MỤC LỤC

CHƯƠNG 1 TỔNG QUAN VỀ AN NINH MẠNG

1.1 Đối tượng và phương pháp nghiên cứu

1.1.1 Bảo mật hệ thống thông tin

Thông tin cho có giá trị cao khi đảm bảo tính chính xác và kịp thời, hệ thống chỉ có thể cung cấp các thông tin có giá trị thực sự khi các chức năng của hệ thống đảm bảo hoạt động đúng đắn. Mục tiêu của việc đảm bảo an toàn an ninh cho hệ thống thông tin là đưa ra các giải pháp và ứng dụng các giải pháp này vào hệ thống để loại trừ hoặc giảm bớt các nguy hiểm. Hiện nay các cuộc tấn công ngày càng tinh vi, gây ra mối đe dọa tới sự an toàn thông tin. Các cuộc tấn công có thể đến từ nhiều hướng theo các cách khác nhau, do đó cần phải đưa ra các chính sách và biện pháp đề phòng cần thiết.

1.1.2 Các nguy cơ đe dọa

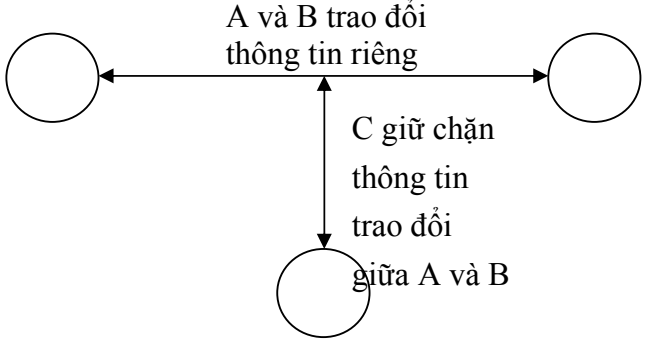
Có rất nhiều nguy cơ ảnh hưởng đến sự an toàn của một hệ thống thông tin. Các nguy cơ này có thể xuất phát từ các hành vi tấn công trái phép bên ngoài hoặc từ bản thân các lỗ hổng bên trong hệ thống.

Tất cả các hệ thống đều mang trong mình lỗ hổng hay điểm yếu. Nhìn một cách khái quát, ta có thể phân ra thành các loại điểm yếu chính sau:

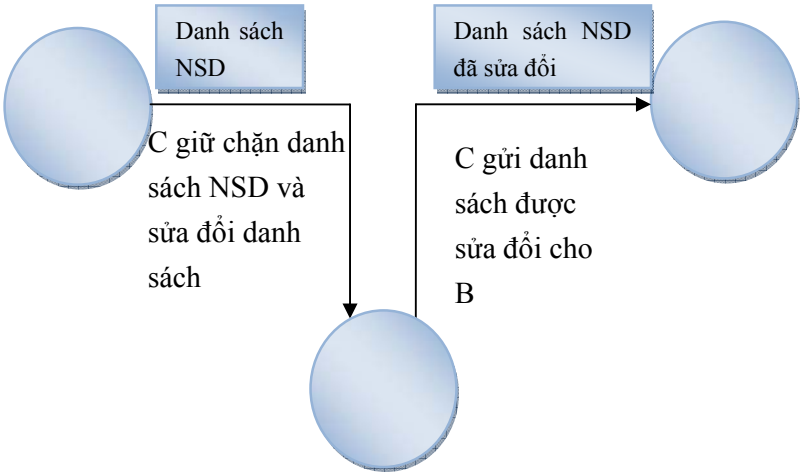
- ✓ ***Phần mềm***: Việc lập trình phần mềm đã ẩn chứa sẵn các lỗ hổng. Theo ước tính cứ 1000 dòng mã sẽ có trung bình từ 5-15 lỗi, trong khi các Hệ điều hành được xấy dựng từ hàng triệu dòng mã(Windows: 50 triệu dòng mã).
- ✓ ***Phần cứng***: Lỗi thiết bị phần cứng như Firewall, Router, . . .
- ✓ ***Chính sách***: Đề ra các quy định không phù hợp, không đảm bảo an ninh, ví dụ như chính sách về xác thực, qui định về nghĩa vụ và trách nhiệm người dùng trong hệ thống.
- ✓ ***Sử dụng***: Cho dù hệ thống được trang bị hiện đại đến đâu do những do con người sử dụng và quản lý, sự sai sót và bất cẩn của người dùng có thể gây ra những lỗ hổng nghiêm trọng.

