Hệ mật khóa công khai

Nguyễn Linh Giang
Khoa CNTT, ĐHBK HN

Chương III. Các hệ mật khóa công khai

- Nguyên lý hệ mật khoá công khai
- Sơ đồ trao đổi khoá Diffie-Hellman
- Thuật toán RSA
- Một số hệ mật khóa công khai

Nguyên lý hệ mật khoá công khai

- Đặc điểm
  - Mật mã công khai dựa trên cơ sở của các hàm toán học chứ không phải dựa trên phép thay thế và đổi chỗ như trong phương pháp mã hoá đối xứng.
  - Mã mật công khai là bất đối xứng. Trong cơ chế mã mật khoá công khai sử dụng hai khoá: khoá mật và khoá công khai. Việc sử dụng hai khoá không đối xứng đưa đến những hệ quả sâu sắc trong lĩnh vực an toàn thông tin: tính toàn vẹn, tính xác thực, phân phối khoá.

Nguyên lý hệ mật khoá công khai

- Xuất xứ:
  - Hệ mã mật khoá công khai được phát triển nhằm giải quyết hai vấn đề phức tạp nảy sinh từ phương pháp mã hoá đối xứng:
    - Vấn đề thứ nhất: bài toán phân phối khoá:
      - Duy trì kênh mật để trao đổi khóa;
      - Độ an toàn của hệ mật phụ thuộc vào độ an toàn của khóa $\Rightarrow$ độ an toàn của kênh mật
    - Vấn đề thứ hai: chữ ký điện tử: dấu hiệu đặc trưng cho từng bên trao đổi thông tin
      - Dấu hiệu này không thể bị giả mạo

Nguyên lý hệ mật khoá công khai

- Vấn đề phân phối khóa: trong sơ đồ mã hoá truyền thống, quá trình phân phối khoá đưa ra yêu cầu hai phía tham gia vào trao đổi thông tin:
  - Phải chia sẻ trước khoá (khóa chính), khoá này phải được phân phối bằng một cách nào đó cho họ.:
  - Phải sử dụng trung tâm phân phối khoá KDC: nơi tạo và phân phối khóa phiên
    - Độ an toàn của toàn bộ hệ mật phụ thuộc vào độ an toàn của KDC.

Nguyên lý hệ mật khoá công khai

- Vấn đề thứ hai là chữ ký điện tử:
  - Chữ ký điện tử phải được sử dụng trong các thông điệp điện tử;
  - Phải có hiệu lực tương đương với chữ ký trên giấy.

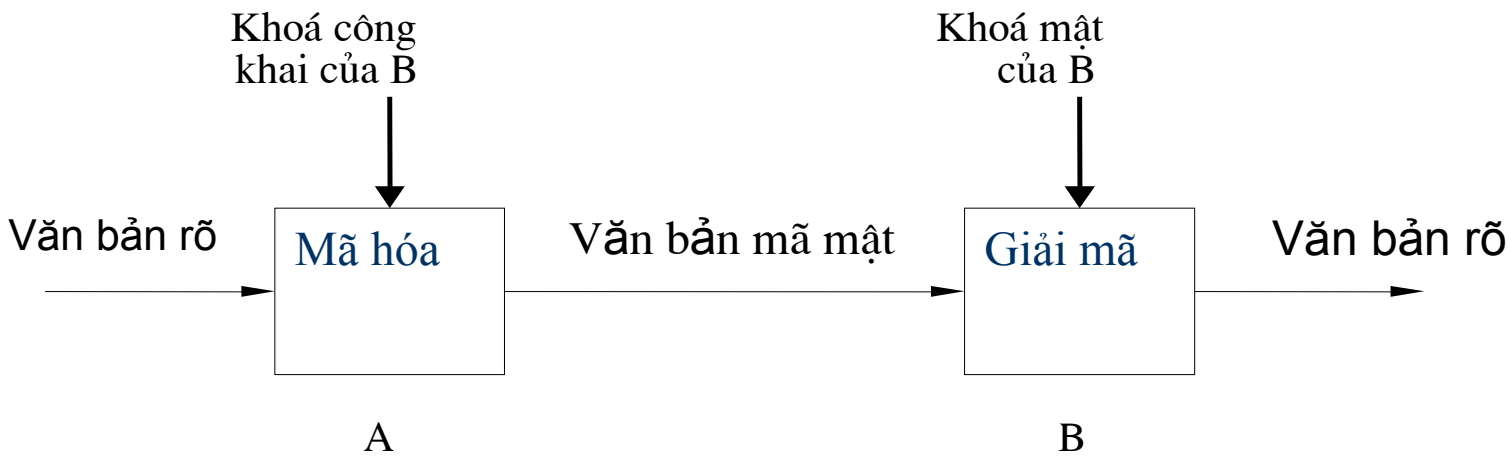
Nguyên lý hệ mật khoá công khai

- Hệ mật khoá công khai.
  - Sơ đồ mã mật khoá công khai sử dụng một khoá để mã hoá và một khoá khác có liên quan để giải mã. Các thuật toán mã hoá và giải mã có một số đặc điểm quan trọng sau:
    - Không thể xác định được khoá giải mã nếu chỉ biết thuật toán mã hoá và khoá mã hoá.
    - Một số hệ mã mật khoá công khai (như RSA) còn cung cấp khả năng sử dụng bất kỳ một khoá trong cặp khoá làm khoá mã hoá thì khoá còn lại sẽ được dùng làm khoá giải mã.

