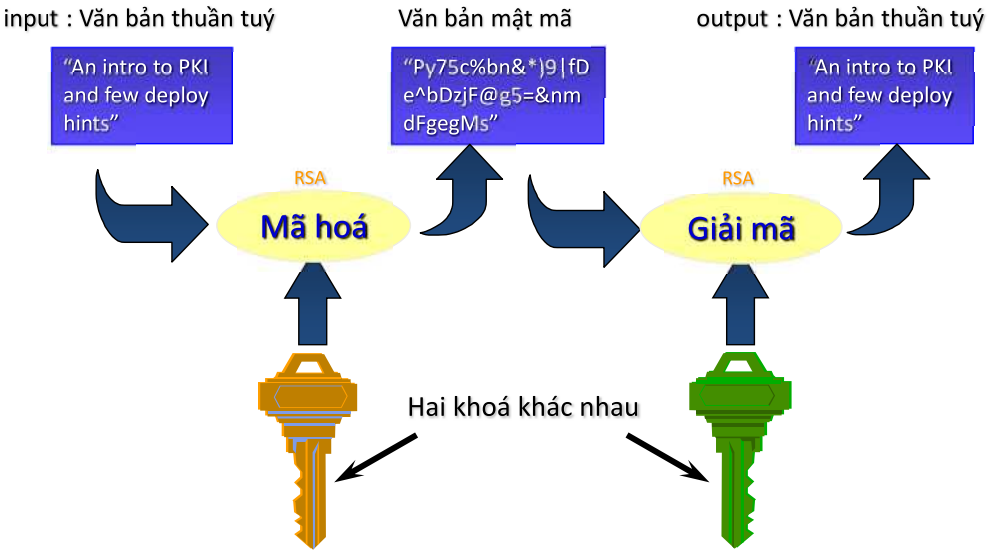
- Các khoá giống nhau được sử dụng cho việc thực hiện mã hoá và giải mã

-Thuật toán mã hoá sử dụng khoá đối xứng thường được biết đến là DES (Data Encryption Standard)

- Các thuật toán mã hoá đối xứng khác được biết đến như:
  + Triple DES, DESX, GDES, RDES - 168 bit key
  + RC2, RC4, RC5 - variable length up to 2048 bits
  + IDEA - basis of PGP - 128 bit key

30

Mã hoá bất đối xứng



31

Mã hoá bất đối xứng

- Các khoá dùng cho mã hoá và giải mã khác nhau nhưng cùng một mẫu và là cặp đôi duy nhất (khoá private/public)
- Khoá riêng (private) chỉ được biết đến bởi người gửi
- Khoá công khai (public) được biết đến bởi nhiều người hơn nó được sử dụng bởi những nhóm người đáng tin cậy đã được xác thực
- Thuật toán mã hoá sử dụng khoá bất đối xứng thường được biết đến là RSA (Rivest,Shamir and Adleman 1978)

