

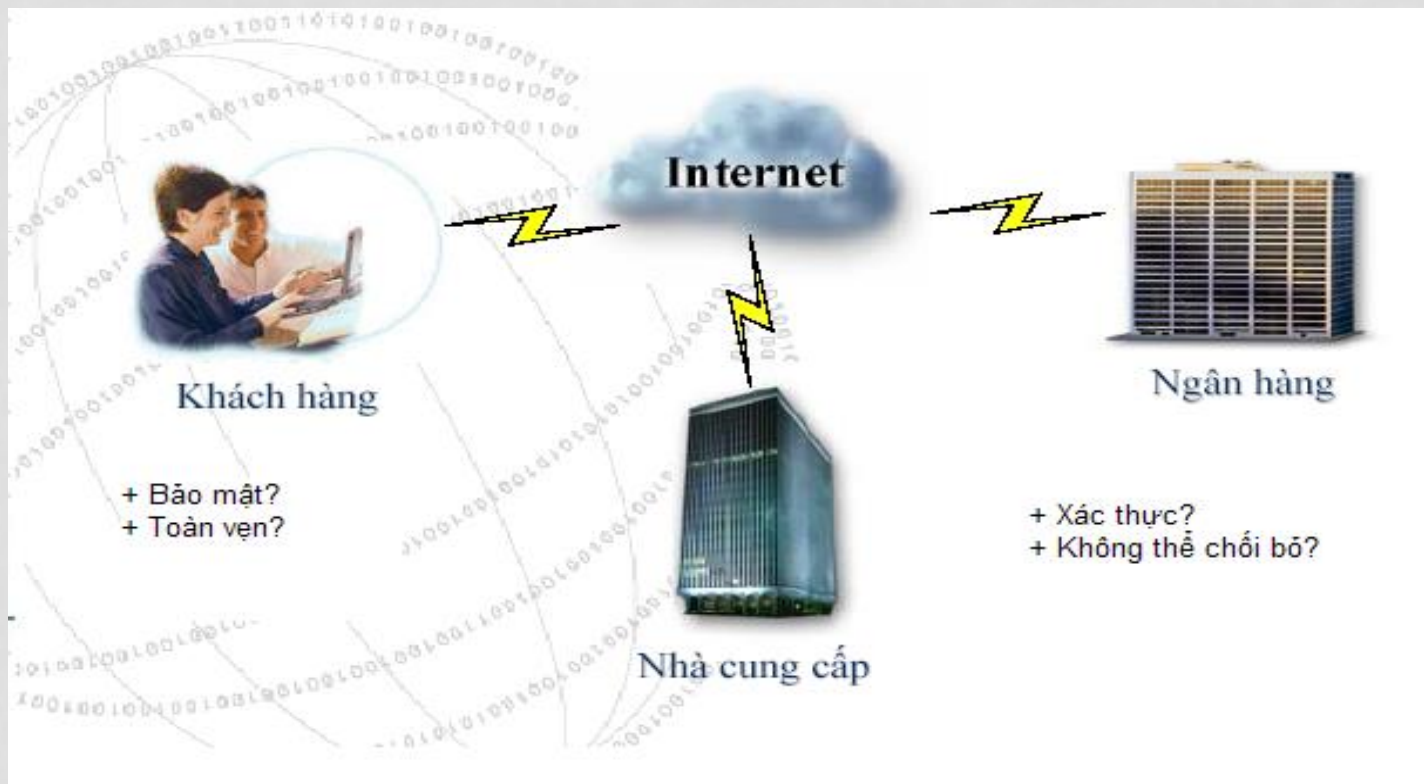
CÁC KHÁI NIỆM CƠ BẢN

CHỨNG THỰC ĐIỆN TỬ

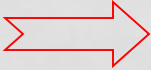
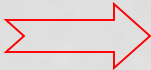
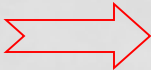
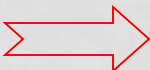


ĐẶT VẤN ĐỀ

Internet: Môi trường lớn cho giao dịch điện tử

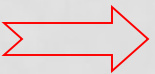
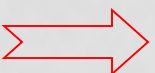

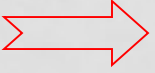


TRONG GIAO DỊCH TRUYỀN THỐNG

- Bảo mật  Sử dụng phong bao
- Toàn vẹn  Chữ ký, condấu, mã vạch
- Xác thực  Công chứng, chứng minh thư, gập mặt
- Chống chối bỏ  Chữ ký, biên nhận

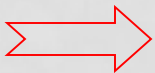



Trong môi trường điện tử -> Nguy cơ tiềm ẩn?

