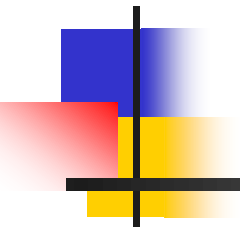


An toàn thông tin

Giáo viên: Lê Quốc Anh

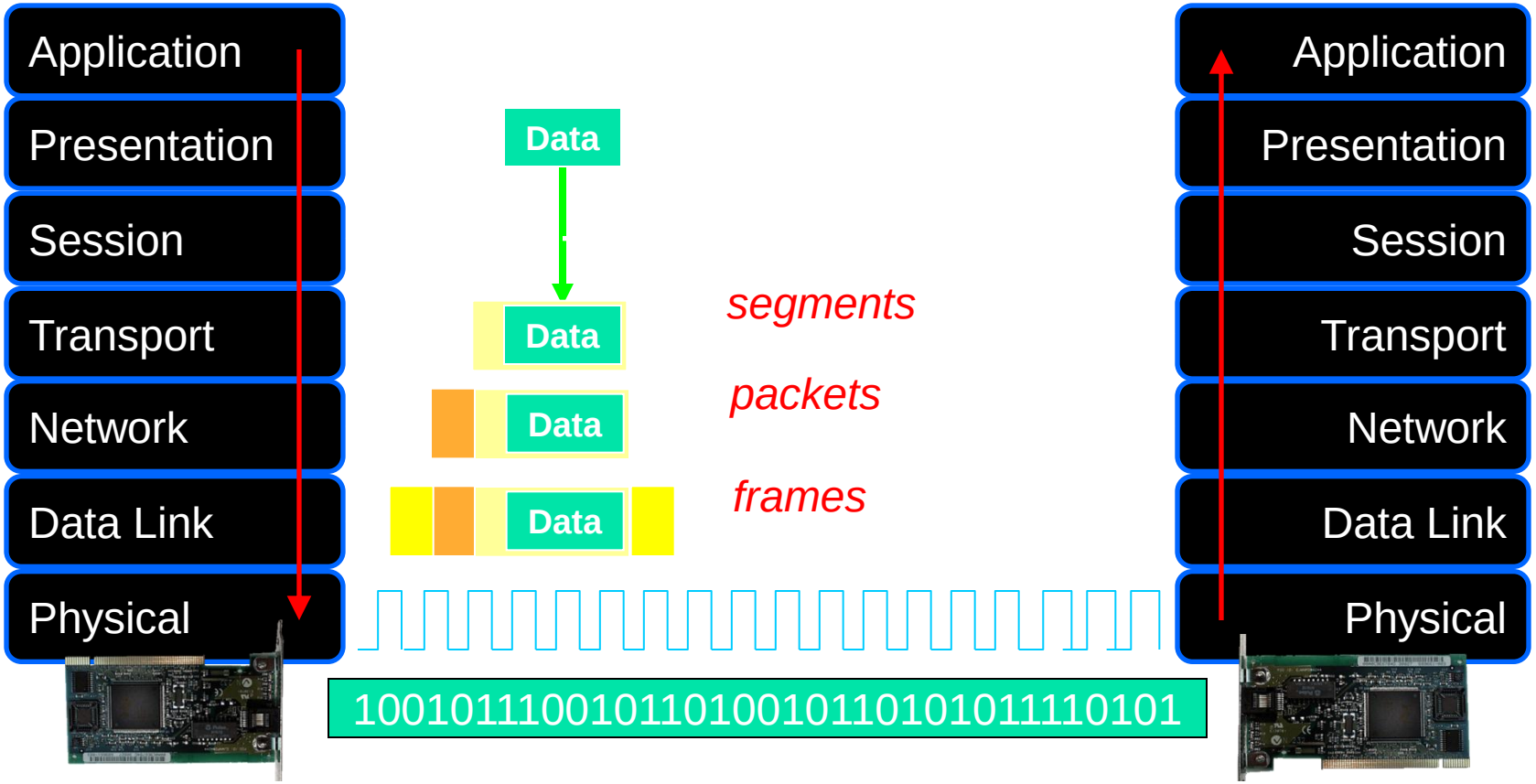
Tài liệu tham khảo

1. Giáo trình an toàn và bảo mật thông tin. Trường đại học Hàng Hải

   http://www.mediafire.com/?abdxi97upa2nqxf

2. An toàn thông tin, tác giả PGS.TS Thái Hồng Nhị, TS Phạm Minh Việt NXB khoa học và kỹ thuật.

Chương 1: Tổng quan về an toàn và bảo mật thông tin



1. Tại sao phải bảo vệ thông tin

- Thông tin là một bộ phần quan trọng và là tài sản thuộc quyền sở hữu của các tổ chức
- Sự thiệt hại và lạm dụng thông tin không chỉ ảnh hưởng đến người sử dụng hoặc các ứng dụng mà nó còn gây ra các hậu quả tai hại cho toàn bộ tổ chức đó
- Thêm vào đó sự ra đời của Internet đã giúp cho việc truy cập thông tin ngày càng trở nên dễ dàng hơn

