Công nghệ bảo mật và chữ ký điện tử

Mục tiêu

- Nhắc lại các kiến thức cơ bản về an toàn dữ liệu
- Cung cấp các thông tin về hệ thống xây dựng, phân phối và chứng thực chữ ký điện tử
- Ứng dụng chữ ký điện tử trong quá trình giao dịch và thanh toán thương mại điện tử

Phân phối chương trình

- Số tín chỉ: 1
  - Số tiết lý thuyết: 18
  - Số tiết tự học: 12

Tài liệu tham khảo

- [1] *Giáo trình An toàn dữ liệu,* Bộ môn CNTT, Đại học Thương Mại, 2007.
- [2] Phan Đình Diệu, *Lý thuyết mật mã và an toàn thông tin,* Đại học Quốc gia Hà Nội, 1999.
- [3] William Stallings, *Cryptography and Network Security Principles and Practices, Fourth Edition,* Prentice Hall, 2005

Bài 1. Tổng quan về bảo mật

- 1.1. Sự cần thiết của bảo mật dữ liệu trong thương mại điện tử
- 1.2. Các nguy cơ tấn công trong thương mại điện tử
- 1.3. Các biện pháp bảo mật dữ liệu trong thương mại điện tử
- 1.4. Nhắc lại về mã hóa và hàm băm

1.1. Sự cần thiết của bảo mật dữ liệu trong thương mại điện tử

- Trước đây:
  - Giao dịch trực tiếp giữa bên mua và bên bán

  -> “Tiền trao, cháo múc” -> khó lừa đảo

- Ngày này:
  - Giao dịch trực tiếp ngày càng giảm, giao dịch từ xa ngày càng tăng
  - Bên mua và bên bán không gặp trực tiếp

  -> Dễ bị lừa đảo, gây mất mát thông tin và tài sản

1.1. Sự cần thiết của bảo mật dữ liệu trong thương mại điện tử

- Các hình thức lừa đảo trong thương mại điện tử:
  - Ăn trộm các thông tin cá nhân nhạy cảm (số tài khoản, thẻ tín dụng, …)
  - Giả mạo các bên giao dịch
  - Lừa đảo trong quá trình giao dịch và thanh toán
  - …

