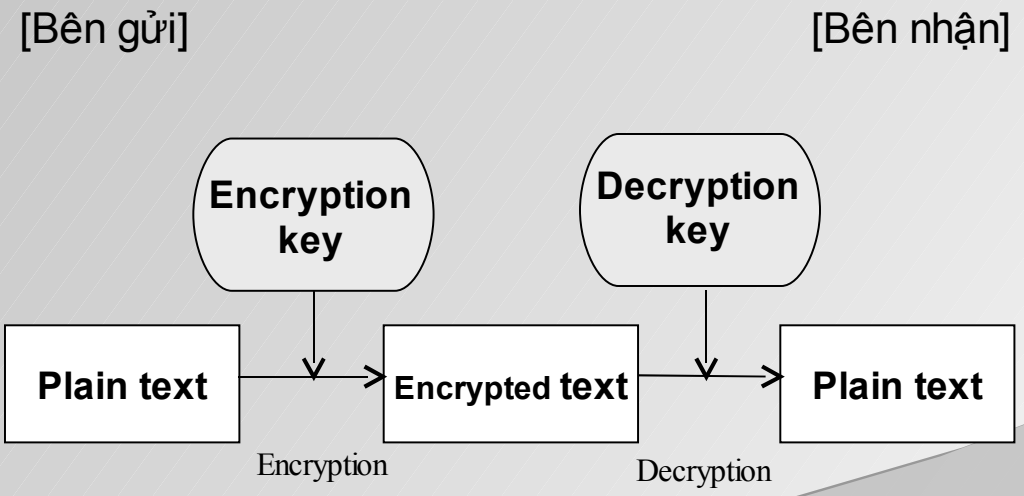
Chương 6 : An ninh và chuẩn hóa thông tin

6.1 An ninh thông tin

- Bảo vệ thông tin
- Virus máy tính
- Tội phạm máy tính

6.1.1 Bảo vệ thông tin

- Các phương pháp bảo vệ : Mã hóa , xác thực, quản lý truy cập.
- Mã hóa : biến đổi thông tin để người thứ ba không xem được.



6.1.1 Bảo vệ thông tin

- Có hai loại mã hóa:
  - Mã hóa riêng – Private Key Cryptography. Dùng chung một khóa cho cả mã hóa và giải mã, còn được gọi là mã hóa đối xứng. VD : DES, FEAL..
  - Mã hóa công khai – Public Key Cryptography. Sử dụng một cặp khóa, một khóa công khai để mã và môt khóa bí mật để giải mã. Loại mã hóa này còn được gọi là mã hóa bất đối xứng. VD : RSA

6.1.1 Bảo vệ thông tin

- Xác thực : cơ chế xác nhận người dùng đó là hợp lệ, tin cậy.
- Có ba loại xác thực:
  - Xác thực thực thể: xác nhận đối tượng đang giao tiếp là hợp lệ. Thông thường cơ chế xác thực này yêu cầu người dùng cung cấp định danh và mật khẩu.
  - Xác thực thông điệp : xác nhận thông điệp truyền đi không bị sai sót thông qua các bit dữ liệu kiểm tra.
  - Chữ ký điện tử : công nghệ đảm bảo tính hợp lệ của tài liệu. Thường sử dụng phương pháp mã hóa công khai.

6.1.1 Bảo vệ thông tin

- Quản lý truy cập : ngăn cản truy nhập trái phép đến tài nguyên trong một hệ thống máy tính.
- Định danh và mật khẩu cũng được sử dụng để cấp quyền sử dụng tài nguyên.
- Các phương pháp quản lý truy cập:
  - Qua trí nhớ người dùng : mật khẩu…
  - Qua thiết bị an ninh : Thẻ ID, Chip ID, Thẻ quang học…
  - Qua đặc điểm người dùng : vân tay, giọng nói, nhãn cầu, bàn tay, chữ ký…

6.1.2 Virus máy tính

- Virus máy tính : chương trình máy tính độc hại, xâm nhập vào máy tính thông qua mạng, các thiết bị lưu trữ…để phá hoại, thay đổi hoặc lấy cắp thông tin.
- Virus tự nhân bản và phát tán sang máy khác cũng theo con đường mạng và thiết bị lưu trữ.