NGUY CƠ TIỀM ẨN TRONG MÔI TRƯỜNG ĐIỆN TỬ

- Bảo mật  Nghe trộm
- Toàn vẹn  Sửa đổi dữ liệu
- Xác thực  Giả mạo
- Chống chối bỏ  Chối bỏ trách nhiệm

Các giải pháp?

GIẢI PHÁP CHO MÔI TRƯỜNG ĐIỆN TỬ

- Bảo mật  Mã hoá dữ liệu
- Toàn vẹn  Hàm băm, chữ ký số
- Xác thực  Chứng chỉ số, chữ ký số
- Chống chối bỏ  Chữ ký số, nhật ký

GIẢI PHÁP CHO MÔI TRƯỜNG ĐIỆN TỬ

- Chứng thực có ý nghĩa rất quan trọng và không thể thiếu được,
- Là hoạt động chứng thực danh tính của những người tham gia vào việc gửi và nhận thông tin

GIẢI PHÁP CHO MÔI TRƯỜNG ĐIỆN TỬ

- Chứng thực điện tử có các chức năng chính:
 - Xác thực:
 - người đối tác,
 - một văn bản quả thực là của người đối tác,
 - một chữ ký quả thực là của đối tác;
 - Toàn vẹn,
 - Bí mật.

GIẢI PHÁP CHO MÔI TRƯỜNG ĐIỆN TỬ

- Nền tảng của CTĐT là

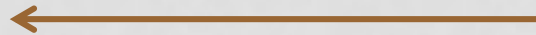
Mật mã khoá công khai

Chữ ký số

VẤN ĐỀ KHI SỬ DỤNG KHOÁ CÔNG KHAI



Bob Gửi Msg mã hoá bởi khoá rỗng e_t : Chỉ có T đọc được



Khoá công khai e_a của A cần được chứng thực,
Vì có thể Bob đã nhận khoá rỗng e_t

CHỮ KÝ ĐIỆN TỬ

- Alice nhận m và chữ ký $\text{Sig}_B(m)$.
- Alice sử dụng khoá công khai của Bob e_B để kiểm tra chữ ký.
- Nếu $e_B(\text{Sig}_B(m)) = m$, thì Alice có thể tin Bob đã ký m .

CHỮ KÝ ĐIỆN TỬ

- Nhưng Bob không công nhận e_B là khoá công khai của mình thì sao ?

Khoá công khai e_B của Bob cần được chứng thực !

AN TOÀN THÔNG TIN

- An toàn thông tin là gì?



AN TOÀN THÔNG TIN

- An toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin
- Đặc tính cơ bản của ATTT
 - Bí mật
 - Toàn vẹn
 - Sẵn sàng



AN TOÀN THÔNG TIN

- Đảm bảo an toàn thông tin
 - An toàn phần cứng
 - Hoạt động cho cơ sở hạ tầng thông tin
 - An toàn phần mềm
 - Các hoạt động quản lý, kỹ thuật bảo vệ hệ thống thông tin

AN TOÀN THÔNG TIN

- Đánh giá an toàn thông tin:
 - Xác định
 - Phân tích nguy cơ
 - Dự báo mức độ
 - Phạm vi ảnh hưởng
 - Khả năng gây thiệt hại