1.1.3 Một số ví dụ về bảo vệ an toàn thông tin

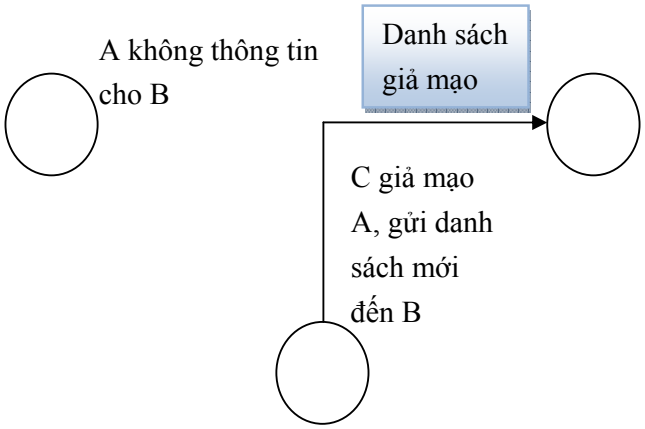
- ✓ ***Truyền file***:



✓ ***Trao đổi thông điệp***



✓ ***Giả mạo***



Qua thực tế người ta nhận thấy rằng, vấn đề bảo mật trong hệ thống mạng hay liên mạng là một bài toán rất phức tạp, vì:

- Không tồn tại phương pháp thích hợp cho mọi trường hợp
- Các cơ chế bảo mật luôn đi đôi với các biện pháp đối phó
- Lựa chọn những giải pháp cụ thể đối với từng ngữ cảnh cụ thể.

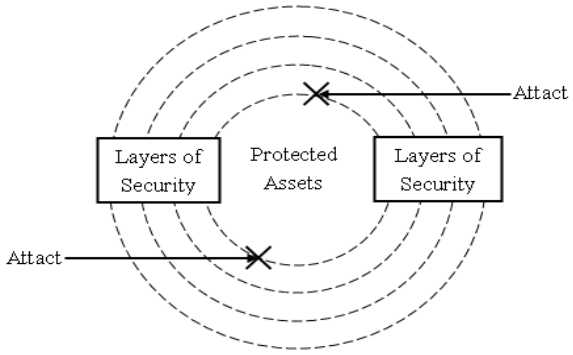
1.2 Các dịch vụ, cơ chế an toàn an ninh thông tin và các dạng tấn công vào hệ thống mạng.

1.2.1 Phân loại các dịch vụ an toàn an ninh, bao gồm:

- Bảo mật riêng tư
- Xác thực
- Toàn vẹn thông tin
- Tính không thể từ chối
- Kiểm soát truy cập
- Tính sẵn sàng

1.2.2 Các cơ chế an toàn an ninh

- Trên thực tế không tồn tại một cơ chế duy nhất nào có thể đảm bảo an toàn thông tin cho mọi hệ thống.
- Để đảm bao an toàn an ninh cho hệ thống thông tin người ta sử các kỹ thuật mã hóa: Mã đối xứng, mã công khai
- Sử dụng Firewall, hệ thống phát hiện xâm nhập - IDS , và các biện pháp phối hợp khác.



Hệ thống phòng thủ theo chiều sâu

1.2.3 Các dạng tấn công, được chia làm 2 loại:

- Tấn công chủ động
- Tấn công thụ động

1.3 Các dạng tấn công

Đối với các hành vi tấn công từ bên ngoài, ta có thể chia thành hai loại là: tấn công thụ động và tấn công chủ động. "Thụ động" và "chủ động" ở đây được hiểu theo nghĩa có can thiệp vào nội dung và vào luồng thông tin trao đổi hay không. Tấn công "thụ động" chỉ nhằm đạt mục tiêu cuối cùng là nắm bắt được thông tin, không biết được nội dung nhưng cũng có thể dò ra được người gửi, người nhận nhờ vào thông tin điều khiển giao thức chứa trong phần đầu của các gói tin. Hơn thế nữa, kẻ xấu còn có thể kiểm tra được số lượng, độ dài và tần số trao đổi để biết được đặc tính trao đổi của dữ liệu.