2. Khái niệm hệ thống và tài sản của hệ thống

- **Khái niệm hệ thống** :Hệ thống là một tập hợp các máy tính bao gồm các thành phần, phần cứng, phần mềm và dữ liệu làm việc được tích luỹ qua thời gian.
- **Tài sản của hệ thống bao gồm:**
  - Phần cứng
  - Phần mềm
  - Dữ liệu
  - Các truyền thông giữa các máy tính của hệ thống
  - Môi trường làm việc
  - Con người

3. Các mối đe doạ đối với một hệ thống và các biện pháp ngăn chặn

- **Có 3 hình thức chủ yếu đe dọa đối với hệ thống:**
  - Phá hoại: kẻ thù phá hỏng thiết bị phần cứng hoặc phần mềm hoạt động trên hệ thống.
  - Sửa đổi: Tài sản của hệ thống bị sửa đổi trái phép. Điều này thường làm cho hệ thống không làm đúng chức năng của nó. Chẳng hạn như thay đổi mật khẩu, quyền ngợời dùng trong hệ thống làm họ không thể truy cập vào hệ thống để làm việc.
  - Can thiệp: Tài sản bị truy cập bởi những người không có thẩm quyền. Các truyền thông thực hiện trên hệ thống bị ngăn chặn, sửa đổi.

3. Các mối đe doạ đối với một hệ thống và các biện pháp ngăn chặn

- **Các đe dọa đối với một hệ thống thông tin có thể đến từ ba loại đối tượng như sau:**
  - Các đối tượng từ ngay bên trong hệ thống (insider), đây là những người có quyền truy cập hợp pháp đối với hệ thống.
  - Những đối tượng bên ngoài hệ thống (hacker, cracker), thường các đối tượng này tấn công qua những đường kết nối với hệ thống như Internet chẳng hạn.
  - Các phần mềm (chẳng hạn nhơ spyware, adware …) chạy trên hệ thống.

3. Các mối đe doạ đối với một hệ thống và các biện pháp ngăn chặn

- **Các biện pháp ngăn chặn:**
  - **Điều khiển thông qua phần mềm**: dựa vào các cơ chế an toàn bảo mật của hệ thống nền (hệ điều hành), các thuật toán mật mã học
  - **Điều khiển thông qua phần cứng**: các cơ chế bảo mật, các thuật toán mật mã học được cứng hóa để sử dụng
  - **Điều khiển thông qua các chính sách của tổ chức:** ban hành các qui định của tổ chức nhằm đảm bảo tính an toàn bảo mật của hệ thống.

4. Mục tiêu chung của an toàn bảo mật thông tin

- **Tính bí mật** *(Confidentiality)*: - Đảm bảo rằng thông tin không bị truy cập bất hợp pháp
  - Thuật ngữ *privacy* thường được sử dụng khi dữ liệu được bảo vệ có liên quan tới các thông tin mang tính cá nhân.
- **Tính toàn vẹn** *(Integrity):* - Đảm bảo rằng thông tin không bị sửa đổi bất hợp pháp.
- **Tính sẵn dùng** *(availability):* - Tài sản luôn sẵn sàng được sử dụng bởi nhưng người có thẩm quyền.
- **Tính xác thực** *(Authentication):* - Đảm bảo rằng dữ liệu nhận được chắc chắn là dữ liệu gốc ban đầu
- **Tính không thể chối bỏ** *(Non-repudation):* - Đảm bảo rằng người gửi hay người nhận dữ liệu không thể chối bỏ trách nhiệm sau khi đã gửi và nhận thông tin.

5. An toàn thông tin bằng mật mã

Mật mã là một ngành khoa học chuyên nghiên cứu các phương pháp truyền tin bí mật. Mật mã bao gồm : Lập mã và phá mã.