6.1.2 Virus máy tính

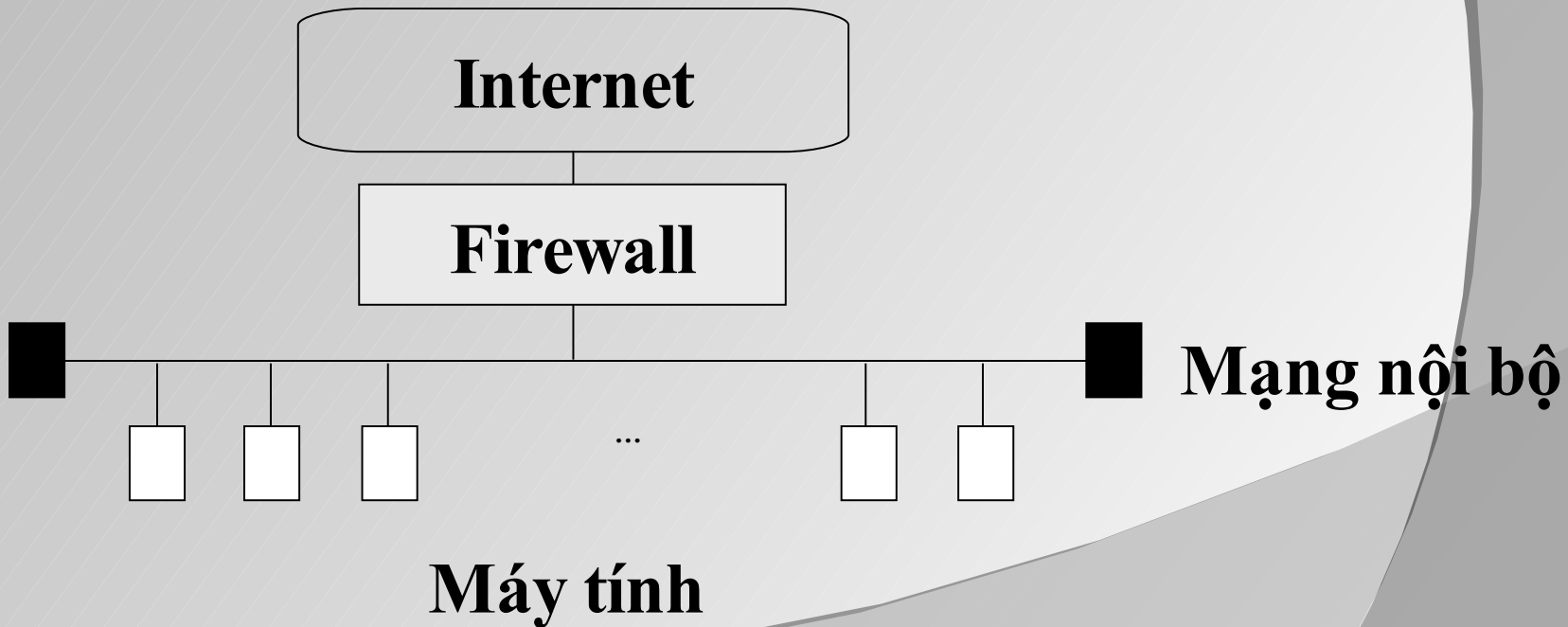
- Virus thường gồm ít nhất một trong các tính năng sau:
  - Tự lây lan : sao chép chính nó và lây nhiễm sang các máy tính khác.
  - Tự lẩn tránh : virus thường tự ẩn đi và kích hoạt khi có điều kiện thích hợp, thí dụ đến ngày tháng nào đó, sau khoảng thời gian bao lâu, số lượng tiến trình…
  - Phá hoại : virus phá hủy dữ liệu, thực hiện những hành động không được phép…

6.1.2 Virus máy tính

- Vắc xin (phần mềm vắc xin): phát hiện và loại bỏ virus bằng một cơ sở dữ liệu chứa mẫu của các virus đã biết.
- Phòng chống virus:
  - Cài đặt chương trình phòng chống virus.
  - Không sao chép phần mềm bất hợp pháp.
  - Không thực hiện những chương trình đáng ngờ.
  - Thiết đặt mật khẩu và quản lý truy cập.
  - Thực hiện sao lưu định kì.
  - Không chia sẻ ổ đĩa.
  - Không mở e-mail đáng ngờ.