Nguyên lý hệ mật khoá công khai

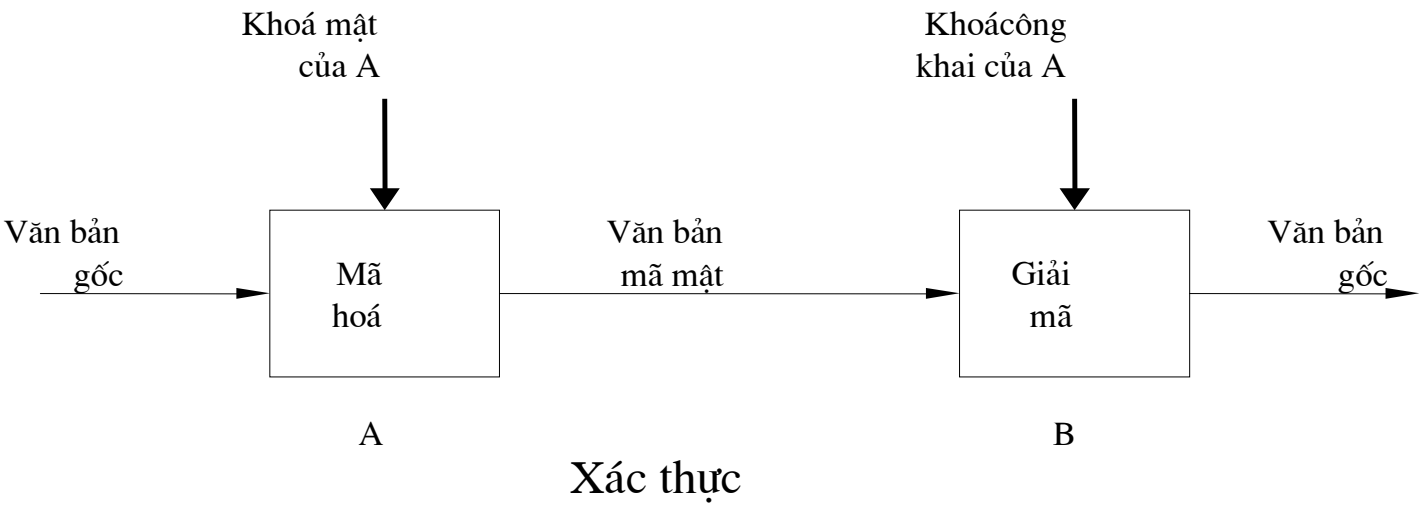
- Sơ đồ mã hoá công khai:
  - Mỗi hệ thống đầu cuối tạo một cặp khoá để mã hoá và giải mã các thông điệp.
  - Mỗi hệ thống đầu cuối công bố một khoá trong cặp khoá còn khoá còn lại được giữ mật.
  - Nếu A muốn gửi thông điệp cho B, A sẽ mã hoá văn bản bằng khoá công khai của B.
  - Khi B nhận được thông điệp, B sẽ giải mã bằng khoá mật. Không một bên thứ ba có thể giải mã được thông điệp vì chỉ có B biết khoá mật của B.

Nguyên lý hệ mật khoá công khai



Sơ đồ đảm bảo tính riêng tư bằng pp mã hóa công khai

Nguyên lý hệ mật khoá công khai



Nguyên lý hệ mật khoá công khai

- Đặc điểm:
  - Mọi bên trao đổi thông tin có truy nhập tới khoá công khai.
  - Khoá mật (khoá riêng tư) được lưu giữ cục bộ tại mỗi bên và không bao giờ được phân phối.
  - Do hệ thống tự quản lý khoá mật nên kênh truyền thông tin tới là mật.
  - Hệ thống có thể thay đổi khoá mật và công bố khoá công khai mới tương ứng để thay thế khoá công khai cũ bất cứ lúc nào.

Nguyên lý hệ mật khoá công khai

	Sơ đồ mã hoá đối xứng	Sơ đồ mã hoá công khai
Hoạt động	1. Cùng một thuật toán và cùng một khoá để mã hoá và giải mã. 2. Người nhận và người gửi phải chia sẻ thuật toán và khoá	1. Một thuật toán để mã hoá, một thuật toán để giải mã sử dụng một cặp khoá. 2. Người gửi và người nhận phải có một cặp khoá của riêng mình.
Bảo mật	1. Khoá phải được giữ mật. 2. Không thể giải mã văn bản nếu không có thông tin bổ sung. 3. Các kiến thức về thuật toán cộng với mẫu của văn bản mật không đủ để xác định khoá.	1. Một trong hai khoá phải được giữ mật. 2. Không thể giải mã văn bản nếu không có thông tin bổ sung. 3. Các kiến thức về thuật toán cộng với mẫu của văn bản mật không đủ để xác định khoá.