1.1. Sự cần thiết của bảo mật dữ liệu trong thương mại điện tử

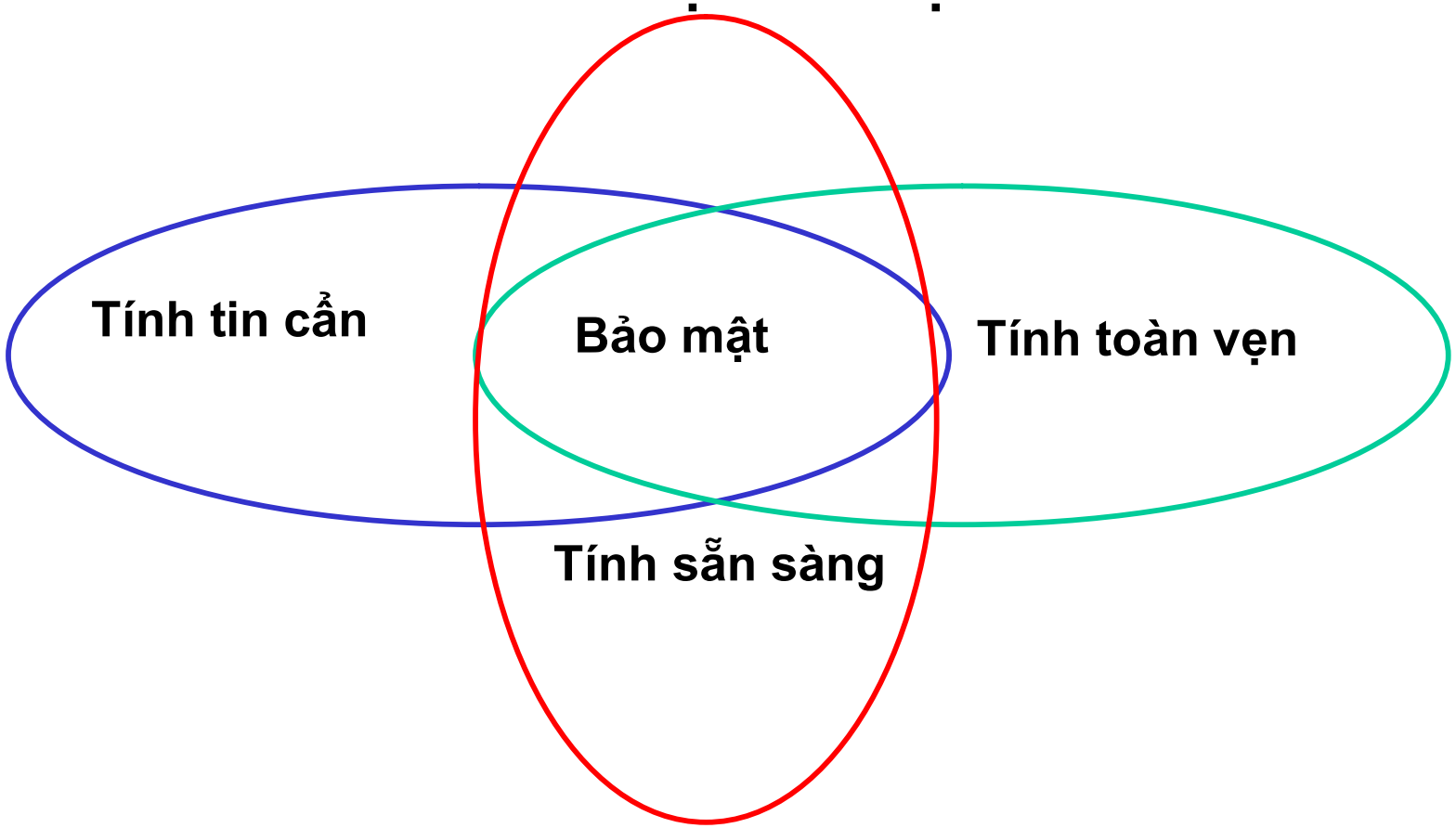
- Ngăn chặn lừa đảo:
  - Sử dụng các biện pháp bảo vệ dữ liệu cá nhân
  - Bảo vệ dữ liệu trong quá trình giao dịch
  - Sử dụng chữ ký số để xác thực các bên mua và bán
  - …

1.1. Sự cần thiết của bảo mật dữ liệu trong thương mại điện tử

- Các yêu cầu của bảo mật dữ liệu
  - Tính toàn vẹn (Integrity):
    - Dữ liệu không bị tạo ra, sửa đổi hay xóa bởi những người không sở hữu.
  - Tính sẵn sàng (Availability):
    - Dữ liệu phải luôn trong trạng thái sẵn sàng.
  - Tính tin cậy (Confidentiality)
    - Thông tin người dùng nhận được là đúng

1.1. Sự cần thiết của bảo mật dữ liệu trong thương mại điện tử

- Yêu cầu của bảo mật dữ liệu



1.2. Các nguy cơ tấn công trong thương mại điện tử

- Tấn công, ăn cắp thông tin trực tiếp trên máy tính
  - Xâm nhập trái phép vào hệ thống (trực tiếp hoặc từ xa)
  - Sử dụng các loại chương trình nguy hiểm (Virus, SpyWare) để ăn trộm thông tin
- Nghe trộm, giả mạo thông tin trên mạng
  - Tấn công thụ động (nghe trộm, phân tích lưu lượng)
  - Tấn công chủ động (sửa đổi, giả mạo, tấn công lặp lại, tấn công từ chối dịch vụ)