Một số hình thức tấn công điển hình:

a) Các hành vi dò quét:

Bất cứ sự xâm nhập vào một môi trường mạng nào đều bắt đầu bằng cách thăm dò để tập hợp thông tin người dùng, cấu trúc hệ thống bên trong và điểm yếu bảo mật. Việc thăm dò được thăm dò theo các bước thăm dò thụ động(thu thập các thông tin được công khai) và thăm dò chủ động(sử dụng các công cụ để

tìm kiếm thông tin trên máy tính của nạn nhân). Các công cụ dò quét được hacker chuyên nghiệp thiết kế và công bố rộng rãi trên Internet. Các công cụ thường hày dùng: Nmap, Essential Network tools… thực hiện các hành động Ping Sweep, Packet Sniffer, DNS Zone Transfer…

b) Tấn công từ chối dịch vụ(Denial Service Attacks):

Đây là kiểu tấn công khó phòng chống nhất và trên thế giới vẫn chưa có cách phòng chống triệt để. Nguyên tắc chung của cách tấn công này là hacker sẽ gửi liên tục nhiều yêu cầu phục vụ đến máy nạn nhân. Máy bị tấn công sẽ phải trả lời tất cả các yêu cầu này. Khi yêu cầu gửi đến quá nhiều, máy bị tấn công sẽ không phục vụ kịp thời dẫn đến việc đáp ứng các yêu cầu của các máy hợp lệ sẽ bị chậm trễ, thậm chí ngừng hẳn hoặc có thể cho phép hacker nắm quyền điều khiển.

c) Các hành vi khai thác lỗ hổng bảo mật:

Các hệ điều hành, cơ sở dữ liệu, các ứng dụng luôn luôn có những điểm yếu xuất hiện hàng tuần thậm chí hàng ngày. Những điểm yếu này thường xuyên được công bố rộng rãi trên nhiều website về bảo mật. Do vậy các yếu điểm của hệ thống là nguyên nhân chính của các tấn công, một thống kê cho thấy hơn 90% các tấn công đều dựa trên các lỗ hổng bảo mật đã được công bố.

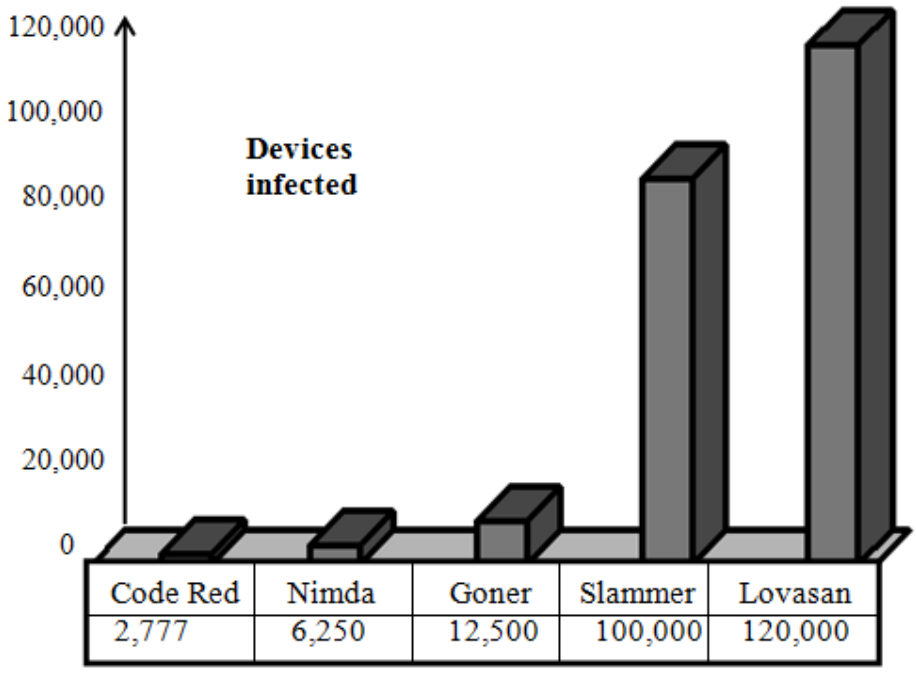
Đối với một hệ thống mạng có nhiều máy chủ máy trạm, việc cập nhật các bản vá lỗ hổng bảo mật là một công việc đòi hỏi tốn nhiều thời gian và khó có thể làm triệt để. Và do đó, việc tồn tại các lỗ hổng bảo mật tại một số điểm trên mạng là một điều chắc chắn. Người ta định nghĩa *Tấn công Zero-Day* là các cuộc tấn công diễn ra ngay khi lỗi được công bố và chưa xuất hiện bản vá lỗi. Như vậy kiểu tấn công này rất nguy hiểm vì các hệ thống bảo mật thông thường không thể phát hiện ra.

d) Các tấn công vào ứng dụng(Application-Level Attacks):

Đây là các tấn công nhằm vào các phần mềm ứng dụng mức dịch vụ. Thông thường các tấn công này, nếu thành công, sẽ cho phép kẻ xâm nhập nắm được quyền điều khiển các dịch vụ và thậm chí cả quyền điều khiển máy chủ bị tấn công.