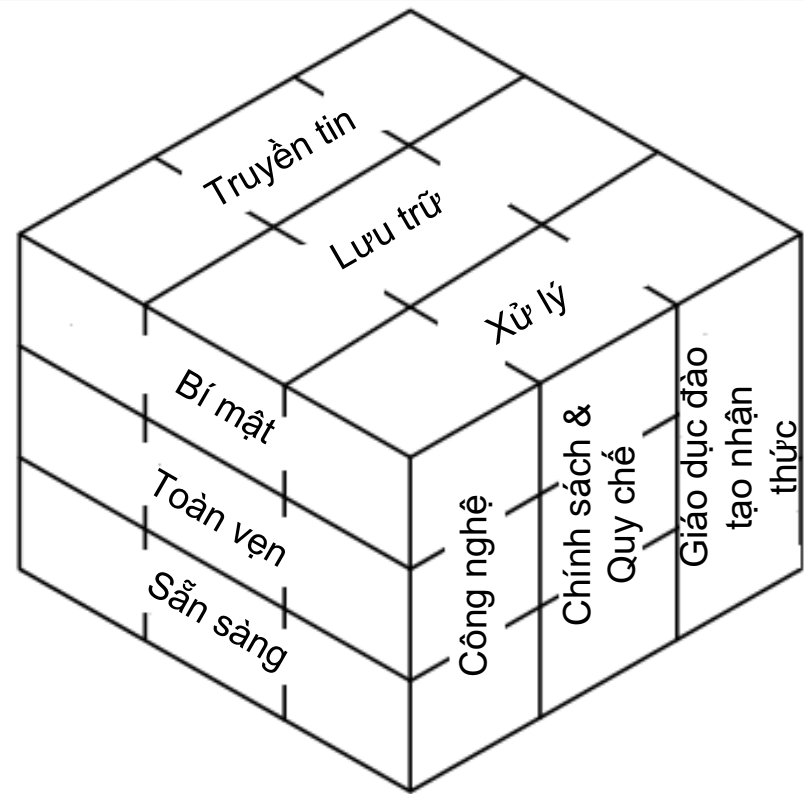


BIỆN PHÁP ĐẢM BẢO ATTT

- Ma trận
 - Trục hoành: 3 trạng thái thông tin
 - Trục tung: 3 đặc tính của thông tin
- Biện pháp:
 - Công nghệ
 - Tổ chức
 - Đào tạo, tập huấn, nâng cao nhận thức

TRẠNG THÁI THÔNG TIN

Các đặc tính thông tin quan trọng



Biện pháp an ninh an toàn

BIỆN PHÁP ĐẢM BẢO ATTT

- Một mô hình tổng thể cho đánh giá an toàn thông tin hết sức cần thiết. Mô hình này không những đáp ứng nhu cầu đảm bảo an toàn các hệ thống thông tin, mà đồng thời còn là một phương tiện hữu hiệu để khảo sát qui hoạch, phát triển hệ thống và đánh giá kết quả
- Cần có **những tiêu chí đánh giá chung** và **lược đồ đánh giá**
- Để tăng cường sự nhất quán và khách quan cho các kết quả đánh giá, cần có một quy trình công nhận/phê chuẩn. Quy trình này xem xét kỹ càng một cách độc lập các kết quả đánh giá để đưa ra chứng nhận/ phê chuẩn về mức độ an toàn cho các sản phẩm/ hệ thống CNTT khi vào sử dụng

GIAO DỊCH ĐIỆN TỬ

- Giao dịch:
 - một chuỗi các hoạt động trao đổi thông tin và các công việc có liên quan nhằm thực hiện một mục tiêu xác định, có bắt đầu và kết thúc, thực hiện giữa hai hay nhiều bên
- Giao dịch điện tử:
 - Giao dịch thực hiện bằng phương tiện điện tử
- Các thông tin được trao đổi trên mạng là thông điệp điện tử



CHÍNH PHỦ ĐIỆN TỬ

- Chính phủ điện tử là chính phủ ứng dụng công nghệ thông tin và truyền thông nhằm tăng hiệu quả hoạt động của các cơ quan chính phủ, phục vụ người dân và doanh nghiệp tốt hơn
- Chức năng:
 - đã đưa chính phủ tới gần dân và đưa dân tới gần chính phủ
 - làm minh bạch hóa hoạt động của chính phủ, chống tham nhũng, quan liêu, độc quyền
 - CPĐT giúp chính phủ hoạt động có hiệu quả trong quản lý và phục vụ dân (cải cách hành chính và nâng cao chất lượng dịch vụ công)

CHÍNH PHỦ ĐIỆN TỬ

- Mục tiêu:
 - Tạo môi trường kinh doanh tốt hơn;
 - Khách hàng trực tuyến, không phải xếp hàng;
 - Tăng cường sự điều hành có hiệu quả của chính phủ và sự tham gia rộng rãi của người dân;
 - Nâng cao năng suất và tính hiệu quả của các cơ quan chính phủ;
 - Nâng cao chất lượng cuộc sống cho các cộng đồng vùng sâu vùng xa.
- Mô hình cơ bản:
 - G2C
 - G2B
 - G2G
 - G2E