1.2. Các nguy cơ tấn công trong thương mại điện tử

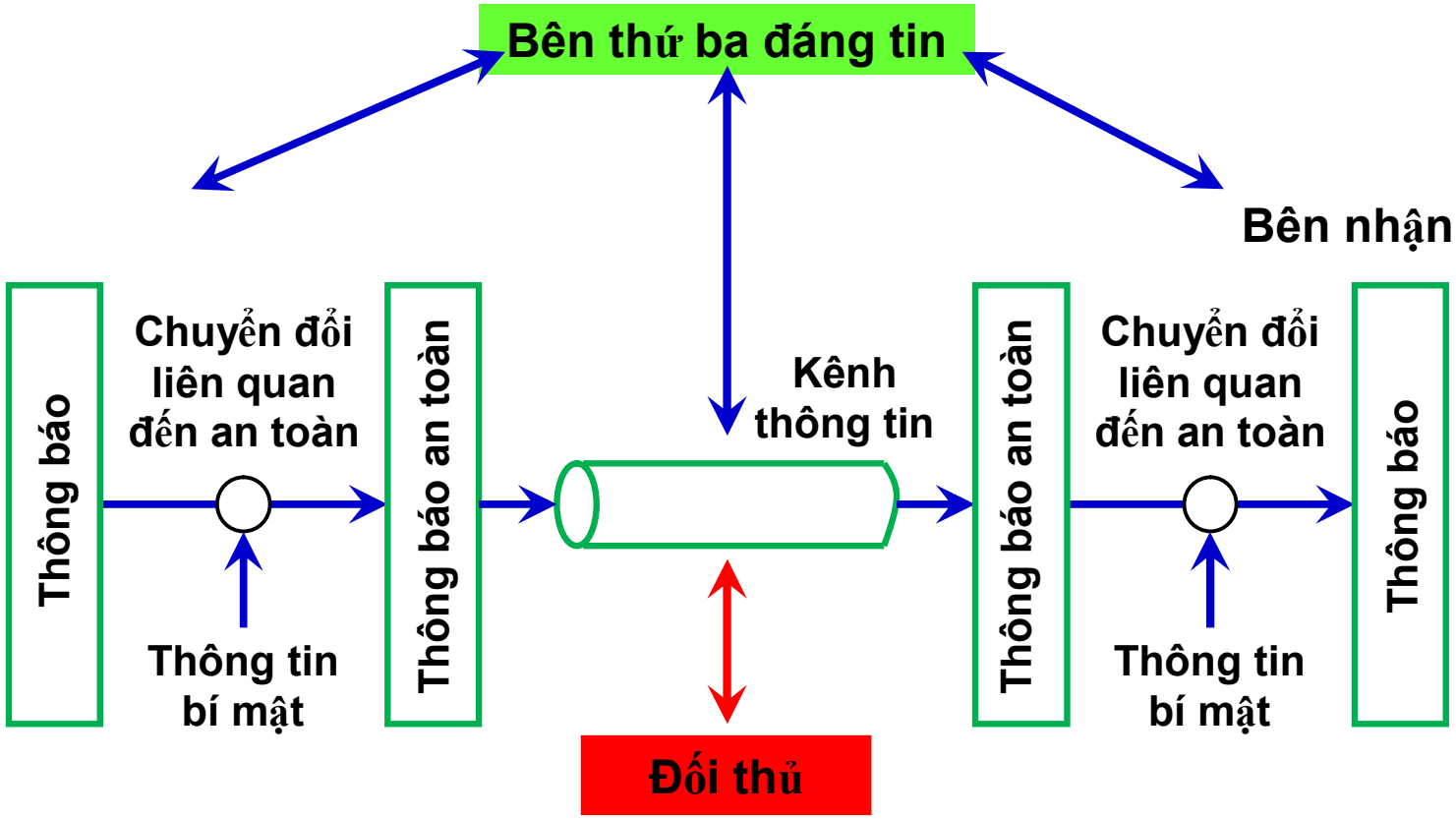
- Một số vụ tấn công dữ liệu trong thương mại điện tử:
  - Ngày 3/3/2006, website Vietco.com của công ty cổ phần Việt Cơ bị tấn công từ chối dịch vụ với một mức độ khủng khiếp. Mọi biện pháp chống đỡ đều vô hiệu.
  - Hơn 40 nhân viên của Việt Cơ "ngồi chơi xơi nước", toàn bộ hoạt động thương mại bị đình trệ. Chỉ cần kéo dài trong vòng 2 tháng, công ty Việt Cơ sẽ phá sản hoàn toàn

1.2. Các nguy cơ tấn công trong thương mại điện tử

- Năm 2004 tại Mỹ, có 205,568 đơn khiếu kiện liên quan đến gian lận Internet, chiếm 53% trong tổng số các đơn kiện về gian lận. Thiệt hại từ các vụ việc liên quan đến gian lận Internet lên tới 265 triệu USD

