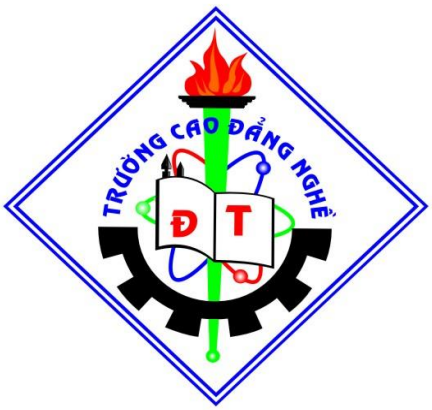
UỶ BAN NHÂN DÂN TỈNH ĐỒNG THÁP
TRƯỜNG CAO ĐẲNG NGHỀ ĐỒNG THÁP



GIÁO TRÌNH

MÔN HỌC: **AN TOÀN VÀ BẢO MẬT THÔNG TIN**
NGÀNH, NGHỀ: **CÔNG NGHỆ THÔNG TIN (UDPM)**
TRÌNH ĐỘ: **CAO ĐẲNG**

(Ban hành kèm theo Quyết định Số: /QĐ-CĐCĐ-ĐT ngày tháng năm 2017 của Hiệu trưởng Trường Cao đẳng nghề Đồng Tháp)

Đồng Tháp, năm 2017

TUYÊN BỐ BẢN QUYỀN

LỜI GIỚI THIỆU

Trong những năm qua, dạy nghề đã có những bước tiến vượt bậc cả về số lượng và chất lượng, nhằm thực hiện nhiệm vụ đào tạo nguồn nhân lực kỹ thuật trực tiếp đáp ứng nhu cầu xã hội. Cùng với sự phát triển của khoa học công nghệ trên thế giới, lĩnh vực Công nghệ thông tin nói chung và ngành Quản trị mạng ở Việt Nam nói riêng đã có những bước phát triển đáng kể.

Chương trình dạy nghề Quản trị mạng đã được xây dựng trên cơ sở phân tích nghề, phần kỹ năng nghề được kết cấu theo các mô đun môn học. Để tạo điều kiện thuận lợi cho các cơ sở dạy nghề trong quá trình thực hiện, việc biên soạn giáo trình theo các mô đun đào tạo nghề là cấp thiết hiện nay.

Môn học 23: An toàn mạng là môn học đào tạo chuyên môn nghề được biên soạn theo hình thức tích hợp lý thuyết và thực hành. Trong quá trình thực hiện, nhóm biên soạn đã tham khảo nhiều tài liệu An toàn mạng trong và ngoài nước, kết hợp với kinh nghiệm trong thực tế.

Mặc dầu có rất nhiều cố gắng, nhưng không tránh khỏi những khiếm khuyết, rất mong nhận được sự đóng góp ý kiến của độc giả để giáo trình được hoàn thiện hơn.

Xin chân thành cảm ơn

……, ngày … tháng … năm 202…
Tham gia biên soạn

MỤC LỤC

GIÁO TRÌNH MÔN HỌC

Tên môn học: An toàn thông tin

Mã môn học: MH23

Thời gian thực hiện môn học: 65 giờ; (Lý thuyết: 25 giờ; Thực hành: 38 giờ; Kiểm tra 2 giờ)

I. Vị trí, tính chất của môn học:

- Vị trí: Môn học được bố trí giảng dạy sau khi đã học xong môn Mạng máy tính.
- Tính chất: Môn học này thuộc nhóm các môn chuyên môn bắt buộc.

II. Mục tiêu của môn học:

- Kiến thức:
  - Trình bày được các nguy cơ mất an toàn; một số kỹ thuật bảo vệ hệ thống máy tính, hệ thống mạng.
  - Hiểu được các nguyên lý an toàn thông tin.
  - Trình bày được các thành phần khác nhau trong mô hình bảo mật.
- Kỹ năng:
  - Có khả năng triển khai hệ thống bảo vệ đồng bộ.
  - Có khả năng phát hiện sự cố mất an toàn máy tính và khắc phục sự cố đơn giản.
- Về năng lực tự chủ và trách nhiệm:

  Nghiêm túc khi nghiên cứu

III. Nội dung môn học.

1. Nội dung tổng quát và phân bổ thời gian

STT	Nội dung	Tổng Số	Lý Thuyết	Thực hành, thí nghiệm, thảo luận, bài tập	Kiểm Tra
1	Chương 1: Các khái niệm cơ bản	8	8	0	0
2	Chương 2: Các kỹ thuật bảo vệ thông tin	26	9	16	1
3	Chương 3: Triển khai hệ thống bảo vệ	31	8	22	1
	Tổng cộng	**65**	**25**	**38**	**2**

Nội dung của môn học/mô đun:

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN

Mã chương: MH 23-01

Giới thiệu:

Bảo mật là một trong những lĩnh vực mà hiện nay giới công nghệ thông tin khá quan tâm. Một khi Internet ra đời và phát triển, nhu cầu trao đổi thông tin trở nên cần thiết. Mục tiêu của việc nối mạng là làm cho mọi người có thể sử dụng chung tài nguyên từ những vị trí địa lý khác nhau. Cũng chính vì vậy mà các tài nguyên cũng rất dễ dàng bị phân tán, dẫn đến một điều hiển nhiên là chúng sẽ bị xâm phạm, gây mất mát dữ liệu cũng như các thông tin có giá trị. Càng giao thiệp rộng thì càng dễ bị tấn công, đó là một quy luật. Từ đó, vấn đề bảo vệ thông tin cũng đồng thời xuất hiện, bảo mật ra đời.

Tất nhiên, mục tiêu của bảo mật không chỉ nằm gói gọn trong lĩnh vực bảo vệ thông tin mà còn nhiều phạm trù khác như kiểm duyệt web, bảo mật internet, bảo mật http, bảo mật trên các hệ thống thanh toán điện tử và giao dịch trực tuyến….

Mọi nguy cơ trên mạng đều là mối nguy hiểm tiềm tàng. Từ một lỗ hổng bảo mật nhỏ của hệ thống, nhưng nếu biết khai thác và lợi dụng với tầng suất cao và kỹ thuật hack điêu luyện thì cũng có thể trở thành tai họa.