6.1.2 Virus máy tính

- Tường lửa : hệ thống bảo vệ mạng nội bộ khỏi những truy nhập trái phép từ bên ngoài.



6.1.3 Xâm phạm máy tính

- Xâm phạm máy tính : hành động truy nhập vào một hệ thống thông tin với mục đích xấu. Thí dụ : phá hủy dữ liệu, phát tán virus.
- Các hành động xâm phạm máy tính bao gồm:
  - Thay đổi hệ thống ngân hàng trực tuyến.
  - Hack vào một hệ thống máy tính từ xa thông qua mạng.
  - Đặt bẫy trong một miền công cộng.

6.1.3 Xâm phạm máy tính

- Các hành động phá hoại : Falsification, Destruction, Leak, Tapping, Disguise.
- Làm sai lệch thông tin – Falsification:
  - Hành động có chủ ý làm sai lệch, thay đổi nội dung tài liệu, thay thế phương tiện lưu trữ, ghi lại dữ liệu, xóa dữ liệu…
  - Phương pháp phát hiện Falsification là xác thực thông điệp – message authentication.

6.1.3 Xâm phạm máy tính

- Phá hủy – Destruction:
  - Hành động xóa dữ liệu quan trọng, chương trình hoặc vô hiệu hóa các thiết bị của hệ thống, các thiết bị lưu trữ bằng cách can thiệp vật lý.
  - Bao gồm : Trojan, bom logic, bom thư điện tử.
  - Trojan : Ẩn trong một chương trình bình thường, thực hiện các chức năng không được phép trong khi chương trình đó vẫn chạy bình thường. Khi một vài điều kiện xảy ra, trojan có thể phá hủy toàn bộ dữ liệu, lấy cắp định danh và mật khẩu của người dùng…
  - Phát hiện Trojan : sao lưu cẩn thận chương trình gốc và so sánh với chương trình đáng ngờ.

6.1.3 Xâm phạm máy tính

- Phá hủy – Destruction (tiếp) :
  - Bom logic : ứng dụng sử dụng phương pháp của Trojan, ẩn mình trong hệ thống và phá hủy hệ thống khi một vài điều kiện thỏa mãn.
  - Bom thư điện tử : hành động gửi một lượng lớn thư điện tử có kích thước lớn trong khoảng thời gian ngắn đến một người cụ thể. Mục đích là phá hỏng hệ thống thư điện tử.

6.1.3 Xâm phạm máy tính

- Lộ thông tin – Leak
  - Lấy trộm hoặc sao chép dữ liệu từ một hệ thống thông tin.
  - Các phương pháp : đặt bộ phát tín hiệu vào đầu ra của thiết bị, trộn dữ liệu mật vào một bảo báo cáo, mã hóa dữ liệu mật sang một dạng khác…
  - **Scaveging** là một loại leak. Lấy trộm thông tin sau khi công việc đã hoàn tất, có thể từ thùng rác trên đĩa cứng hoặc trong bộ nhớ.