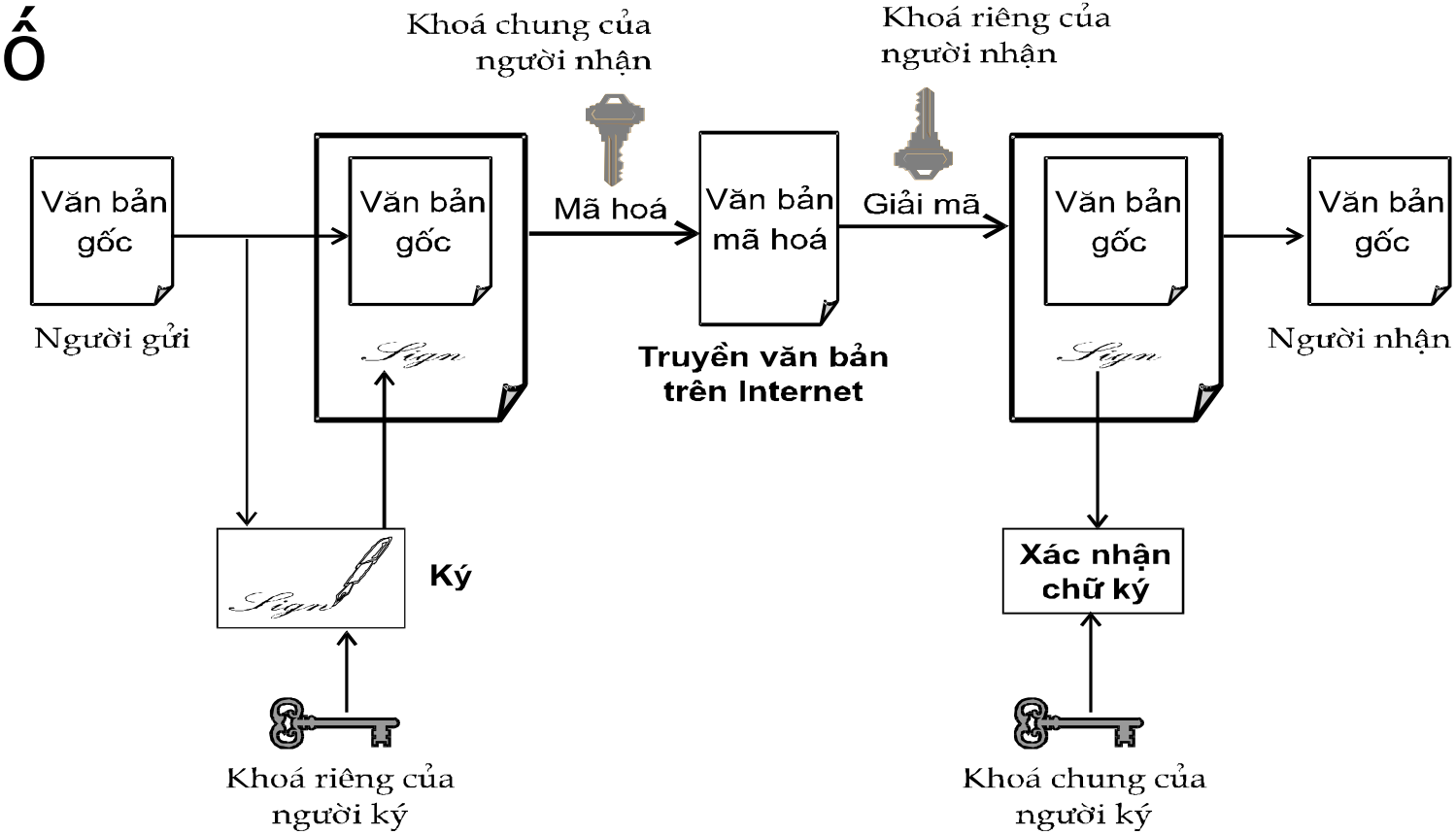
1.3. Các biện pháp bảo mật dữ liệu trong thương mại điện tử