Theo thống kê của tổ chức bảo mật nổi tiếng **CERT** (Computer Emegancy Response Team) thì số vụ tấn công ngày càng tăng. Cụ thể năm 1989 có khoản 200 vụ, đến năm 1991 có 400 vụ, đến năm 1994 thì con số này tăng lên đến mức 1330 vụ, và sẽ còn tăng mạnh trong thời gian tới.

Như vậy, số vụ tấn công ngày càng tăng lên với mức độ chóng mặt. Điều này cũng dễ hiểu, vì một thực thể luôn tồn tại hai mặt đối lập nhau. Sự phát triển mạnh mẽ của công nghệ thông tin và kỹ thuật sẽ làm cho nạn tấn công, ăn cắp, phá hoại trên internet bùng phát mạnh mẽ.

Internet là một nơi cực kỳ hỗn loạn. Mọi thông tin mà bạn thực hiện truyền dẫn đều có thể bị xâm phạm, thậm chí là công khai. Bạn có thể hình dung internet là một phòng họp, những gì được trao đổi trong phòng họp đều được người khác nghe thấy. Với internet thì những người này không thấy mặt nhau, và việc nghe thấy thông tin này có thể hợp pháp hoặc là không hợp pháp.

Tóm lại, internet là một nơi mất an toàn. Mà không chỉ là internet các loại mạng khác, như mạng LAN, đến một hệ thống máy tính cũng có thể bị xâm phạm. Thậm chí, mạng điện thoại, mạng di động cũng không nằm ngoài cuộc. Vì thế chúng ta nói rằng, phạm vi của bảo mật rất lớn, nói không còn gói gọn trong một máy tính một cơ quan mà là toàn cầu.

Mục tiêu:

- Trình bày được các hình thức tấn công vào hệ thống mạng;
- Xác định được các thành phần của một hệ thống bảo mật;
- Thực hiện các thao tác an toàn với máy tính.

Nội dung chính:

1. Các khái niệm chung

Mục tiêu:

- Mô tả được các đối tượng tấng công hệ thống mạng ;

- Xác định được các lỗ hổng bảo mật.

1.1. Đối tượng tấn công mạng (Intruder)

Là những cá nhân hoặc các tổ chức sử dụng các kiến thức về mạng và các công cụ phá hoại (phần mềm hoặc phần cứng) để dò tìm các điểm yếu, lỗ hổng bảo mật trên hệ thống, thực hiện các hoạt động xâm nhập và chiếm đoạt tài nguyên mạng trái phép.

Một số đối tượng tấn công mạng là:

- **Hacker:** Là những kẻ xâm nhập vào mạng trái phép bằng cách sử dụng các công cụ phá mật khẩu hoặc khai thác các điểm yếu của các thành phần truy nhập trên hệ thống.

- **Masquerader:** Là những kẻ giả mạo thông tin trên mạng. Một số hình thức giả mạo như giả mạo địa chỉ IP, tên miền, định danh người dùng ...

- **Eavesdropping:** Là những đối tượng nghe trộm thông tin trên mạng, sử dụng các công cụ sniffer; sau đó dùng các công cụ phân tích và debug để lấy được các thông tin có giá trị. Những đối tượng tấn công mạng có thể nhằm nhiều mục đích khác nhau: như ăn cắp những thông tin có giá trị về kinh tế, phá hoại hệ thống mạng có chủ định, hoặc cũng có thể chỉ là những hành động vô ý thức, thử nghiệm các chương trình không kiểm tra cẩn thận ...

1.2. Các lỗ hổng bảo mật

Các lỗ hổng bảo mật là những điểm yếu kém trên hệ thống hoặc ẩn chứa trong một dịch vụ mà dựa vào đó kẻ tấn công có thể xâm nhập trái phép để thực hiện các hành động phá hoại hoặc chiếm đoạt tài nguyên bất hợp pháp.

Nguyên nhân gây ra những lỗ hổng bảo mật là khác nhau: có thể do lỗi của bản thân hệ thống, hoặc phần mềm cung cấp, hoặc do người quản trị yếu kém không hiểu sâu sắc các dịch vụ cung cấp ...

Mức độ ảnh hưởng của các lỗ hổng là khác nhau. Có những lỗ hổng chỉ ảnh hưởng tới chất lượng dịch vụ cung cấp, có những lỗ hổng ảnh hưởng nghiêm trọng tới toàn bộ hệ thống ...

2. Nhu cầu bảo vệ thông tin

Mục tiêu:

- Trình bày được các nhu cầu cần bảo vệ trên hệ thống mạng

2.1. Nguyên nhân

Tài nguyên đầu tiên mà chúng ta nói đến chính là dữ liệu. Đối với dữ liệu, chúng ta cần quan tâm những yếu tố sau:

2.2 Bảo vệ dữ liệu

Những thông tin lưu trữ trên hệ thống máy tính cần được bảo vệ do các yêu cầu sau:

- Bảo mật: những thông tin có giá trị về kinh tế, quân sự, chính sách vv... cần được bảo vệ và không lộ thông tin ra bên ngoài.

- Tính toàn vẹn: Thông tin không bị mất mát hoặc sửa đổi, đánh tráo.

- Tính kịp thời: Yêu cầu truy nhập thông tin vào đúng thời điểm cần thiết.

Trong các yêu cầu này, thông thường yêu cầu về bảo mật được coi là yêu cầu số 1 đối với thông tin lưu trữ trên mạng. Tuy nhiên, ngay cả khi những thông tin này không được giữ bí mật, thì những yêu cầu về tính toàn vẹn cũng rất quan trọng. Không một cá nhân, một tổ chức nào lãng phí tài nguyên vật chất và thời gian để lưu trữ những thông tin mà không biết về tính đúng đắn của những thông tin đó.

2.3. Bảo vệ tài nguyên sử dụng trên mạng

Trên thực tế, trong các cuộc tấn công trên Internet, kẻ tấn công, sau khi đã làm chủ được hệ thống bên trong, có thể sử dụng các máy này để phục vụ cho mục đích của mình như chạy các chương trình dò mật khẩu người sử dụng, sử dụng các liên kết mạng sẵn có để tiếp tục tấn công các hệ thống khác.