CHÍNH PHỦ ĐIỆN TỬ

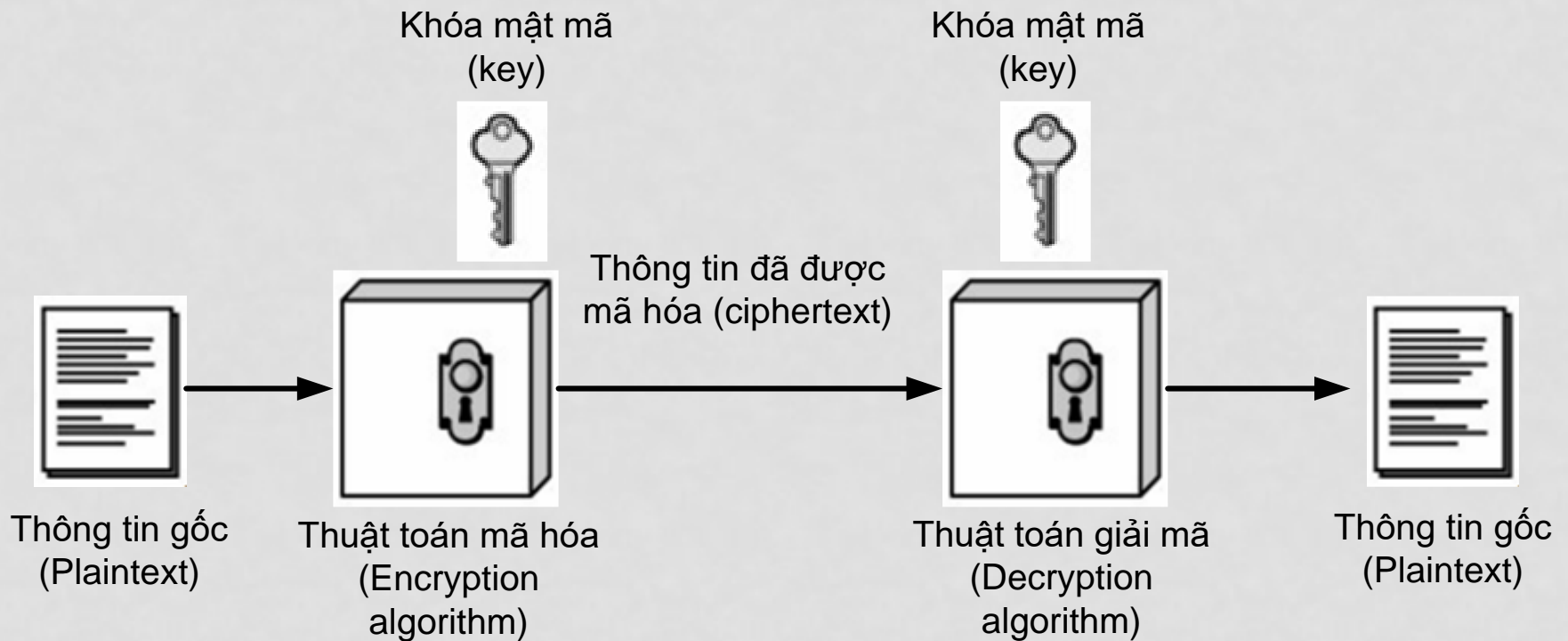
- Lợi ích
 - Đáp ứng mọi nhu cầu của công dân
 - Mang lại sự thuận tiện,
 - Cung cấp dịch vụ hiệu quả, kịp thời
 - Đơn giản hóa các thủ tục hành chính
 - Tăng hiệu quả cho việc xử lý công việc
- Nhược điểm
 - Tăng chi phí an ninh
 - Nguy cơ mất mát dữ liệu và vi phạm tính riêng tư
 - Phải có bên thứ ba giám sát hoạt động của nhà nước và bảo vệ người dân
 - Liên tục cập nhật nâng cấp để theo kịp sự phát triển CNTT
 - Xảy ra vấn đề về tính tương thích
 - Thông tin của người dân có thể bị lạm dụng, rò rỉ, ăn cắp, sử dụng trái phép

MẬT MÃ TRONG ATTT

- Mật mã là một khoa học bảo vệ dữ liệu, cung cấp cách thức và phương tiện chuyển đổi dữ liệu sang dạng không dễ dàng đọc được, do vậy:
 - Người dùng bất hợp pháp không thể truy cập dữ liệu
 - Nội dung của cấu trúc dữ liệu bị ẩn
 - Tính chất xác thực của dữ liệu có thể được chứng minh
 - Ngăn chặn được việc sửa đổi dữ liệu trái phép
 - Người khởi tạo thông điệp không thể từ chối được trách nhiệm của mình với dữ liệu

MẬT MÃ TRONG ATTT

- Mô hình mã hóa thông thường:

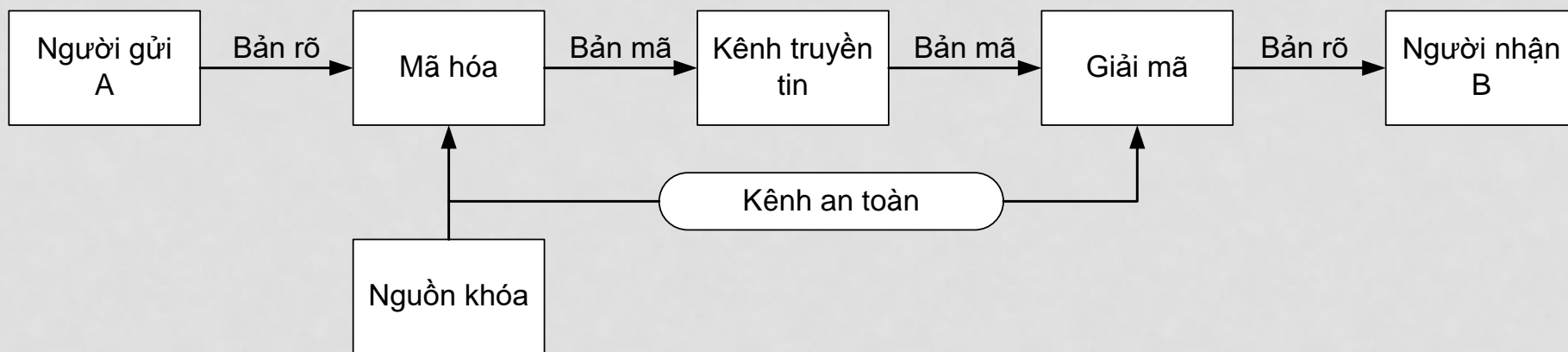


MẬT MÃ TRONG ATTT

- 2 kỹ thuật mã hóa chính
 - Mật mã khóa bí mật – mật mã khóa đối xứng
 - Mật mã khóa công khai – mật mã khóa bất đối xứng

MẬT MÃ TRONG ATTT

- Mật mã khóa đối xứng
 - Sử dụng 1 khóa đơn cho cả quá trình giải mã và mã hóa



Nhược điểm chính là gì?

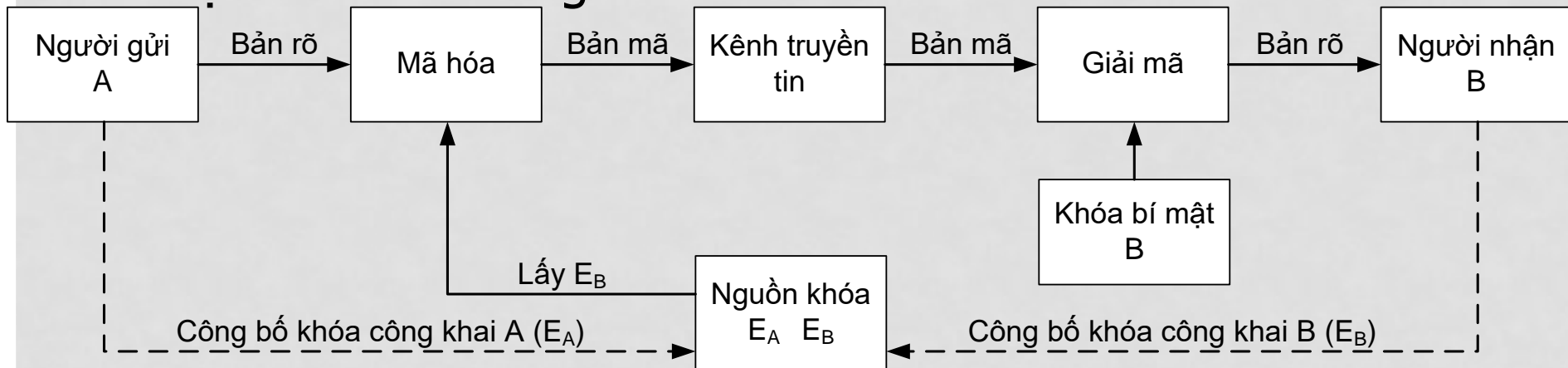
Quá trình phân phối
và trao đổi khóa

Khắc phục?