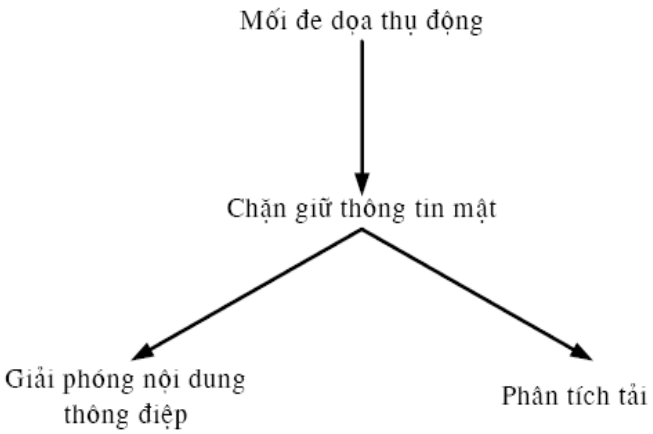
Số lượng các vụ tấn công liên tục tăng trong khi hình thức tấn công theo kiểu dựa trên điểm yếu của con người (tấn công kiểu Sophistication) lại giảm. Rõ ràng các hình thức tấn công vào hệ thống máy tính hiện nay ngày càng đa dạng

và phức tạp với trình độ kỹ thuật rất cao. Ngoài ra quá trình tấn công ngày càng được tự động hóa với những công cụ nhỏ được phát tán khắp nơi trên mạng



Số lượng máy bị tấn công ngày càng tăng (Nguồn: IDC2002)

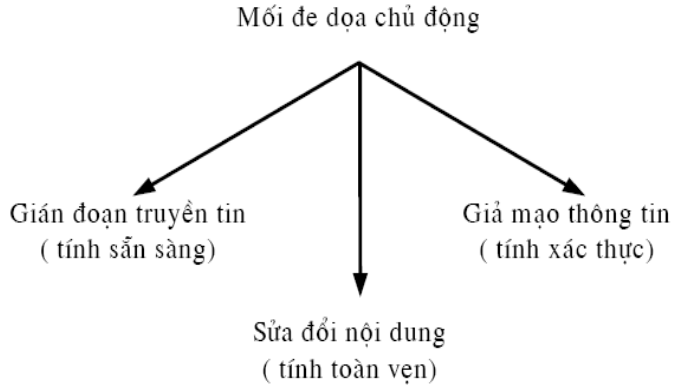
- *Các dạng tấn công thụ động:*



- Giải phóng nội dung của thông điệp: ngăn chặn đối phương thu và tìm hiểu nội dung của thông tin truyền tải.
- Phân tích tải: Khi phân tích tải đối phương có thể xác định được vị trí của các máy tham gia vào quá trình truyền tin; tần suất và kích thước bản tin.

Dạng tấn công thụ động rất khó phát hiện vì không làm thay đổi dữ liệu, với dạng tấn công này người ta quan tâm đến vấn để ngăn chặn hơn là vấn đề phát hiện.

- ✓ *Các dạng tấn công chủ động:*



- Giả danh
- Phát lại
- Thay đổi nội dung thông điệp
- Từ chối dịch vụ

Dạng tấn công chủ động rất khó có thể ngăn chặn tuyệt đối. Vì vậy yêu cầu phải bảo vệ vật lý mọi đường truyền thông tại mọi thời điểm. Mục tiêu an toàn của dạng tấn công này là có thể phát hiện và phục hồi lại thông tin từ mọi trường hợp bị phá hủy và làm trễ.