2.4. Bảo bệ danh tiếng của cơ quan

Một phần lớn các cuộc tấn công không được thông báo rộng rãi, và một trong những nguyên nhân là nỗi lo bị mất uy tín của cơ quan, đặc biệt là các công ty lớn và các cơ quan quan trọng trong bộ máy nhà nước. Trong trường hợp người quản trị hệ thống chỉ được biết đến sau khi chính hệ thống của mình được dùng làm bàn đạp để tấn công các hệ thống khác, thì tổn thất về uy tín là rất lớn và có thể để lại hậu quả lâu dài.

Bài tập thực hành của học viên

Câu 1: Trình bày các đối tượng tấng công hệ thống mạng

Câu 2: Đối với dữ liệu, chúng ta cần quan tâm những yếu tố nào?

CHƯƠNG 2: MÃ HÓA THÔNG TIN

Mã chương: MH23-02

Mục tiêu:

- Liệt kê và phân biệt được các kiểu mã hóa dữ liệu;
- Áp dụng được việc mã hóa và giải mã với một số phương pháp cơ bản;
- Mô tả về hạ tầng ứng dụng khóa công khai;
- Thực hiện các thao tác an toàn với máy tính.

1. Cơ bản về mã hoá (Cryptography)

Mục tiêu:

- Trình bày được nhu cầu sử dụng mã hóa;

- Mô tả được quá trình mã hóa và giải mã.

Những điều căn bản về mã hoá

Khi bắt đầu tìm hiểu về mã hoá, chúng ta thường đặt ra những câu hỏi chẳng hạn như là: Tại sao cần phải sử dụng mã hoá ? Tại sao lại có quá nhiều thuật toán mã hoá ?...

1.1. Tại sao cần phải sử dụng mã hoá

Thuật toán Cryptography đề cập tới nghành khoa học nghiên cứu về mã hoá và giải mã thông tin. Cụ thể hơn là nghiên cứu các cách thức chuyển đổi thông tin từ dạng rõ (clear text) sang dạng mờ (cipher text) và ngược lại. Đây là một phương pháp hỗ trợ rất tốt cho trong việc chống lại những truy cập bất hợp pháp tới dữ liệu được truyền đi trên mạng, áp dụng mã hoá sẽ khiến cho nội dung thông tin được truyền đi dưới dạng mờ và không thể đọc được đối với bất kỳ ai cố tình muốn lấy thông tin đó.

1.2. Nhu cầu sử dụng kỹ thuật mã hoá

Không phải ai hay bất kỳ ứng dụng nào cũng phải sử dụng mã hoá. Nhu cầu về sử dụng mã hoá xuất hiện khi các bên tham gia trao đổi thông tin muốn bảo vệ các tài liệu quan trọng hay gửi chúng đi một cách an toàn. Các tài liệu quan trọng có thể là: tài liệu quân sự, tài chính, kinh doanh hoặc đơn giản là một thông tin nào đó mang tính riêng tư.

Như chúng ta đã biết, Internet hình thành và phát triển từ yêu cầu của chính phủ Mỹ nhằm phục vụ cho mục đích quân sự. Khi chúng ta tham gia trao đổi thông tin, thì Internet là môi trường không an toàn, đầy rủi ro và nguy hiểm, không có gì đảm bảo rằng thông tin mà chúng ta truyền đi không bị đọc trộm trên đường truyền. Do đó, mã hoá được áp dụng như một biện pháp nhằm giúp chúng ta tự bảo vệ chính mình cũng như những thông tin mà chúng ta gửi đi. Bên cạnh đó, mã hoá còn có những ứng dụng khác như là bảo đảm tính toàn vẹn của dữ liệu.

Tại sao lại có quá nhiều thuật toán mã hoá

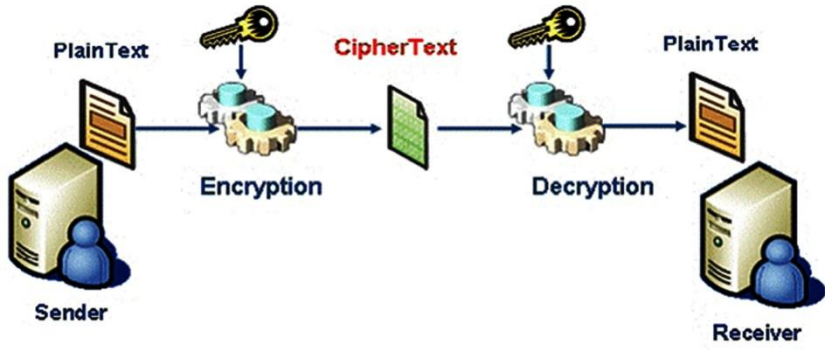
Theo một số tài liệu thì trước đây tính an toàn, bí mật của một thuật toán phụ thuộc vào phương thức làm việc của thuật toán đó. Nếu như tính an toàn của một thuật toán chỉ dựa vào sự bí mật của thuật toán đó thì thuật toán đó là một thuật toán hạn chế

(Restricted Algrorithm). Restricted Algrorithm có tầm quan trọng trong lịch sử nhưng không còn phù hợp trong thời đại ngày nay. Giờ đây, nó không còn được mọi người sử dụng do mặt hạn chế của nó: mỗi khi một user rời khỏi một nhóm thì toàn bộ nhóm đó phải chuyển sang sử dụng thuật toán khác hoặc nếu người đó người trong nhóm đó tiết lộ thông tin về thuật toán hay có kẻ phát hiện ra tính bí mật của thuật toán thì coi như thuật toán đó đã bị phá vỡ, tất cả những user còn lại trong nhóm buộc phải thay đổi lại thuật toán dẫn đến mất thời gian và công sức.