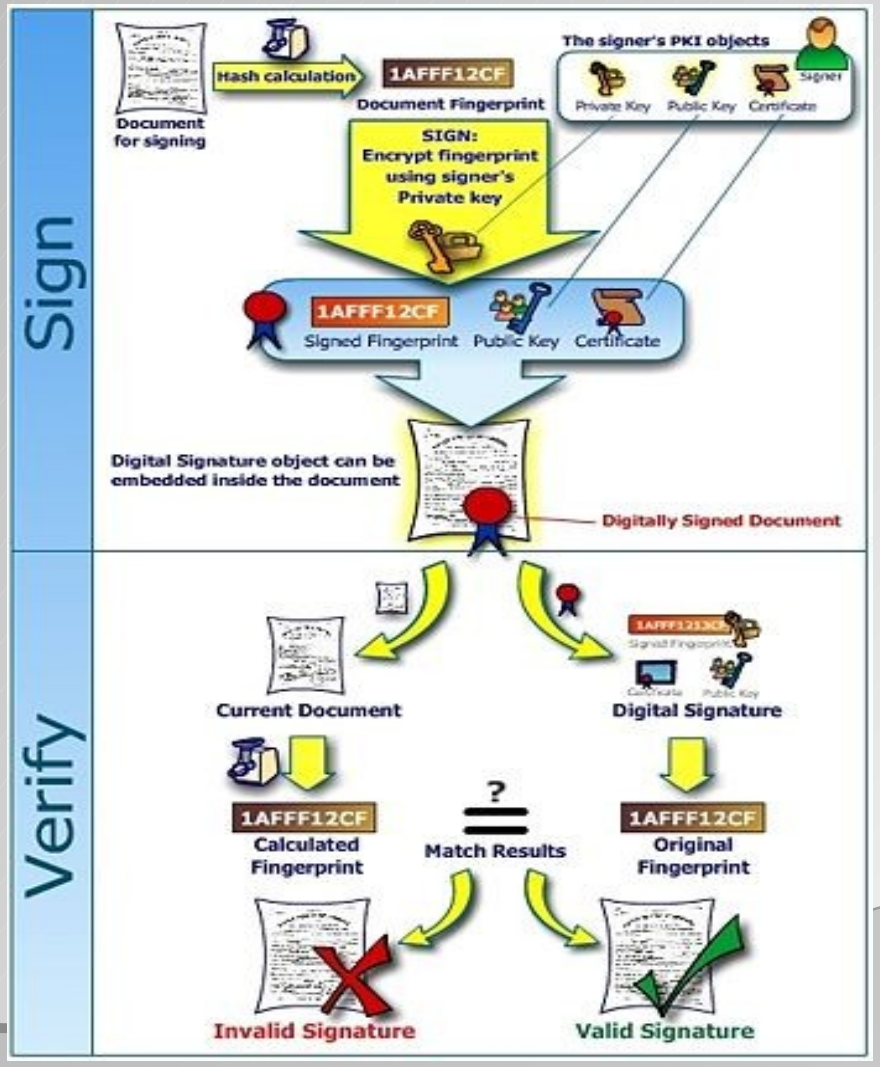
6.1.3 Xâm phạm máy tính

- Nghe lén thông tin :
  - Chặn dữ liệu trên đường truyền mạng và lấy cắp thông tin hoặc truy cập hệ thống bất hợp pháp.
  - Đối tượng của nghe lén không chỉ có dữ liệu máy tính mà có thể còn là dữ liệu âm thanh.
  - Mã hóa là phương pháp hiệu quả chống lại nghe lén.

6.1.3 Xâm phạm máy tính

- Mạo danh
  - Lấy trộm định danh và mật khẩu của người có thẩm quyền trên mạng và sử dụng định danh đó để lấy thông tin mật mà chỉ người đó mới có quyền truy nhập.
  - Chữ ký điện tử là phương pháp hữu hiệu để ngăn chặn tình trạng mạo danh

6.1.3 Xâm phạm máy tính



6.2 Chuẩn hóa

- Các tổ chức chuẩn hóa, chuẩn hóa phát triển và chuẩn hóa môi trường.
- Chuẩn hóa dữ liệu.
- Chuẩn hóa phần mềm và trao đổi dữ liệu.