Mật mã khóa công khai

MẬT MÃ TRONG ATTT

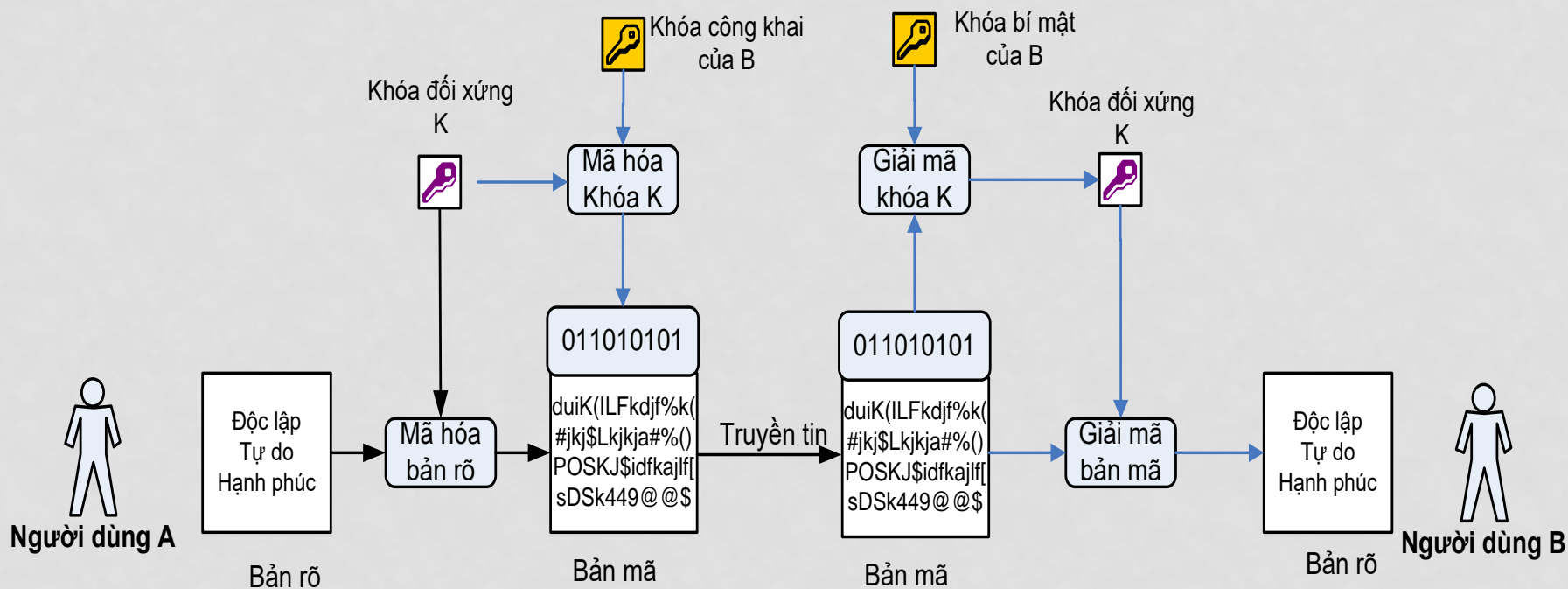
- Mật mã khóa công khai



- Một cặp khóa: một khóa công khai và một khóa bí mật (khóa riêng)
- Giải quyết vấn đề phân phối khóa
- Quản lý khóa đơn giản hơn
- Đảm bảo tính toàn vẹn dữ liệu, xác thực và chống chối bỏ. Vì sao?

MẬT MÃ TRONG ATTT

- So sánh ưu và nhược điểm của hệ mật khóa công khai và hệ mật khóa đối xứng
- Vẽ mô hình kết hợp 2 hệ mật này



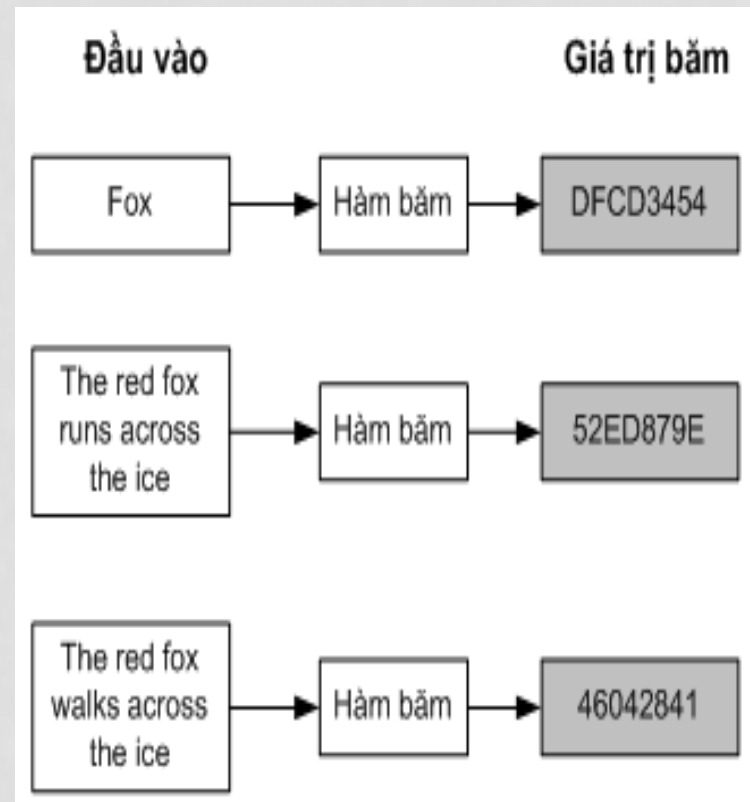
MẬT MÃ TRONG ATTT

- Chữ ký số:
 - Một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã khóa công khai.
 - Có thể kiểm tra được:
 - Khóa bí mật tạo lên chữ ký với khóa công khai dùng để kiểm tra là cùng một cặp khóa
 - Sự toàn vẹn của thông điệp được ký.