Hệ thống mã hoá hiện nay đã giải quyết vấn đề trên thông qua khoá (Key) là một yếu tố có liên quan nhưng tách rời ra khỏi thuật toán mã hoá. Do các thuật toán hầu như được công khai cho nên tính an toàn của mã hoá giờ đây phụ thuộc vào khoá. Khoá này có thể là bất kì một giá trị chữ hoặc số nào. Phạm vi không gian các giá trị có thể có của khoá được gọi là Keyspace . Hai quá trình mã hoá và giải mã đều dùng đến khoá. Hiện nay, người ta phân loại thuật toán dựa trên số lượng và đặc tính của khoá được sử dụng.

Nói đến mã hoá tức là nói đến việc che dấu thông tin bằng cách sử dụng thuật toán. Che dấu ở đây không phải là làm cho thông tin biến mất mà là cách thức chuyển từ dạng tỏ sang dạng mờ. Một thuật toán là một tập hợp của các câu lệnh mà theo đó chương trình sẽ biết phải làm thế nào để xáo trộn hay phục hồi lại dữ liệu. Chẳng hạn một thuật toán rất đơn giản mã hoá thông điệp cần gửi đi như sau:
Bước 1: Thay thế toàn bộ chữ cái “e” thành số “3”
Bước 2: Thay thế toàn bộ chữ cái “a” thành số “4”
Bước 3: Đảo ngược thông điệp

Trên đây là một ví dụ rất đơn giản mô phỏng cách làm việc của một thuật toán mã hoá. Sau đây là các thuật ngữ cơ bản nhất giúp chúng ta nắm được các khái niệm:



Hinh1: Minh hoạ quá trình mã hóa và giải mã
Sender/Receiver: Người gửi/Người nhận dữ liệu
- Plaintext (Cleartext): Thông tin trước khi được mã hoá. Đây là dữ liệu ban đầu ở dạng rõ
- Ciphertext: Thông tin, dữ liệu đã được mã hoá ở dạng mờ
- Key: Thành phần quan trọng trong việc mã hoá và giải mã
- CryptoGraphic Algorithm: Là các thuật toán được sử dụng trong việc mã hoá hoặc giải mã thông tin
- CryptoSystem: Hệ thống mã hoá bao gồm thuật toán mã hoá, khoá, Plaintext, Ciphertext

Kí hiệu chung: P là thông tin ban đầu, trước khi mã hoá. E() là thuật toán mã hoá. D() là thuật toán giải mã. C là thông tin mã hoá. K là khoá.

1.3. Quá trình mã hoá và giải mã như sau:

- Quá trình mã hoá được mô tả bằng công thức: EK(P)=C
- Quá trình giải mã được mô tả bằng công thức: DK(C)=P

Bên cạnh việc làm thế nào để che dấu nội dung thông tin thì mã hoá phải đảm bảo các mục tiêu sau:

a. Confidentiality (Tính bí mật): Đảm bảo dữ liệu được truyền đi một cách an toàn và không thể bị lộ thông tin nếu như có ai đó cố tình muốn có được nội dung của dữ liệu gốc ban đầu. Chỉ những người được phép mới có khả năng đọc được nội dung thông tin ban đầu.

b. Authentication (Tính xác thực): Giúp cho người nhận dữ liệu xác định được chắc chắn dữ liệu mà họ nhận là dữ liệu gốc ban đầu. Kẻ giả mạo không thể có khả năng để giả dạng một người khác hay nói cách khác không thể mạo danh để gửi dữ liệu. Người nhận có khả năng kiểm tra nguồn gốc thông tin mà họ nhận được.

c. Integrity (Tính toàn vẹn): Giúp cho người nhận dữ liệu kiểm tra được rằng dữ liệu không bị thay đổi trong quá trình truyền đi. Kẻ giả mạo không thể có khả năng thay thế dữ liệu ban đầu băng dữ liệu giả mạo

d. Non-repudation (Tính không thể chối bỏ): Người gửi hay người nhận không thể chối bỏ sau khi đã gửi hoặc nhận thông tin.

2. Độ an toàn của thuật toán

Mục tiêu:

- *Trình bày được các thuật toán mã hóa*

Nguyên tắc đầu tiên trong mã hoá là "Thuật toán nào cũng có thể bị phá vỡ". Các thuật toán khác nhau cung cấp mức độ an toàn khác nhau, phụ thuộc vào độ phức tạp để phá vỡ chúng. Tại một thời điểm, độ an toàn của một thuật toán phụ thuộc:

- Nếu chi phí hay phí tổn cần thiết để phá vỡ một thuật toán lớn hơn giá trị của thông tin đã mã hóa thuật toán thì thuật toán đó tạm thời được coi là an toàn.
- Nếu thời gian cần thiết dùng để phá vỡ một thuật toán là quá lâu thì thuật toán đó tạm thời được coi là an toàn.
- Nếu lượng dữ liệu cần thiết để phá vỡ một thuật toán quá lơn so với lượng dữ liệu đã được mã hoá thì thuật toán đó tạm thời được coi là an toàn

Từ tạm thời ở đây có nghĩa là độ an toàn của thuật toán đó chỉ đúng trong một thời điểm nhất định nào đó, luôn luôn có khả năng cho phép những người phá mã tìm ra cách để phá vỡ thuật toán. Điều này chỉ phụ thuộc vào thời gian, công sức, lòng đam mê cũng như tính kiên trì bên bỉ. Càng ngày tốc độ xử lý của CPU càng cao, tốc độ tính toán của máy tính ngày càng nhanh, cho nên không ai dám khẳng định chắc chắn một điều rằng thuật toán mà mình xây dựng sẽ an toàn mãi mãi. Trong lĩnh vực mạng máy tính và truyền thông luôn luôn tồn tại hai phe đối lập với nhau những người chuyên đi tấn công, khai thác lỗ hổng của hệ thống và những người chuyên phòng thủ, xây dựng các qui trình bảo vệ hệ thống. Cuộc chiến giữa hai bên chẳng khác gì một cuộc chơi trên bàn cờ, từng bước đi, nước bước sẽ quyết định số phận của mối bên.

Trong cuộc chiến này, ai giỏi hơn sẽ dành được phần thắng. Trong thế giới mã hoá cũng vậy, tất cả phụ thuộc vào trình độ và thời gian…sẽ không ai có thể nói trước được điều gì. Đó là điểm thú vị của trò chơi.