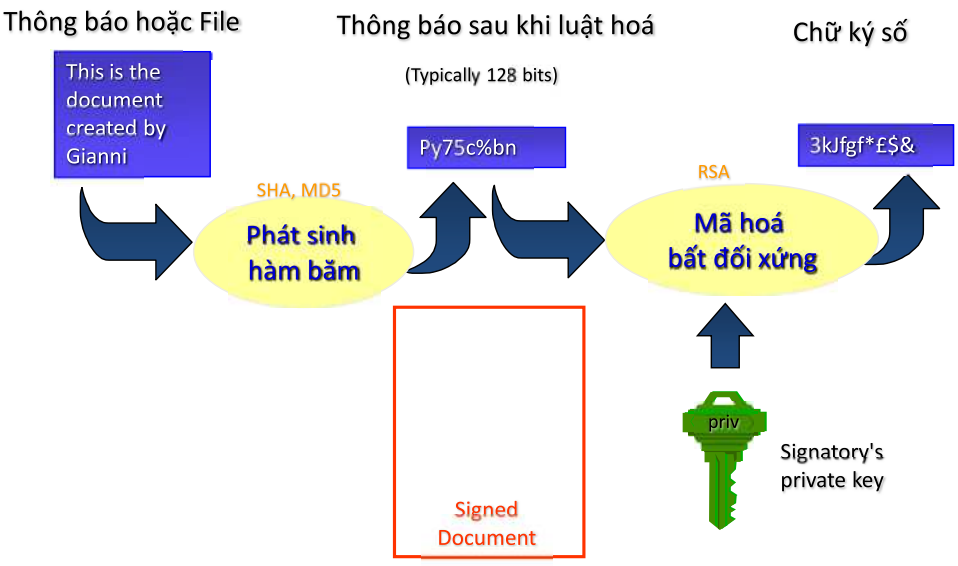
32

Hàm băm

- Một hàm băm H nhận được một thông báo *m* với một độ dài bất kỳ từ đầu vào và đưa ra một chuỗi bít *h* có độ dài cố định ở đầu ra *h = H(m).*
- Hàm băm là một hàm một chiều, điều đó có nghĩa là ta không thể tính toán được đầu vào *m* nếu biết đầu ra *h.*
- Thuật toán sử dụng hàm băm thường được biết đến là MD5

33

Tạo ra chữ ký số



34

Xác thực quyền

Xác minh quyền hạn của các thành viên tham gia quá trình truyền thông trên hệ thống thông tin

Phương pháp phổ biến:

Sử dụng password để xác thực người sử dụng

Một số phương pháp xác thực khác

35

Xác thực quyền

- Sử dụng Kerberos: phương thức mã hoá và xác thực trong AD của công nghệ Window
- Sử dụng Secure Remote Password (SRP): là một giao thức để xác thực đối với các truy cập từ xa
- Sử dụng Hardware Token
- Sử dụng SSL/TLS Certificate Based Client Authentication: sử dụng SSL/TLS để mã hoá, xác thực trong VPN, Web…
- Sử dụng X.509 Public Key
- Sử dụng PGP Public Key
- Sử dụng SPKI Public Key
- Sử dụng XKMS Public Key.
- Sử dụng XML Digital Signature

36

Tiêu chuẩn đánh giá hệ mật mã

Độ an toàn: Một hệ mật mã khi được đưa vào sử dụng điều đầu tiên phải có độ an toàn cao, đáng tin cậy.

- Chúng phải có phương pháp bảo vệ mà chỉ dựa trên sự bí mật của các khoá, còn thuật toán thì công khai. Tại một thời điểm, độ an toàn của một thuật toán phụ thuộc:
  - ✓Nếu chi phí hay phí tổn cần thiết để phá vỡ một thuật toán lớn hơn giá trị của thông tin đã mã hóa thuật toán thì thuật toán đó tạm thời được coi là an toàn.
  - ✓Nếu thời gian cần thiết dùng để phá vỡ một thuật toán là quá lâu thì thuật toán đó tạm thời được coi là an toàn.
  - ✓Nếu lượng dữ liệu cần thiết để phá vỡ một thuật toán rất lớn so với lượng dữ liệu đã được mã hoá thì thuật toán đó tạm thời được coi là an toàn
- Bản mã C không được có các đặc điểm gây chú ý, nghi ngờ.

37

Tiêu chuẩn đánh giá hệ mật mã

- **Tốc độ mã và giải mã:** Khi đánh giá hệ mật mã cần chú ý đến tốc độ mã và giải mã. Hệ mật mã tốt thì thời gian mã và giải mã nhanh.

- **Phân phối khóa:** Một hệ mật mã phụ thuộc vào khóa, khóa này được sẽ được phân phối công khai hay truyền khóa bí mật. Phân phối khóa bí mật thì chi phí sẽ cao hơn so với các hệ mật có khóa công khai và đây cũng là một tiêu chí khi lựa chọn hệ mật mã.

38

Các loại tấn công

Các kiểu tấn công khác nhau

E biết được Y (ciphertext only attack).

Eavesdropper: kẻ nghe trộm (Eve)

E biết một số cặp plaintext-ciphertext X-Y (known plaintext attack).

E biết được một số X-Y, cryptogram của một số tin X do bản thân soạn ra hỗ trợ phá mã (chosen plaintext attack).

39

Một số ứng dụng của mã hóa trong security

- Một số ứng dụng của mã hoá trong đời sống hằng ngày nói chung và trong lĩnh vực bảo mật nói riêng. Đó là:

- ✓ Securing Email
- ✓ Authentication System
- ✓ Secure E-commerce
- ✓ Virtual Private Network
- ✓ Wireless Encryption

40