- **Lập mã bao gồm hai quá trình:** mã hóa và giải mã.Các sản phẩm của lĩnh vực này là các hệ mã mật , các hàm băm, các hệ chữ ký điện tử, các cơ chế phân phối, quản lý khóa và các giao thức mật mã.
- **Phá mã**: Nghiên cứu các phương pháp phá mã hoặc tạo mã giả. Sản phẩm của lĩnh vực này là các phương pháp phá mã , các phương pháp giả mạo chữ ký, các phương pháp tấn công các hàm băm và các giao thức mật mã

5. An toàn thông tin bằng mật mã

- Một trong những nghệ thuật để bảo vệ thông tin là biến đổi nó thành một định dạng mới khó đọc.
- Viết mật mã có liên quan đến việc mã hoá các thông báo trước khi gửi chúng đi và tiến hành giải mã chúng lúc nhận được

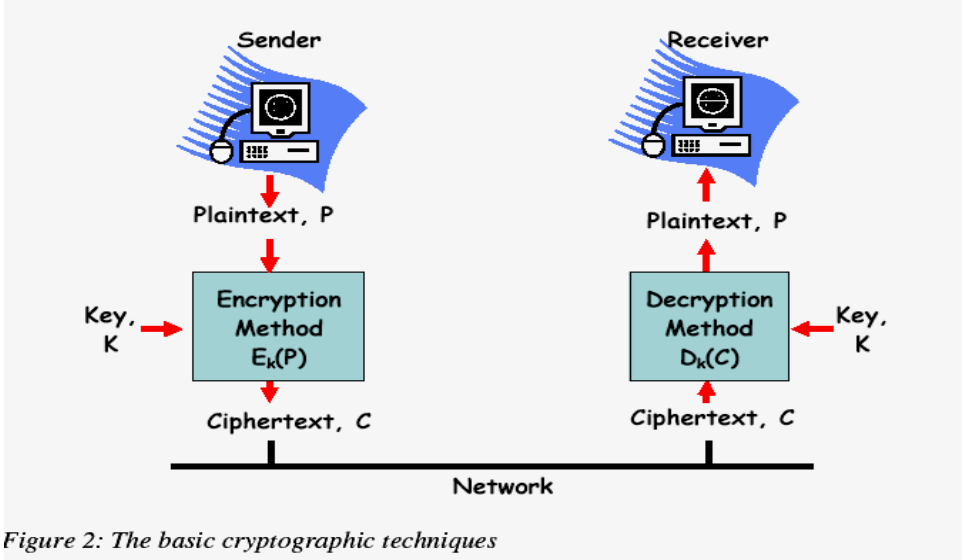


Figure 2: The basic cryptographic techniques

5. An toàn thông tin bằng mật mã

- **Có 2 phương thức mã hoá cơ bản: thay thế và hoán vị:**
  - **Phương thức mã hoá thay thế**: là phương thức mã hoá mà từng ký tự gốc hay một nhóm ký tự gốc của bản rõ được thay thế bởi các từ, các ký hiệu khác hay kết hợp với nhau cho phù hợp với một phương thức nhất định và khoá.
  - **Phương thức mã hoá hoán vị:** là phương thức mã hoá mà các từ mã của bản rõ được sắp xếp lại theo một phương thức nhất định.

6. Hệ mật mã

- **Vai trò của hệ mật mã:**
  - Hệ mật mã phải che dấu được nội dung của văn bản rõ (PlainText).
  - Tạo các yếu tố xác thực thông tin, đảm bảo thông tin lưu hành trong hệ thống đến người nhận hợp pháp là xác thực (Authenticity).
  - Tổ chức các sơ đồ chữ ký điện tử, đảm bảo không có hiện tượng giả mạo, mạo danh để gửi thông tin trên mạng.

6. Hệ mật mã

- **Khái niệm cơ bản**
  - **Bản rõ** X được gọi là là bản tin gốc. Bản rõ có thể được chia nhỏ có kích thước phù hợp.
  - **Bản mã** Y là bản tin gốc đã được mã hoá. Ở đây ta thường xét phương pháp mã hóa mà không làm thay đổi kích thước của bản rõ, tức là chúng có cùng độ dài.
  - **Mã** là thuật toán E chuyển bản rõ thành bản mã. Thông thường chúng ta cần thuật toán mã hóa mạnh, cho dù kẻ thù biết được thuật toán, nhưng không biết thông tin về khóa cũng không tìm được bản rõ.

6. Hệ mật mã

- **Các thành phần của một hệ mật mã** :

Một hệ mã mật là bộ 5 (P, C, K, E, D) thoả mãn các điều kiện sau:

- **P** là không gian bản rõ: là tập hữu hạn các bản rõ có thể có.
- **C** là không gian bản mã: là tập hữu hạn các bản mã có thể có.
- **K** là không gian khoá: là tập hữu hạn các khoá có thể có.