3. Phân loại các thuật toán mã hoá

Có rất nhiều các thuật toán mã hoá khác nhau. Từ những thuật toán được công khai để mọi người cùng sử dụng và áp dụng như là một chuẩn chung cho việc mã hoá dữ liệu; đến những thuật toán mã hoá không được công bố. Có thể phân loại các thuật toán mã hoá như sau:

Phân loại theo các phương pháp:

- Mã hoá cổ điển (Classical cryptography)
- Mã hoá đối xứng (Symetric cryptography)
- Mã hoá bất đối xứng(Asymetric cryptography)
- Hàm băm (Hash function)

Phân loại theo số lượng khoá:

- Mã hoá khoá bí mật (Private-key Cryptography)
- Mã hoá khoá công khai (Public-key Cryptography)

3.1. Mã hoá cổ điển:

Xuất hiện trong lịch sử, các phương pháp này không dùng khoá. Thuật toán đơn giản và dễ hiểu. Những từ chính các phương pháp mã hoá này đã giúp chúng ta tiếp cận với các thuật toán mã hoá đối xứng được sử dụng ngày nay. Trong mã hoá cổ điển có 02 phương pháp nổi bật đó là:

- Mã hoá thay thế (Substitution Cipher):

Là phương pháp mà từng kí tự (hay từng nhóm kí tự) trong bản rõ (Plaintext) được thay thế bằng một kí tự (hay một nhóm kí tự) khác để tạo ra bản mờ (Ciphertext). Bên nhận chỉ cần đảo ngược trình tự thay thế trên Ciphertext để có được Plaintext ban đầu.

Các hệ mật mã cổ điển- Hệ mã hóa thay thế(Substitution Cipher)

Chọn một hoán vị p: Z26 → Z26 làm khoá.

VD:

Mã hoá

ep(a)=X

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t

n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

Giải mã:

dp(A)=d

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

Bảng rõ "nguyenthanhnhut"
Mã hóa "SOUDHSMGXSGSGUM"

- Mã hoá hoán vị (Transposition Cipher):

Bên cạnh phương pháp mã hoá thay thế thì trong mã hoá cổ điển có một phương pháp khác nữa cũng nổi tiếng không kém, đó chính là mã hoá hoán vị. Nếu như trong phương pháp mã hoá thay thế, các kí tự trong Plaintext được thay thế hoàn toàn bằng các kí tự trong Ciphertext, thì trong phương pháp mã hoá hoán vị, các kí tự trong Plaintext vẫn được giữ nguyên, chúng chỉ được sắp xếp lại vị trí để tạo ra Ciphertext. Tức là các kí tự trong Plaintext hoàn toàn không bị thay đổi bằng kí tự khác.

Mã hoán vị - Permutation Cipher

Chuyển đổi vị trí bản thân các chữ cái trong văn bản gốc từng khối m chữ cái.

Mã hoá:

$e\pi(x1, \ldots, xm) = (x\pi(1), \ldots, x\pi m))$.

Giải mã:

$d\pi(y1, \ldots, ym) = (y\pi'(1), \ldots, y\pi'(m))$.

Trong đó, π: Z26 → Z26 là một hoán vị, π' :=π-1 là nghịch đảo của π.

Hoán vị

x	1	2	3	4	5	6
Π(x)	3	5	1	6	4	2

x	1	2	3	4	5	6
Π^{-1}(x)	3	6	1	5	2	4

"shesellsseashellsbytheseashore".
shesel | lsseas | hellsb | ythese | ashore
EESLSH | SALSES | LSHBLE | HSYEET | HRAEOS
"EESLSHSALSESLSHBLEHSYEETHRAEOS".

3.2. Mã hoá đối xứng:

Ở phần trên, chúng ta đã tìm hiểu về mã hoá cổ điển, trong đó có nói rằng mã hoá cổ điển không dùng khoá. Nhưng trên thực nếu chúng ta phân tích một cách tổng quát, chúng ta sẽ thấy được như sau:

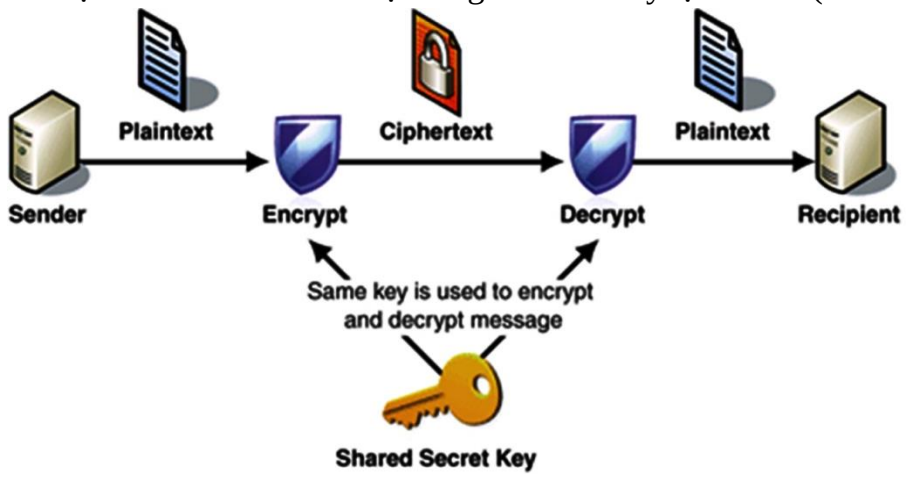
- Mã hoá cổ điển có sử dụng khoá. Bằng chứng là trong phương pháp Ceaser Cipher thì khoá chính là phép dịch ký tự, mà cụ thể là phép dịch 3 ký tự. Trong phương pháp mã hoá hoán vị thì khóa nằm ở số hàng hay số cột mà chúng ta qui định. Khoá này có thể được thay đổi tuỳ theo mục đích mã hoá của chúng ta, nhưng nó phải nằm trong một phạm vi cho phép nào đó.