1.4 Các dịch vụ an toàn an ninh.

Các dịch vụ an toàn an ninh của hệ thống thông tin phải đảm bảo các yêu cầu sau:

- ✓ ***Đảm bảo tính tin cậy***: Thông tin không thể bị truy nhập trái phép bởi những người không có thẩm quyền.
- ✓ ***Đảm bảo tính nguyên vẹn***: Thông tin không thể bị sửa đổi, bị làm giả bởi những người không có thẩm quyền.
- ✓ ***Đảm bảo tính sẵn sàng***: Thông tin luôn sẵn sàng để đáp ứng sử dụng cho người có thẩm quyền.
- ✓ ***Đảm bảo tính không thể từ chối***: Thông tin được cam kết về mặt pháp luật của người cung cấp.
- ✓ ***Đảm bảo tính riêng tư***: Bảo vệ dữ liệu được truyền tải khỏi các tân công thụ động.

✓ ***Kiểm soát truy cập***: Cung cấp khả năng giới hạn và kiểm soát các truy cập tới các máy chủ hoặc tới các ứng dụng thông qua đường truyền tin.

1.5 Các mô hình an toàn an ninh mạng.

1.5.1 Mô hình an toàn mạng: Bài toán an toàn an ninh thông tin mạng nảy sinh khi:

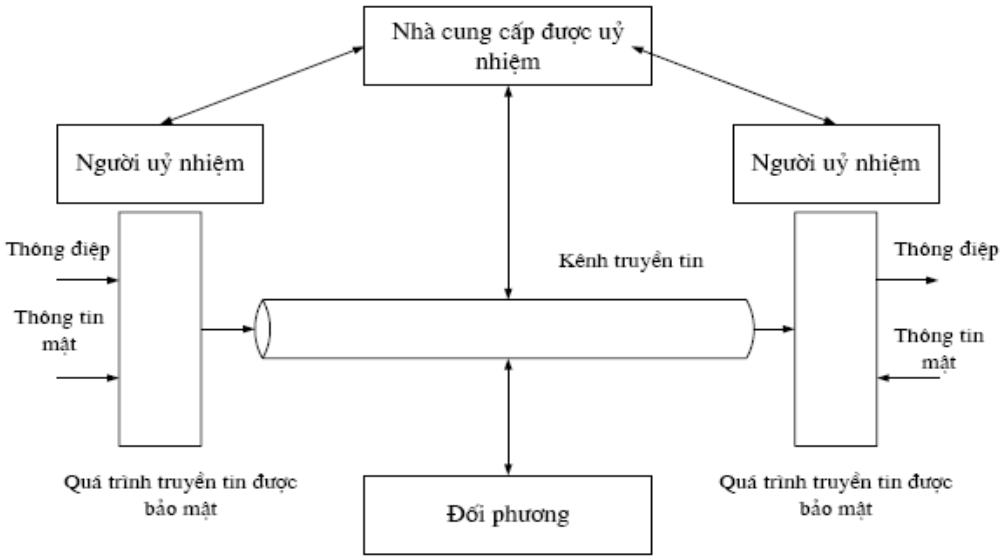
✓ Cần thiết phải bạo vệ quá trình truyền tin khỏi các hành động truy cập trái phép

✓ Đảm bảo tính riêng tư và tính toàn vẹn

✓ Đảm bảo tính xác thực, . . .

Mô hình an toàn mạng yêu cầu:

- Thiết kế một giải thuật thích hợp cho việc chuyển đổi liên quan đến an toàn
- Tạo ra thông tin bí mật (khóa) đi kèm với giải thuật
- Phát triển các phương pháp phân bổ và chia sẻ thông tin bí mật
- Đặc tả một giao thức sử dụng bởi hai bên gửi và nhận dựa trên giải thuật an toàn và thông tin bí mật, làm cơ sở cho một dịch vụ an toàn



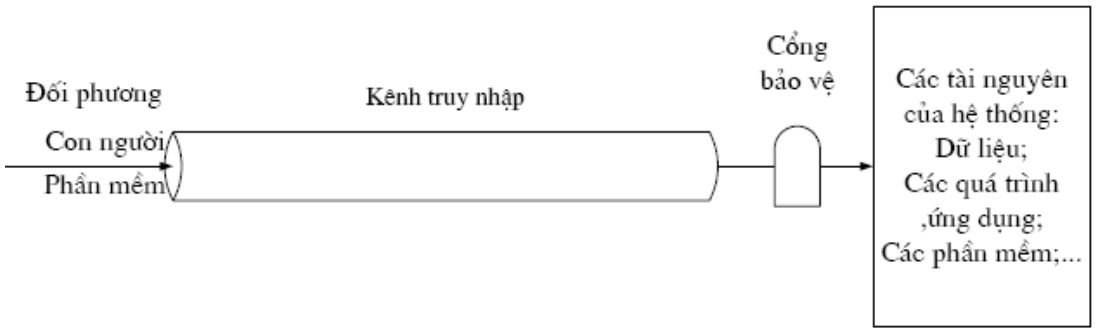
Mô hình truyền tin an toàn

1.5.2 Mô hình an toàn truy cập mạng:

Mô hình này yêu cầu:

- Lựa chọn các chức năng gác cổng thích hợp để định danh người dùng

- Cài đặt các điều khiển an toàn để đảm bảo chỉ những người dùng được phép mới có thể truy nhập được vào các thông tin và tài nguyên tương ứng.
- Các hệ thống máy tính đáng tin cậy có thể dùng để cài đặt mô hinh này



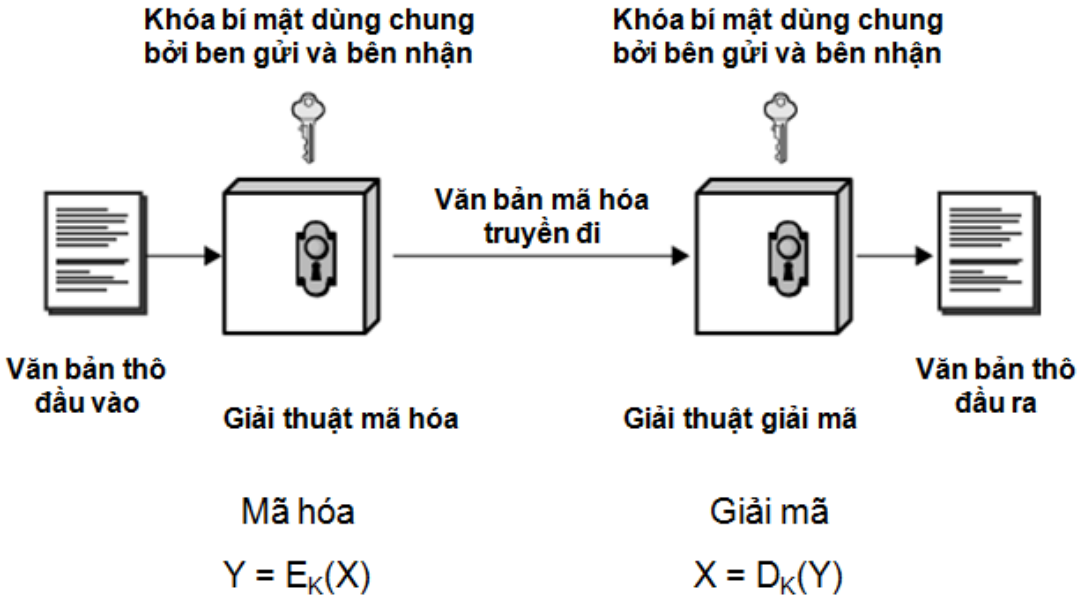
Cần nhấn mạnh một thực tế rằng không có một hệ thống nào an toàn tuyệt đối cả. Bởi vì bất kỳ một hệ thống bảo vệ nào dù hiện đại và chắc chắn đến đâu đi nữa thì cũng có lúc bị vô hiệu hóa bởi những kẻ phá hoại có trình độ cao và có đủ thời gian. Chưa kể rằng tính an toàn của một hệ thống thông tin còn phụ thuộc rất nhiều vào việc sử dụng của con người. Từ đó có thể thấy rằng vấn đề an toàn mạng thực tế là cuộc chạy tiếp sức không ngừng và không ai dám khẳng định là có đích cuối cùng hay không.

CHƯƠNG 2 MỘT SỐ PHƯƠNG PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN

2.1 Nguyên lý các phương pháp mã hoá đối xứng

2.1.1 Sơ đồ chung của phương pháp mã hóa đối xứng.

Sơ đồ mã hóa đối xứng



Mô hình hệ mã hóa đối xứng

Mô hình này gồm có 5 thành phần:

- Văn bản thô
- Giải thuật mã hóa
- Khóa bí mật
- Văn bản mã hóa
- Giải thuật giải mã

Giả thiết rằng:

- Thuật toán mã hóa phải đủ mạnh để không thể giải mã được thông điệp nếu chỉ dựa trên duy nhất nội dung của văn bản được mã hóa.
- Sự an toàn của phương pháp mã hóa đối xứng chỉ phụ thuộc vào độ bí mật của khóa mà không phụ thuộc vào độ bí mật của thuật toán.