Đối với mỗi $k \in K$ có một quy tắc mã $e_K: P \rightarrow C$ và một quy tắc giải mã tương ứng $d_K \in D$.

Với mỗi $e_K: P \rightarrow C$ và $d_K: C \rightarrow P$ là những hàm mà

$d_K(e_K(x))=x$ với mọi bản rõ $x \in P$.

Hàm giải mã d_k chính là ánh xạ ngược của hàm mã hóa e_k

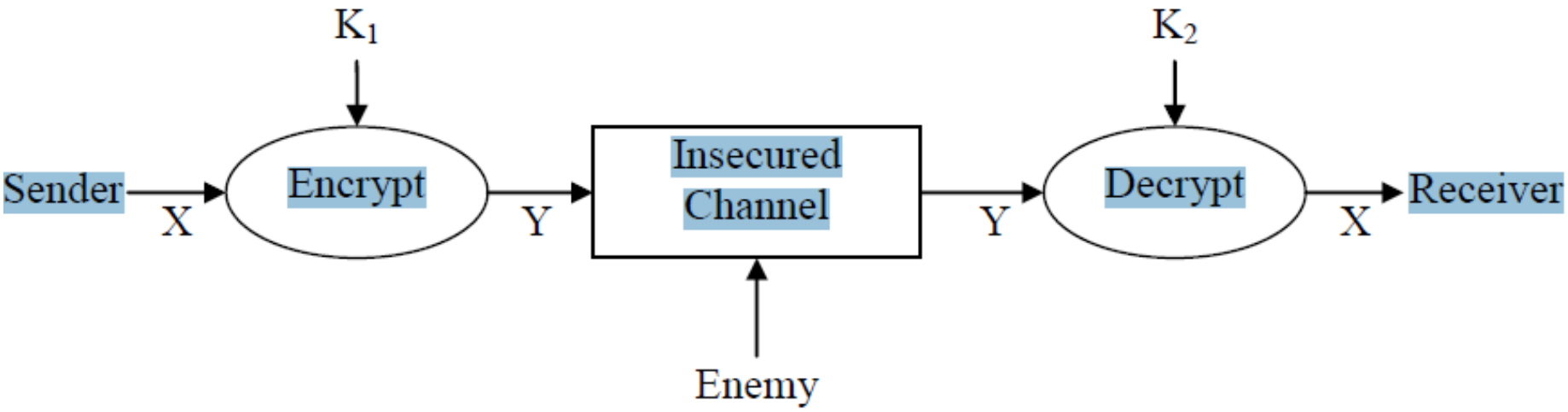
7.Tiêu chuẩn đánh giá hệ mật mã

- **Độ an toàn:** Một hệ mật được đưa vào sử dụng điều đầu tiên phải có độ an toàn cao.
  - Chúng phải có phương pháp bảo vệ mà chỉ dựa trên sự bí mật của các khoá, còn thuật toán thì công khai. 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
  - Bản mã C không được có các đặc điểm gây chú ý, nghi ngờ.

7.Tiêu chuẩn đánh giá hệ mật mã

- **Tốc độ mã và giải mã:** Khi đánh giá hệ mật mã chúng ta phải chú ý đến tốc độ mã và giải mã. Hệ mật tốt thì thời gian mã và giải mã nhanh.
- **Phân phối khóa:** Một hệ mật mã phụ thuộc vào khóa, khóa này được truyền công khai hay truyền khóa bí mật. Phân phối khóa bí mật thì chi phí sẽ cao hơn so với các hệ mật có khóa công khai. Vì vậy đây cũng là một tiêu chí khi lựa chọn hệ mật mã.

8. Mô hình truyền tin cơ bản của mật mã học và luật Kirchoff



Hình 1.1: Mô hình cơ bản của truyền tin bảo mật

8. Mô hình truyền tin cơ bản của mật mã học và luật Kirchoff

- **Theo luật Kirchoff (1835 - 1903)** (một nguyên tắc cơ bản trong mã hoá) thì: *toàn bộ cơ chế mã/giải mã trừ khoá là không bí mật đối với kẻ địch.*
- **Ý nghĩa của luật Kirchoff**: sự an toàn của các hệ mã mật không phải dựa vào sự phức tạp của thuật toán mã hóa sử dụng.

9. Một số ứng dụng của mã hóa 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
- Authentication System
- Secure E-commerce
- Virtual Private Network
- Wireless Encryption