- Để dùng được mã hoá cổ điển thì bên mã hoá và bên giải mã phải thống nhất với nhau về cơ chế mã hoá cũng như giải mã. Nếu như không có công việc này thì hai bên sẽ không thể làm việc được với nhau.

Mã hoá đối xứng còn có một số tên gọi khác như Secret Key Cryptography (hay Private Key Cryptography), sử dụng cùng một khoá cho cả hai quá trình mã hoá và giải mã.

Quá trình thực hiện như sau:

Trong hệ thống mã hoá đối xứng, trước khi truyền dữ liệu, 2 bên gửi và nhận phải thoả thuận về khoá dùng chung cho quá trình mã hoá và giải mã. Sau đó, bên gửi sẽ mã hoá bản rõ (Plaintext) bằng cách sử dụng khoá bí mật này và gửi thông điệp đã mã hoá cho bên nhận. Bên nhận sau khi nhận được thông điệp đã mã hoá sẽ sử dụng chính khoá bí mật mà hai bên thoả thuận để giải mã và lấy lại bản rõ (Plaintext).



Hình 2: Mã hóa đối xứng

Hình vẽ trên chính là quá trình tiến hành trao đổi thông tin giữa bên gửi và bên nhận thông qua việc sử dụng phương pháp mã hoá đối xứng. Trong quá trình này, thì thành phần quan trọng nhất cần phải được giữ bí mật chính là khoá. Việc trao đổi, thoả thuận về thuật toán được sử dụng trong việc mã hoá có thể tiến hành một cách công khai, nhưng bước thoả thuận về khoá trong việc mã hoá và giải mã phải tiến hành bí mật. Chúng ta có thể thấy rằng thuật toán mã hoá đối xứng sẽ rất có lợi khi được áp dụng trong các cơ quan hay tổ chức đơn lẻ. Nhưng nếu cần phải trao đổi thông tin với một bên thứ ba thì việc đảm bảo tính bí mật của khoá phải được đặt lên hàng đầu.

Mã hoá đối xứng có thể được phân thành 02 loại:

- **Loại thứ nhất** tác động trên bản rõ theo từng nhóm bits. Từng nhóm bits này được gọi với một cái tên khác là khối (Block) và thuật toán được áp dụng gọi là **Block Cipher**. Theo đó, từng khối dữ liệu trong văn bản ban đầu được thay thế bằng một

khối dữ liệu khác có cùng độ dài. Đối với các thuật toán ngày nay thì kích thước chung của một Block là 64 bits.

- **Loại thứ hai** tác động lên bản rõ theo từng bit một. Các thuật toán áp dụng được gọi là **Stream Cipher**. Theo đó, dữ liệu của văn bản được mã hoá từng bit một. Các thuật toán mã hoá dòng này có tốc độ nhanh hơn các thuật toán mã hoá khối và nó thường được áp dụng khi lượng dữ liệu cần mã hoá chưa biết trước.
Một số thuật toán nổi tiếng trong mã hoá đối xứng là: DES, Triple DES(3DES), RC4, AES…

+ **DES:** viết tắt của Data Encryption Standard. Với DES, bản rõ (Plaintext) được mã hoá theo từng khối 64 bits và sử dụng một khoá là 64 bits, nhưng thực tế thì chỉ có 56 bits là thực sự được dùng để tạo khoá, 8 bits còn lại dùng để kiểm tra tính chẵn, lẻ. DES là một thuật toán được sử dụng rộng rãi nhất trên thế giới. Hiện tại DES không còn được đánh giá cao do kích thước của khoá quá nhỏ 56 bits, và dễ dàng bị phá vỡ.

+ **Triple DES (3DES):** 3DES cải thiện độ mạnh của DES bằng việc sử dụng một quá trình mã hoá và giải mã sử dụng 3 khoá. Khối 64-bits của bản rõ đầu tiên sẽ được mã hoá sử dụng khoá thứ nhất. Sau đó, dữ liệu bị mã hóa được giải mã bằng việc sử dụng một khoá thứ hai. Cuối cùng, sử dụng khoá thứ ba và kết quả của quá trình mã hoá trên để mã hoá.

C = EK3(DK2(EK1(P)))

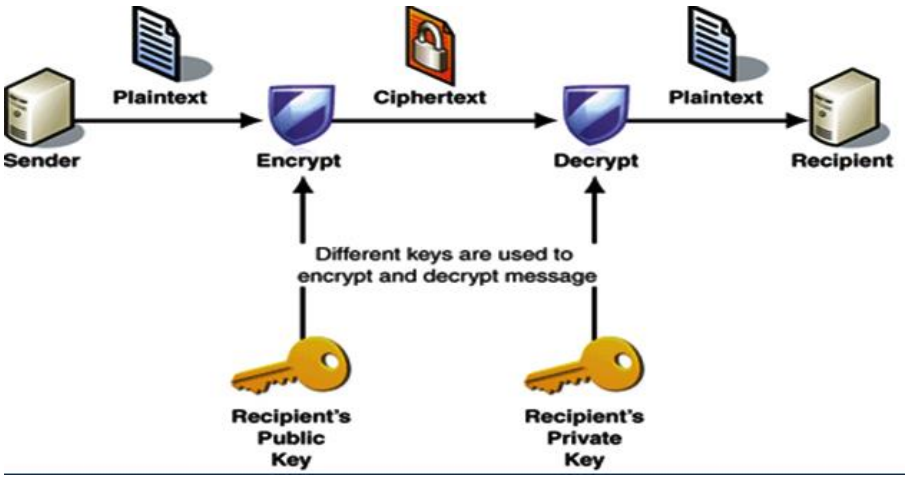
P = DK1(EK2(DK3(C)))

+ **AES**: Viết tắt của Advanced Encryption Standard, được sử dụng để thay thế cho DES. Nó hỗ trợ độ dài của khoá từ 128 bits cho đến 256 bits.