6.2.1 Các tổ chức chuẩn hóa, chuẩn hóa phát triển và chuẩn hóa môi trường

- Các tổ chức chuẩn hóa

Tên	Diễn giải
ISO	***International Organization for Standardization*** Tổ chức quốc tế quy định và hợp nhất các chuẩn trong lĩnh vực liên quan đến công nghiệp. Trong mỗi lĩnh vực có các ủy ban kỹ thuật (Technical Comitte) trong đó lại có các ủy ban con và dưới cùng là các nhóm làm
ITU	***International Telecommunications Union*** Tổ chức quốc tế chuẩn hóa các công nghệ viễn thông cũng như giới thiệu và chuẩn hóa các chuẩn quốc tế về truyền thông. ITU-R chịu trách nhiệm về viễn thông, ITU-R chịu trách nhiệm về sóng vô tuyến và các hệ thống không dây.
ANSI	***American National Standards Institute*** Tổ chức phi lợi nhuận thiết lập các chuẩn công nghiệp ở Mỹ và là thành viên của ISO

6.2.1 Các tổ chức chuẩn hóa, chuẩn hóa phát triển và chuẩn hóa môi trường

- Bộ tiêu chuẩn ISO 9000 : Tập hợp các chuẩn quốc tế về hệ thống quản lý chất lượng cho công ty .

ISO 9000		Các hệ thống quản lý chất lượng – Các tiêu chuẩn cơ bản Các hệ thống quản lý chất lượng – Các yêu cầu
	ISO 9001	Trách nhiệm quản lý (tập trung vào khách hàng, chính sách chất lượng, phê duyệt...) Quản lý tài nguyên (cung cấp tài nguyên, nguồn nhân lực, môi trường làm việc...) Hiện thực sản phẩm (lập kế hoạch hiện thực hóa sản phẩm, các quá trình liên quan đến khách hàng, thiết kế và phát triển...) Đo đạc, phân tích và cải tiến (theo dõi và đo đạc, điều khiển các sản phẩm không phù hợp…)
	ISO 9004	Các hướng dẫn để cải thiện hiệu năng

6.2.1 Các tổ chức chuẩn hóa, chuẩn hóa phát triển và chuẩn hóa môi trường

- Bộ tiêu chuẩn ISO 14000
  - Tập hợp các chuẩn quốc tế về quản lý bảo vệ môi trường.
  - Đó là tập hợp các hướng dẫn để xác định các vấn đề ảnh hưởng đến môi trường toàn cầu, như mức độ tiêu thụ năng lượng, rác rải công nghiệp…

6.2.2 Chuẩn hóa dữ liệu

- Dữ liệu truyền đi giữa các hệ thống phải có chung một khuôn dạng. Khuôn dạng ký tự, hình ảnh, video, tài liệu…
- Mã ký tự : Một con số được gán cho mỗi ký tự hoặc biểu tượng phục vụ cho mục đích xử lý trên máy tính.Ví dụ : ASCII, EUC, Unicode…

Loại mã	Giải thích
EBCDIC	Extended Binary Coded Decimal Interchange Code Bộ mã được IBM đưa ra để sử dụng cho mục đích chung Một tập 8 bit biểu diễn một ký tự.
Unicode (UCS-2)	Bộ mã biểu diễn tất cả các ký tự của các ngôn ngữ trên thế giới. Mỗi ký tự biểu diễn bằng hai byte.

6.2.2 Chuẩn hóa dữ liệu

- Các tệp hình ảnh :
  - Hình ảnh được số hóa và lưu lại dưới dạng các tệp nhị phân.
  - Có nhiều định dạng lưu lại ảnh : JPG, BMP, PNG, GIF…

Định dạng	Giải thích
JPEG	Joint Photographic Experts Group: Một tổ chức chung của ISO và ITU-T nghiên cứu mã hóa ảnh tỉnh, phương pháp nén/giải nén ảnh.
GIF	Graphic Interchange Format: Định dạng ảnh phát triển bởi CumpuServe, một công ty dịch vụ trực tuyến lớn ở Mỹ. Định dạng này thích hợp với ảnh đơn sắc hoặc có ít hơn 256 màu.
BMP	Định dạng lưu ảnh dưới dạng dữ liệu bitmap được sử dụng trong Windows.
TIFF	Target Image File Format: Biểu diễn dữ liệu bằng các thẻ trong khối dữ liệu trong tệp. Định dạng dữ liệu cũng được chỉ ra trong tệp này.