MẬT MÃ TRONG ATTT

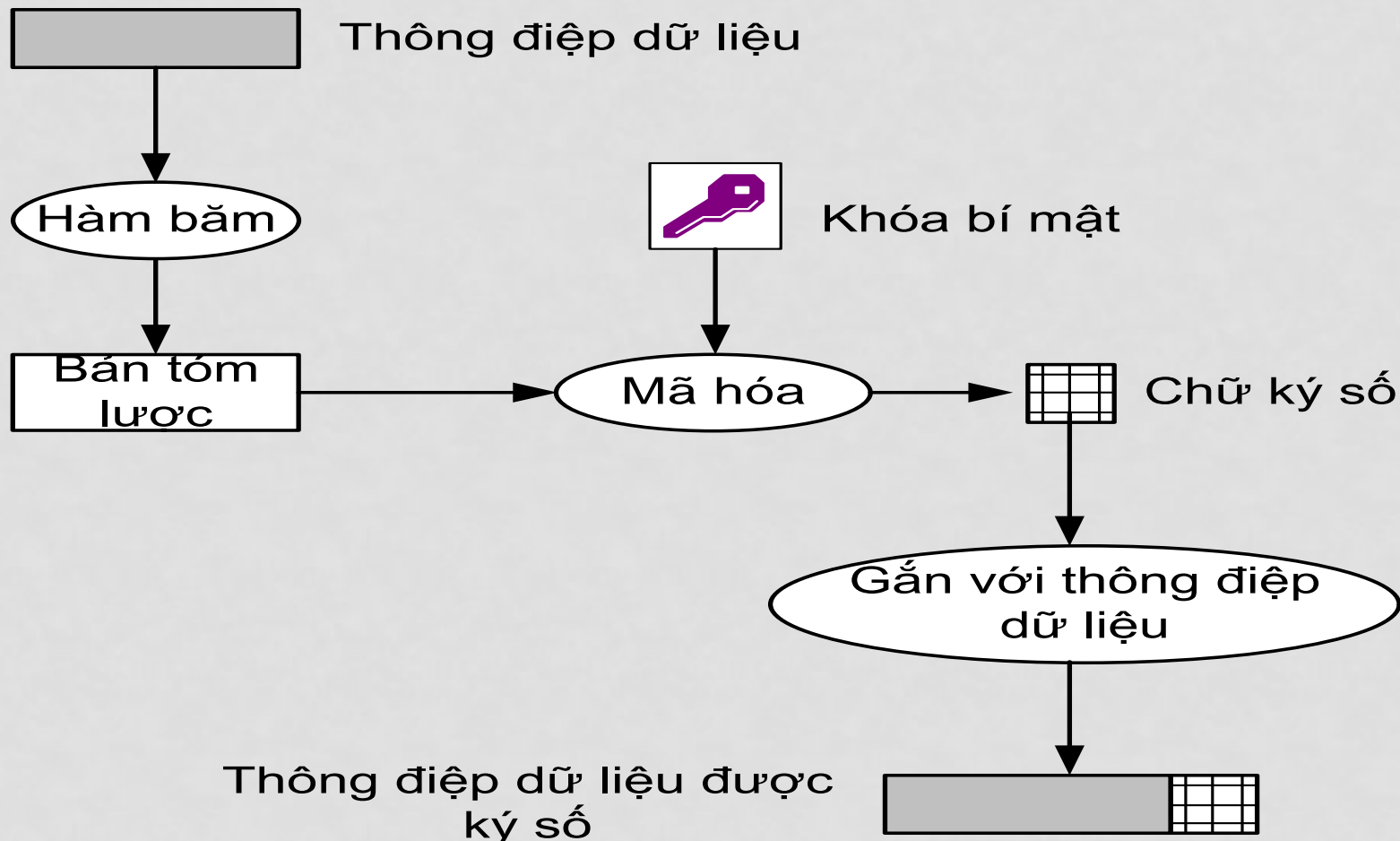
- Hàm băm

- Là hàm một chiều. Từ một khối dữ liệu hay giá trị băm đầu vào chỉ có thể đưa ra một giá trị băm **duy nhất**.
- Nếu đầu vào thay đổi thì giá trị băm cũng bị thay đổi
- Giá trị băm đóng vai trò gần như một khóa để phân biệt các khối dữ liệu