3.3. Mã hoá bất đối xứng:

Hay còn được gọi với một cái tên khác là mã hoá khoá công khai (Public Key Cryptography), nó được thiết kế sao cho khoá sử dụng trong quá trình mã hoá khác biệt với khoá được sử dụng trong quá trình giải mã. Hơn thế nữa, khoá sử dụng trong quá trình giải mã không thể được tính toán hay luận ra được từ khoá được dùng để mã hoá và ngược lại, tức là hai khoá này có quan hệ với nhau về mặt toán học nhưng không thể suy diễn được ra nhau. Thuật toán này được gọi là mã hoá công khai vì khoá dùng cho việc mã hoá được công khai cho tất cả mọi người. Một người bất kỳ có thể dùng khoá này để mã hoá dữ liệu nhưng chỉ duy nhất người mà có khoá giải mã tương ứng mới có thể đọc được dữ liệu mà thôi. Do đó trong thuật toán này có 2 loại khoá: Khoá để mã hoá được gọi là Public Key, khoá để giải mã được gọi là Private Key.

Mã hoá khoá công khai ra đời để giải quyết vấn đề về quản lý và phân phối khoá của các phương pháp mã hoá đối xứng. Hình minh hoạ ở trên cho chúng ta thấy được quá trình truyền tin an toàn dựa vào hệ thống mã hoá khoá công khai. Quá trình truyền và sử dụng mã hoá khoá công khai được thực hiện như sau:



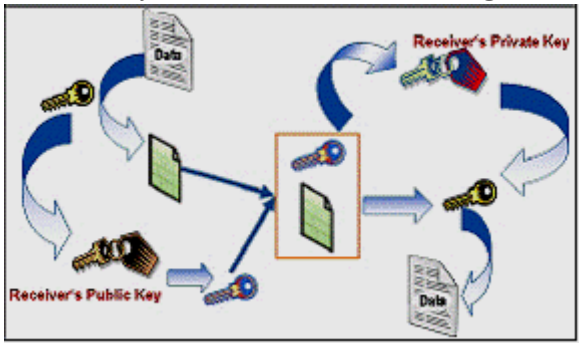
Hình 3: mã hóa bất đối xứng

- Bên gửi yêu cầu cung cấp hoặc tự tìm khoá công khai của bên nhận trên một server chịu trách nhiệm quản lý khoá.
- Sau đó hai bên thống nhất thuật toán dùng để mã hoá dữ liệu, bên gửi sử dụng khoá công khai của bên nhận cùng với thuật toán đã thống nhất để mã hoá thông tin được gửi đi.
- Khi nhận được thông tin đã mã hoá, bên nhận sử dụng khoá bí mật của mình để giải mã và lấy ra thông tin ban đầu.

Vậy là với sự ra đời của Mã hoá công khai thì khoá được quản lý một cách linh hoạt và hiệu quả hơn. Người sử dụng chỉ cần bảo vệ Private key. Tuy nhiên nhược điểm của Mã hoá khoá công khai nằm ở tốc độ thực hiện, nó chậm hơn rất nhiều so với mã hoá đối xứng. Do đó, người ta thường kết hợp hai hệ thống mã hoá khoá đối xứng và công khai lại với nhau và được gọi là Hybrid Cryptosystems. Một số thuật toán mã hoá công khai nổi tiếng: Diffle-Hellman, RSA,…

3.4. Hệ thống mã hoá khoá lai (Hybrid Cryptosystems):

Trên thực tế hệ thống mã hoá khoá công khai chưa thể thay thế hệ thống mã hoá khoá bí mật được, nó ít được sử dụng để mã hoá dữ liệu mà thường dùng để mã hoá khoá. Hệ thống mã hoá khoá lai ra đời là sự kết hợp giữa tốc độ và tính an toàn của hai hệ thống mã hoá ở trên. Dưới đây là mô hình của hệ thống mã hoá lai:



Hình 4: Mã hóa công khai

Nhìn vào mô hình chúng ta có thể hình dung được hoạt động của hệ thống mã hoá này như sau:

- Bên gửi tạo ra một khoá bí mật dùng để mã hoá dữ liệu. Khoá này còn được gọi là Session Key.

- Sau đó, Session Key này lại được mã hoá bằng khoá công khai của bên nhận dữ liệu.
- Tiếp theo dữ liệu mã hoá cùng với Session Key đã mã hoá được gửi đi tới bên nhận.
- Lúc này bên nhận dùng khoá riêng để giải mã Session Key và có được Session Key ban đầu.
- Dùng Session Key sau khi giải mã để giải mã dữ liệu.

Như vậy, hệ thống mã hoá khoá lai đã tận dụng tốt được các điểm mạnh của hai hệ thống mã hoá ở trên đó là: tốc độ và tính an toàn. Điều này sẽ làm hạn chế bớt khả năng giải mã của tin tặc.

*** Một số ứng dụng của mã hoá trong Security**

Một số ứng dụng của mã hoá trong đời sống hằng ngày nói chung và trong lĩnh vực bảo mật nói riêng.

Đó là:

- Securing Email - Bảo mật hệ thông mail
- Authentication System – Hệ thống xác thực
- Secure E-commerce – Bảo mật trong thương mại điện tử
- Virtual Private Network – Mạng riêng ảo
- Wireless Encryption – Mã hóa hệ thống Wireless

Bài tập thực hành của học viên

Câu 1: Tại sao cần phải sử dụng mã hoá thông tin?

Câu 2: Trình bày phương pháp mã hóa cổ điển

Câu 3: Trình bày phương pháp mã hóa dối xứng

Bài 1:

Thực hiện với hệ mã hóa thay thế(Substitution Cipher) mã hóa và giải mã với bảng rõ sau:

“ khoacongnghethongtin”

“sinhviencongnghethongtin”

Bài 2:

Thực hiện với hệ Mã hoá hoán vị (**Permutation Cipher**) mã hóa và giải mã với bảng rõ sau:

“ khoacongnghethongtin”

“sinhviencongnghethongtin”

CHƯƠNG 3: NAT (Network Address Translation)

Mã chương: MH23-03

Mục tiêu:

- Trình bày được quá trình NAT của một hệ thống mạng;
- Trình bày được NAT tĩnh và NAT động;
- Thiết lập cấu hình NAT trên Windows server;
- Thực hiện các thao tác an toàn với hệ thống mạng.