- Bảo mật dữ liệu trên mạng



1.3. Các biện pháp bảo mật dữ liệu trong thương mại điện tử

- Xác thực các bên giao dịch bằng chữ ký số



1.3. Các biện pháp bảo mật dữ liệu trong thương mại điện tử

- Các biện pháp phi kỹ thuật
  - Tăng cường ý thức của những người hoạt động trong lĩnh vực thương mại điện tử
  - Ban hành các luật để ngăn chặn các hành vi tấn công dữ liệu

Một số luật công nghệ thông tin ở Việt Nam

- **Đi u 71.** Ch.ng vi rút máy tính và ph.n m.m gây h.i
- T. ch.c, cá nhân không đư.c t.o ra, cài đ.t, phát tán vi rút máy tính, ph.n m.m gây h.i vào thi.t b. s. c.a ngư.i khác đ. th.c hi.n m.t trong nh.ng hành vi sau đây:
- 1. Thay đ.i các tham s. cài đ.t c.a thi.t b. s.;
- 2. Thu th.p thông tin c.a ngư.i khác;
- 3. Xóa b., làm m.t tác d.ng c.a các ph.n m.m b.o đ.m an toàn, an ninh thông tin đư.c cài đ.t trên thi.t b. s.;
- 4. Ngăn ch.n kh. năng c.a ngư.i s. d.ng xóa b. ho.c h.n ch. s. d.ng nh.ng ph.n m.m không c.n thi.t;
- 5. Chi.m đo.t quy.n đi.u khi.n thi.t b. s.;
- 6. Thay đ.i, xóa b. thông tin lưu tr. trên thi.t b. s.;
- 7. Các hành vi khác xâm h.i quy.n, l.i ích h.p pháp c.a ngư.i s. d.ng.

Đi u 72. B.o đ.m an toàn, bí m.t thông tin

1. Thông tin riêng h.p pháp c.a t. ch.c, cá nhân trao đ.i, truy.n đưa, lưu tr. trên môi trư.ng m.ng đư.c b.o đ.m bí m.t theo quy đ.nh c.a pháp lu.t.
2. T. ch.c, cá nhân không đư.c th.c hi.n m.t trong nh.ng hành vi sau đây:

a) Xâm nh.p, s.a đ.i, xóa b. n.i dung thông tin c.a t. ch.c, cá nhân khác trên môi trư.ng m.ng;

b) C.n tr. ho.t đ.ng cung c.p d.ch v. c.a h. th.ng thông tin;

c) Ngăn ch.n vi.c truy nh.p đ.n thông tin c.a t. ch.c, cá nhân khác trên môi trư.ng m.ng, tr. trư.ng h.p pháp lu.t cho phép;

d) B. khóa, tr.m c.p, s. d.ng m.t kh.u, khóa m.t mã và thông tin c.a t. ch.c, cá nhân khác trên môi trư.ng m.ng;

đ) Hành vi khác làm m.t an toàn, bí m.t thông tin c.a t. ch.c, cá nhân khác đư.c trao đ.i, truy.n đưa, lưu tr. trên môi trư.ng m.ng.

Nhắc lại về mã hóa

- Phương pháp duy nhất để đảm bảo bí mật thông tin trong trường hợp đường truyền không an toàn
- Khái niệm: là phương thức biến đổi thông tin từ định dạng thông thường thành một dạng khác (mã hóa) không giống như ban đầu nhưng có thể khôi phục lại được (giải mã)

Nhắc lại về mã hóa

- Mã hóa
  - Giai đoạn chuyển thông tin nguyên gốc ban đầu thành các dạng thông tin được mã hóa (gọi là bản mã).
- Giải mã
  - Thực hiện biến đổi bản mã để thu lại thông tin nguyên gốc như trước khi mã hóa.