6.2.2 Chuẩn hóa dữ liệu

- Nén ảnh động (video) :
  - Giảm kích thước dữ liệu video.
  - Chuẩn nén rất phổ biến hiện nay là MPEG.
  - MPEG – Moving Picture Experts Group, một tổ chức cấp con của JCT1.
  - Gồm các chuẩn con MPEG-1, MPEG-2, MPEG-4…
  - Được sử dụng rộng rãi trong các thiết bị giải trí gia đình : VCD , DVD, SVCD…

6.2.2 Chuẩn hóa dữ liệu

- Định dạng tài liệu:
  - Các tài liệu cần chuẩn hóa khuôn dạng để có thể trao đổi dễ dàng.
  - Thông thường phân biệt dựa vào phần mở rộng của tên tệp và phần header của tệp.

Định dạng	Giải thích
SGML	Standard Generalized Markup Language Ngôn ngữ diễn tả cấu trúc ngữ nghĩa là logic của tài liệu. Có thể sử dụng tài liệu như một cơ sở dữ liệu
XML	eXtensible Markup Language Ngôn ngữ ra đời sau HTML với tập mở rộng tính năng của SGML sử dụng trên Web. Người dùng có thể tự định nghĩa các thẻ của riêng họ.
HTML	HyperText Markup Language. Ngôn ngữ sử dụng để tạo lên các trang Web trên Internet. Các thẻ trong "<>" mô tả kích thước, màu sắc chữ và các siêu liên kết.
TeX	Định dạng sử dụng trong các tài liệu với các công thức toán học phức tạp và công thức hóa học.
CSV	Comma Separated Value Format Mỗi mục dữ liệu được kết thúc bằng dấu phảy, sử dụng chủ yếu để ghi dữ liệu từ cơ sở dữ liệu và bảng tính.
PDF	Portable Document Format Định dạng tài liệu điện tử phát triển bởi Adobe Systems . Tài liệu dạng này có thể được trao đổi mà không phụ thộc vào loại máy tính và nền tảng phần mềm.

6.2.3 Chuẩn hóa trao đổi dữ liệu và phần mềm

- Chuẩn hóa trao đổi dữ liệu : chuẩn hóa dữ liệu khi trao đổi giữa các công ty

Chuẩn	Giải thích
EDI	Electronic Data Interchange (giao dịch điện tử, trao đổi dữ liệu điện tử)
CALS	Commerce At Light Speed
EC	Electronic Commerce
STEP	Standard for the Exchange of Product Model Data, ISO 10303 standard Chuẩn quốc tế về trao đổi dữ liệu mô hình sản phẩm.

6.2.3 Chuẩn hóa trao đổi dữ liệu và phần mềm

- Hệ thống mở :
  - Hệ thống máy tính được xây dựng bằng việc chuẩn hóa các đặc tả hệ thống.
  - Phần cứng và phần mềm có thể hoạt động nhịp nhàng mà không phụ thuộc vào nhà sản xuất nào.
  - Các hệ xử lý phân tán là những hệ thống mở. Phần cứng và phần mềm đều đã được chuẩn hóa.

6.2.3 Chuẩn hóa trao đổi dữ liệu và phần mềm

- Chuẩn hóa phần mềm : chuẩn hóa các quy trình xây dựng phát triển, vận hành , bảo trì phần mềm.

Tên chuẩn	Giải thích
CORBA	Common Object Request Broker Architecture Đặc tả chia sẻ dữ liệu mà nhờ đó các đối tượng có thể trao đổi thông điệp trong môi trường hệ phân tán. Chuẩn này được OMG đề xuất (Object Management Group).
EJB	JavaBeans Các đặc tả chuẩn để xây dựng ứng dụng hướng đối tượng phân tán Java. Nó cho phép kết hợp các thành phần bằng những công cụ của các nhà sản xuất kháu nhau. Chuẩn này tương thích với CORBA.
RFC	Request for Comments Một nhóm các tài liệu kỹ thuật và nhận xét của IETF. Các tài liệu này có thể dễ dàng tìm thấy trên Internet. TCP/IP và các giao thức liên quan được xây dựng nhờ RFC.
OMG	Object Management Group Một tổ chức phi lợi nhuận có mục đích chuẩn hóa và phổ thông công nghệ hướng đối tượng.