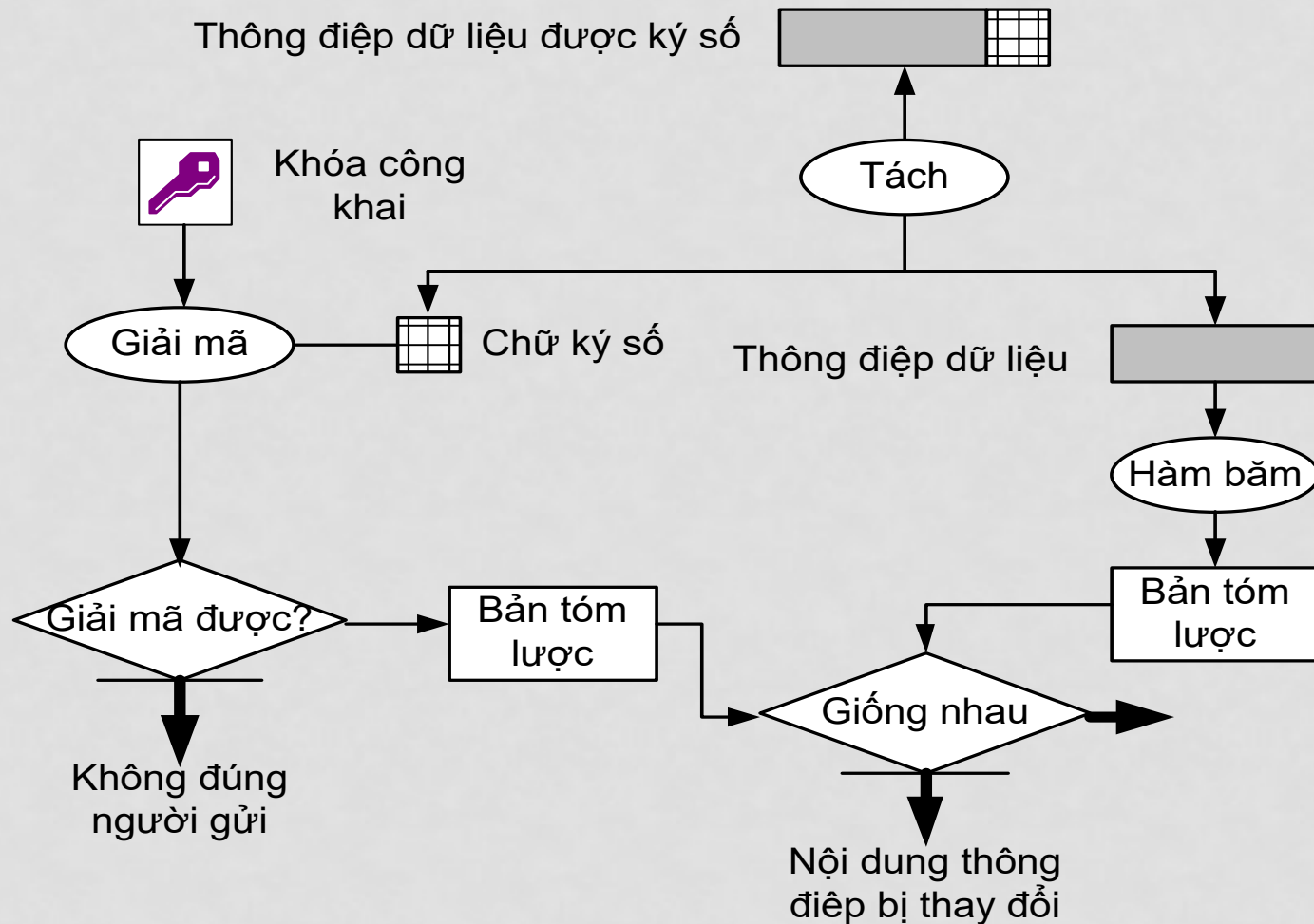
CHỮ KÝ SỐ

- Tạo chữ ký số



CHỮ KÝ SỐ

- Kiểm tra chữ ký số



KẾT CHƯƠNG 1

- Khái niệm:
 - Chứng thực điện tử
 - An toàn thông tin
 - Giao dịch điện tử và chính phủ điện tử
 - Mật mã trong an toàn thông tin
 - Mật mã khóa đối xứng
 - Mật mã khóa công khai
 - Chữ ký số