Nhắc lại về mã hóa

- Để mã hóa và giải mã cần một giá trị đặc biệt gọi là khóa (key)
- Giải mã văn bản khi không biết khóa gọi là phá mã
- Các thuật toán mã hóa phải đảm bảo việc phá mã là không thể hoặc cực kỳ khó khăn

Nhắc lại về mã hóa

Độ an toàn của giải thuật mã hóa

- An toàn vô điều kiện: bản mã không chứa đủ thông tin để xác định duy nhất nguyên bản tương ứng. Tức là không thể giải mã được cho dù có máy tính có tốc độ nhanh thế nào đi chăng nữa. (Chỉ duy nhất thuật toán mã hóa độn một lần thỏa mãn an toàn vô điều kiện)

- An toàn tính toán: thỏa mãn một trong hai điều kiện
  - Chi phí phá mã vượt quá giá trị thông tin
  - Thời gian phá mã vượt quá tuổi thọ thông tin

Nhắc lại về mã hóa

- Hiện nay có hai phương pháp mã hóa
  - Mã hóa đối xứng
  - Mã hóa khóa công khai (bất đối xứng)

Nhắc lại về mã hóa

- Mã hóa khóa đối xứng
  - Là phương pháp mã hóa duy nhất trước những năm 70
  - Dùng 1 khóa để vừa mã hóa, vừa giải mã

Nhắc lại về mã hóa

- Một số phương pháp mã hóa khóa đối xứng
  - Mã hóa Ceasar
  - Mã hóa Vigenere
  - Mã hóa hàng rào
  - Mã hóa DES
  - …

