**Đỗ Nguyễn Sĩ - DH51502355**

**Nguyễn Ngọc Khánh - DH51502114**

**Nguyễn Văn Trường - DH51502357**

**Trần Quốc Hòa - DH51501877**

Câu 1: Tìm hiểu về cơ chế chữ ký số

* Về căn bản, khái niệm chữ ký số cũng giống như chữ viết tay. Bạn dùng nó để xác nhận lời hứa hay cam kết của mình và sau đó không thể rút lại được. Chữ ký số không đòi hỏi phải sử dụng giấy mực, nó gắn đặc điểm nhận dạng của người ký vào một bản cam kết nào đó.
  + 1 số khái niệm riêng về chữ ký số
    - “PRIVATE KEY” là một khóa trong cặp khóa thuộc hệ thống mã không đối xứng được dùng để tạo chữ ký số.
    - “PUBLIC KEY” là một khóa trong cặp khóa thuộc hệ thống mã không đối xứng, được sử dụng để kiểm tra chữ ký số được tạo bởi khóa bí mật tương ứng trong cặp khóa.
    - “KÝ SỐ” là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu.
    - “NGƯỜI KÝ” là thuê bao dùng đúng khóa bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.
    - “NGƯỜI NHẬN” là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng các chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.
* Để tạo 1 chữ ký số sử dụng các ứng dụng hỗ trợ tạo chữ ký số từ khóa bí mật, khóa bí mật do nhà cung cấp dịch vụ chứng thức chữ ký số công cộng cấp được lưu giữ dưới dạng tệp tin (có mật khẩu khi sử dụng), để an toàn và chống copy khóa bí mật một số nhà cung cấp dịch vụ lưu trữ khóa bí mật trong một thiết bị phần cứng chuyên dụng là USB Token hoặc SmartCard. Thiết bị này sẽ đảm bảo khóa bí mật được lưu trữ an toàn, không thể sao chép hay nhân bản được và cũng không thể bị virus phá hỏng.
* Để giải mã lấy ra được chữ kí số dựa trên công nghệ mã hóa công khai (RSA): mỗi người dùng phải có 1 cặp khóa (keypair) gồm khóa công khai (public key) và khóa bí mật (private key)
  + RSA là một thuật toán mật mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa. Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công cộng. RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.
* 1 số nhà cung cấp chữ ký số
  + Nhà cung cấp chữ ký số VNPT
  + Nhà cung cấp chữ ký số Viettel
  + Nhà cung cấp chữ ký số Newca
  + Nhà cung cấp chữ ký vina (smart sign)
  + Nhà cung cấp chữ ký số điện tử Bkav Ca
  + Nhà cung cấp chữ ký số điện tử Nacencomm (Ca2)
  + Nhà cung cấp chữ ký số điện tử fpt
  + Nhà cung cấp chữ ký số Safe Ca
  + Nhà cung cấp chữ ký số điện tử CKCA
* Các khái niệm liên quan đến chữ ký số
  + Chứng thư số : là một dạng chứng thư điện tử do tổ chức chuyên cung cấp các dịch vụ chứng thực chữ ký số cấp. Chứng thư số có thể được hiểu như một dạng “chứng minh thư” để sử dụng trong môi trường mạng kết nối giữa máy tính và internet.
    - Chứng thư số thường được dùng để thay thế cho các chữ ký thông thường, ký trên các văn bản và tài liệu như: excel, pdf, word . Những tài liệu này các doanh nghiệp dùng để nộp thuế qua mạng , kê khai hải quan và thực hiện các giao dịch điện tử có liên quan khác.
  + Phong bì số : là kết hợp được ưu điểm của cả khóa đối xứng(Symmetric Key) and khóa bất đối xứng (Asymmetric Key). Nội dung được mã hóa và giải mã bằng khóa đối xứng và khóa đối xứng được mã hóa bằng public key chuyển đến cho người nhận trong một khối gọi nôm na là phong bì số.

Câu 2: Làm thế nào để cấp chữ kí số nội bộ