1. Giới thiệu:

Mục tiêu:

- Trình bày được quá trình NAT của một hệ thống mạng;

- Trình bày được NAT tĩnh và NAT động.

Lúc đầu, khi NAT được phát minh ra nó chỉ để giải quyết cho vấn đề thiếu IP. Vào lúc ấy không ai nghĩ rằng NAT có nhiều hữu ích và có lẽ nhiều ứng dụng trong những vấn đề khác của NAT vẫn chưa được tìm thấy.

Trong ngữ cảnh đó nhiều người đã cố gắng tìm hiểu vai trò của NAT và lợi ích của nó trong tương lai. Khi mà IPv6 được hiện thực thì nó không chỉ giải quyết cho vấn đề thiếu IP. Qua nhiều cuộc thử nghiệm họ đã chỉ ra rằng viêc chuyển hoàn toàn qua IPv6 thì không có vấn đề gì và mau lẹ nhưng để giải quyết những vấn đề liên qua giữa IPv6 và IPv4 là khó khăn. Bởi vậy có khả năng IPv4 sẽ là giao thức chủ yếu cho Internet và Intranet … lâu dài hơn những gì họ mong muốn.

Trước khi giải thích vai trò của NAT ngày nay và trong tương lai, những người này muốn chỉ ra sự khác nhau về phạm vi của NAT được sủ dụng vào ngày đó. Sự giải thích sẽ đưa ra một cái nhìn tổng quan và họ không khuyên rằng làm thế nào và nên dùng loại NAT nào. Sau đây chỉ là giới thiệu và phân loại các NAT phần chi tiết sẽ được thảo luận và đề cập trong chương sau khi hiện thực NAT là một layd out.

Phần trình bày được chia làm 2 phần :

- Phần đầu được đặt tên là CLASSIC NAT nó là các kỹ thuật NAT vào những thời kỳ sơ khai (đầu những năm 90) được trình bày chi tiết trong RFC 1931. Ứng dụng của nó chủ yếu giải quyết cho bài toán thiếu IP trên Internet.
- Phần hai trình bày những kỹ thuật NAT được tìm ra gần đây và ứng dụng trong nhiều mục đích khác.

2. Các kỹ thuật NAT cổ điển:

Nói về NAT chúng ta phải biết rằng có 2 cách là tĩnh và động. Trong trường hợp đầu thì sự phân chia IP là rõ ràng còn trường hợp sau thì ngược lại. Với NAT tĩnh thì một IP nguồn luôn được chuyển thành chỉ một IP đích mà thôi trong bất kỳ thời gian nào. Trong khi đó NAT động thì IP này là thay đổi trong các thời gian và trong các kết nối khác nhau.

Trong phần này chúng ta định nghĩa :

m: số IP cần được chuyển đổi (IP nguồn)

n: số IP sẵn có cho việc chuyển đổi (IP NATs hay gọi là IP đích)

2.1. NAT tĩnh

Yêu cầu m, n >= 1; m = n (m, n là số tự nhiên)

Với cơ chế IP tĩnh chúng ta có thể chuyển đổi cùng một số lượng các IP nguồn và đích. Trường hợp đặc biệt là khi cả 2 chỉ chứa duy nhất một IP ví dụ netmask là 255.255.255.255. Cách thức hiện thực NAT tĩnh thì dễ dàng vì toàn bộ cơ chế dịch địa chỉ được thực hiện bởi một công thức đơn giản:

Địa chỉ đích = Địa chỉ mạng mới OR (địa chỉ nguồn AND (NOT netmask))
Không có thông tin về trạng thái kết nối. Nó chỉ cần tìm các IP đích thích hợp là đủ. Các kết nối từ bên ngoài hệ thống vào bên trong hệ thống thì chỉ khác nhau về IP vì thế cơ chế NAT tĩnh thì hầu như hoàn toàn trong suốt.

Ví dụ một rule cho NAT tĩnh:

Dịch toàn bộ IP trong mạng 138.201.148.0 đến mạng có địa chỉ là 94.64.15.0, netmask là 255.255.255.0 cho cả hai mạng.

Dưới đây là mô tả việc dịch từ địa chỉ có IP là 138.201.148.27 đến 94.64.15.27, các cái khác tương tự.

10001010.11001001.10010100.**00011011** (host 138.201.148.0) AND

00000000.00000000.00000000.**11111111** (reverse netmask)

01011110.01000000.00001111 (new net: 94.64.15.0)

01011110.01000000.00001111.**00011011** (địa chỉ mới)

2.2. NAT động

Yêu cầu m >= 1 và m >= n

NAT động được sử dụng khi số IP nguồn không bằng số IP đích. Số host chia sẻ nói chung bị giới hạn bởi số IP đích có sẵn. NAT động phức tạp hơn NAT tĩnh vì thế chúng phải lưu giữ lại thông tin kết nối và thậm chí tìm thông tin của TCP trong packet.

Như đã đề cập ở trên NAT động cũng có thể sử dụng như một NAT tĩnh khi m = n. Một số người dùng nó thay cho NAT tĩnh vì mục đích bảo mật. Những kẻ từ bên ngoài không thể tìm được IP nào kết nối với host chỉ định vì tại thời điểm tiếp theo host này có thể nhận một IP hoàn toàn khác. Trong trường hợp đặc biệt thậm chí có nhiều địa chỉ đích hơn địa chỉ nguồn (m< n)
Những kết nối từ bên ngoài thì chỉ có thể khi những host này vẫn còn nắm giữ một IP trong bảng NAT động. Nơi mà NAT router lưu giữ những thông tin về IP bên trong (IP nguồn) được liên kết với NAT-IP(IP đích).

Cho một ví dụ trong một session của FPT non-passive. Nơi mà server cố gắng thiết lập một kênh truyền dữ liệu, vì thế khi server cố gắng gửi một IP packet đến FTP client thì phải có một entry cho client trong bảng NAT. Nó vẫn phải còn liên kết một IP client với cùng một NAT-IPs khi client bắt đầu một kênh truyền control trừ khi FTP session rỗi sau một thời gian timeout. Giao thức FTP có 2 cơ chế là passive và non-