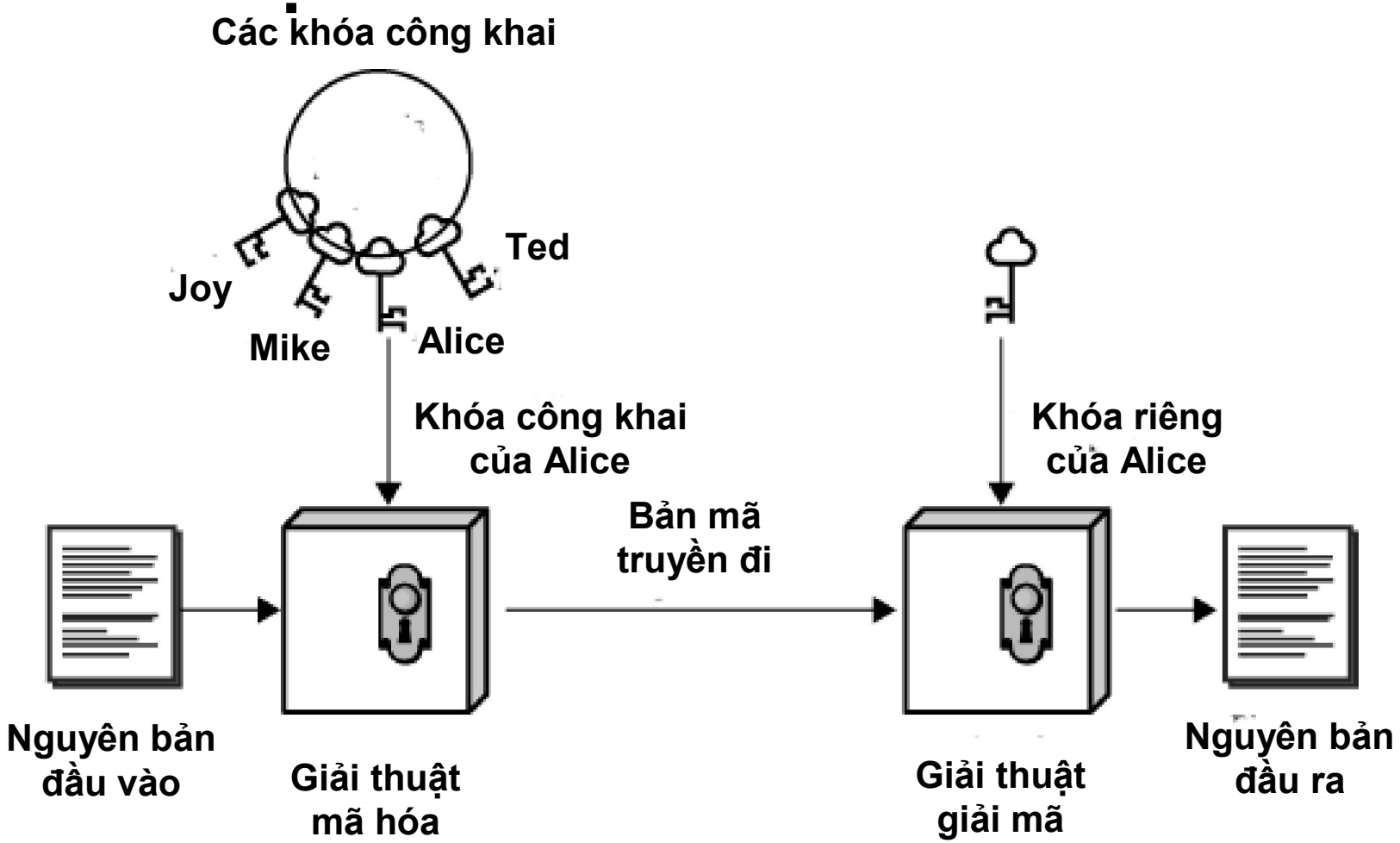
Nhắc lại về mã hóa

- Nhược điểm của mã hóa đối xứng:
  - Trao đổi khóa rất khó khăn
  - Không kiểm tra được gian lận ở một trong hai bên

Nhắc lại về mã hóa

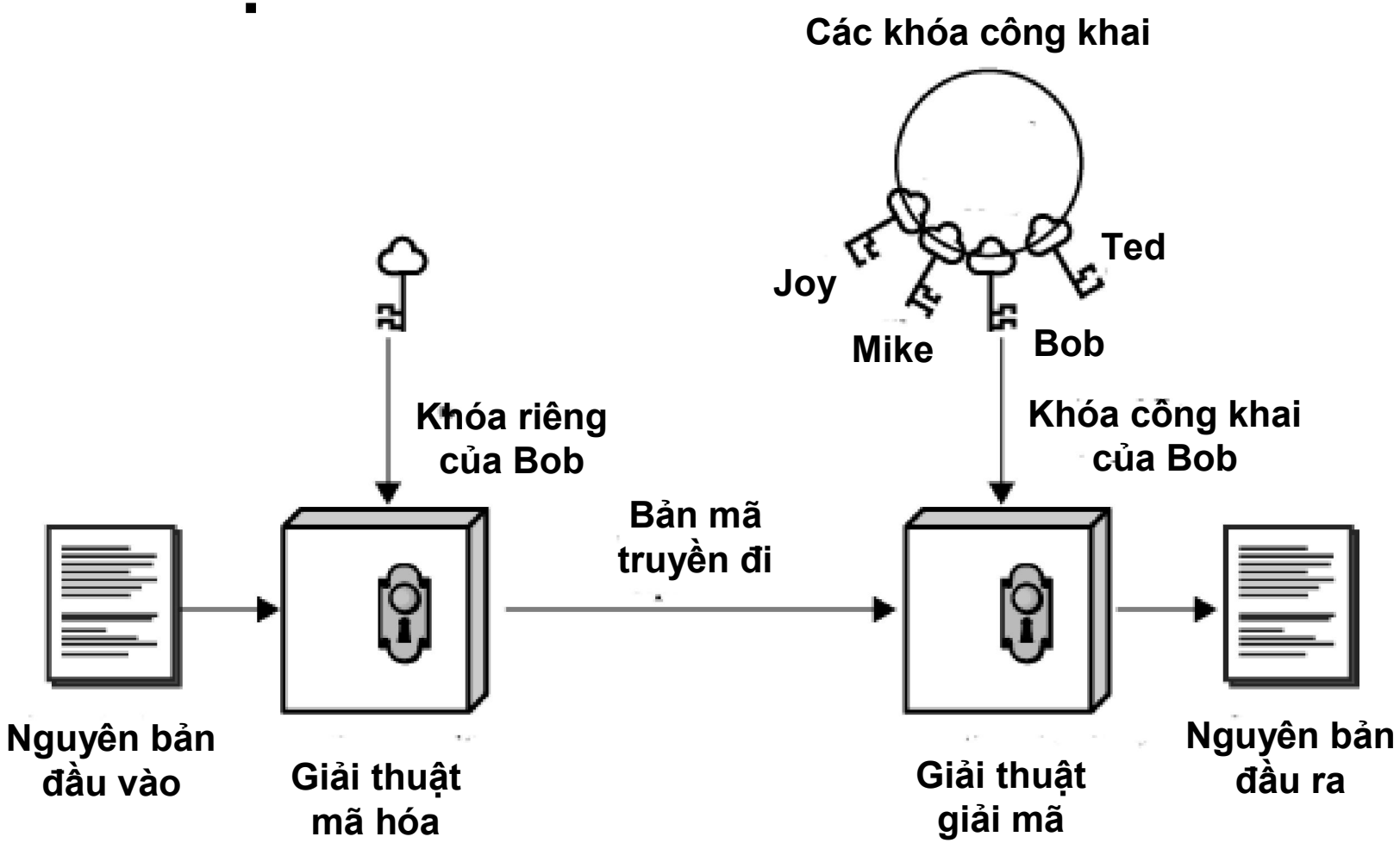
- Mã hóa khóa công khai
  - Sử dụng một cặp gồm 2 khóa, một khóa công khai và một khóa bí mật
  - Khóa công khai:
    - Ai cũng được biết
    - Dùng để mã hóa thông điệp hoặc kiểm tra chữ ký
  - Khóa bí mật:
    - Chỉ nơi giữ được biết
    - Để giải mã thông điệp hoặc tạo chữ ký

Nhắc lại về mã hóa



Mã hóa sử dụng khóa công khai

Nhắc lại về mã hóa



Xác thực bằng khóa công khai

Nhắc lại về mã hóa

- Ứng dụng của mã hóa khóa công khai
  - Mã hóa/giải mã
    - Đảm bảo sự bí mật của thông tin
  - Chữ ký số
    - Hỗ trợ xác thực văn bản
  - Trao đổi khóa
    - Cho phép chia sẻ khóa phiên trong mã hóa đối xứng

Nhắc lại về mã hóa

- Ưu điểm của mã hóa khóa công khai
  - Khóa để mã hóa và giải mã riêng biệt nên khó bị lộ (Chỉ 1 người biết khóa bí mật)
  - Không cần phải trao đổi khóa

Nhắc lại về mã hóa

- Nhược điểm của mã hóa khóa công khai
  - Tốc độ xử lý rất chậm
  - Việc xác thực khóa cũng tương đối khó khăn

Nhắc lại về mã hóa

- Hệ mã hóa RSA
  - Đề xuất bởi Ron Rivest, Adi Shamir và Len Adleman (MIT) vào năm 1977
  - Hệ mã hóa công khai phổ dụng nhất
  - Là hệ mã hóa khối với mỗi khối là một số nguyên < n (Thường kích cỡ n là 1024 bit)

Hàm băm

- Tạo ra một giá trị băm có kích thước cố định từ thông báo đầu vào (không dùng khóa) h = H(M)
- Hàm băm tương tự như việc tạo ra một bản tóm tắt của thông báo
- Bất kỳ sự thay đổi nào dù nhỏ của thông báo cũng tạo ra một giá trị băm khác
- Giá trị băm gắn kèm với thông báo dùng để kiểm tra tính toàn vẹn của thông báo

Hàm băm

- Ví dụ về hàm băm:
  - Thông báo gồm các số 18, 24, 5, 99, 36
  - Tạo ra một hàm băm bằng cách cộng tất cả các số này lại:
    - Giá trị băm h = 18 + 24 + 5 + 99 + 36 = 182
  - Khi một số bất kỳ trong thông báo thay đổi, ta có thể biết được nhờ vào giá trị băm

Hàm băm

- Yêu cầu đối với hàm băm
  - Có thể áp dụng với thông báo M có độ dài bất kỳ
  - Tạo ra giá trị băm h có độ dài cố định
  - H(M) dễ dàng tính được với bất kỳ M nào
  - Tính một chiều: từ giá trị băm h rất khó tìm được thông báo M sao cho H(M) = h

Hàm băm

- Trên thực tế, chữ ký điện tử không được ký trực tiếp vào thông báo mà ký vào giá trị băm. Nhờ tính tương quan giữa thông báo và hàm băm, vẫn có thể kiểm tra tính xác thực của thông báo qua chữ ký này.
- Giá trị băm có kích thước nhỏ, giúp tăng tốc độ trong việc tạo ra chữ ký điện tử.