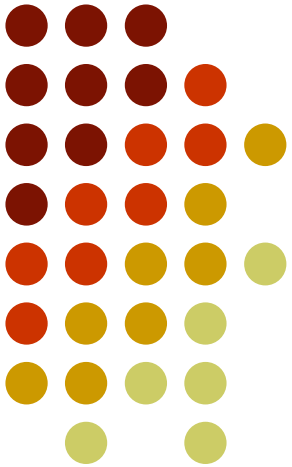
AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN

KHOA CÔNG NGHỆ THÔNG TIN – ĐẠI HỌC SÀI GÒN

ThS. Trương Tấn Khoa

truongtankhoa@sgu.edu.vn



GIỚI THIỆU MÔN HỌC

- Số tín chỉ: 3 (2LT + 1TH)
- Số tiết: 60 tiết
  - ✓ Lý thuyết: 30 tiết
  - ✓ Thực hành: 30 tiết
- Môn học cần:
  - ✓ Cơ sở dữ liệu, Xác suất thống kê, Toán cao cấp, Toán rời rạc, Mạng máy tính

MỤC TIÊU MÔN HỌC

- **Về kiến thức:**
  - ✓ Khái niệm: hệ thống thông tin mạng máy tính, an toàn và bảo mật thông tin trong các hệ thống thông tin.
  - ✓ Các kiến thức cơ bản về bảo mật thông tin mạng máy tính.
  - ✓ Các phương pháp bảo mật giúp sinh viên hiểu được làm thế nào để đảm bảo an toàn bảo mật thông tin

MỤC TIÊU MÔN HỌC

- **Về kỹ năng:**
  - ✓ Nắm được nguyên lý để thiết lập các biện pháp an toàn thông tin mức cơ bản.
  - ✓ Hiểu, áp dụng một số các thuật toán mã hóa cơ bản.
  - ✓ Sử dụng được các phần mềm hỗ trợ việc đảm bảo an toàn và bảo mật thông tin được trang bị sẵn trong các hệ điều hành, các phần mềm phổ dụng.

MỤC TIÊU MÔN HỌC

- **Về thái độ:**
  - ✓ Hiểu được các nguy cơ mất an toàn dữ liệu.
  - ✓ Hiểu được tính cấp thiết của vấn đề đảm bảo an toàn bảo mật dữ liệu.
  - ✓ Nhận thức được vai trò của việc bảo vệ dữ liệu, an toàn thông tin trong thời đại 4.0 hiện nay.

HÌNH THỨC ĐÁNH GIÁ

- **Điểm quá trình: 50%**
  - ✓ Chuyên cần: 10%
  - ✓ Điểm thực hành bài tập trên lớp: 10%
  - ✓ Điểm đồ án: 30%
- **Điểm cuối kỳ: 50%**
  - ✓ Thi tự luận + trắc nghiệm (nếu có)

NỘI DUNG MÔN HỌC

- Chương 1: Giới thiệu tổng quan
- Chương 2: Cơ sở lý thuyết số học
- Chương 3: Các hệ mã hóa khóa bí mật
- Chương 4: Các hệ mã khóa công khai
- Chương 5: Chữ ký điện tử và hàm băm
- Chương 6: Quản lý khóa trong hệ thống mật mã

TÀI LIỆU THAM KHẢO

[1] William Stallings, “Cryptography and Network Security Principles and Practices, Fourth Edition”, Prentice Hall, 2005.

[2] Nguyễn Bình, “Giáo trình mật mã học”, Học viện bưu chính viễn thông, NXB bưu điện, 2004.

[3] “Giáo trình An toàn và Bảo mật thông tin”, Đại học Bách Khoa Hà Nội.

Chương 1:
GIỚI THIỆU TỔNG QUAN

1. Tại sao phải bảo vệ thông tin

- Thông tin là một 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.

Chương 1:
GIỚI THIỆU TỔNG QUAN

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

- Khái niệm hệ thống: Hệ thống là một tập hợp máy tính bao gồm các thành phần:
  - Phần cứng
  - Phần mềm
  - Dữ liệu làm việc được tích lũy qua thời gian

Chương 1:
GIỚI THIỆU TỔNG QUAN

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

- Tài sản của hệ thống bao gồm:
  - Phần cứng
  - Phần mềm
  - Dữ liệu
  - Truyền thông giữa các máy tính trong hệ thống
  - Môi trường làm việc
  - Con người

Chương 1:
GIỚI THIỆU TỔNG QUAN

3. Các mối đe dọa và các biện pháp ngăn chặn

- Có 3 hình thức chủ yếu đe dọa 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.
  - 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.

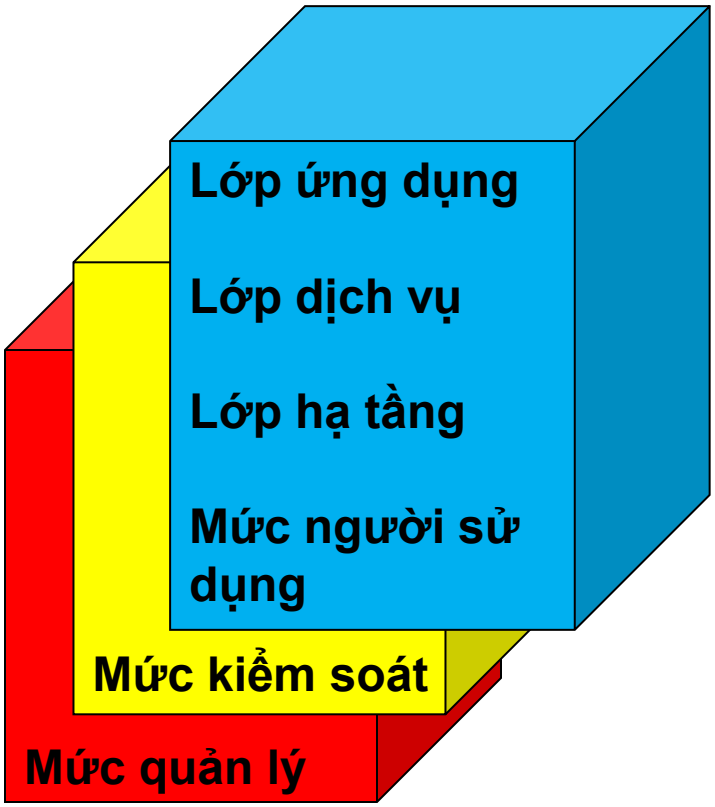
Chương 1:
GIỚI THIỆU TỔNG QUAN

3. Các mối đe dọa 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 với hệ thống
  - Những đối tượng bên ngoài hệ thống (hacker, cracker), thường tấn công qua những đường kết nối với hệ thống như Internet chẳng hạn.
  - Các phần mềm (chẳng hạn spyware, adware…) chạy trên hệ thống.

Chương 1:
GIỚI THIỆU TỔNG QUAN

3. Các mối đe dọa và các biện pháp ngăn chặn



Kiểm soát truy nhập
Chứng thực
Chống chối bỏ
Bảo mật số liệu
An toàn luồng tin
Nguyên vẹn số liệu
Khả dụng
Riêng tư

Nguy cơ
Phá hủy
Sửa đổi
Cắt bỏ
Bóc, tiết lộ
Gián đoạn
Tấn công

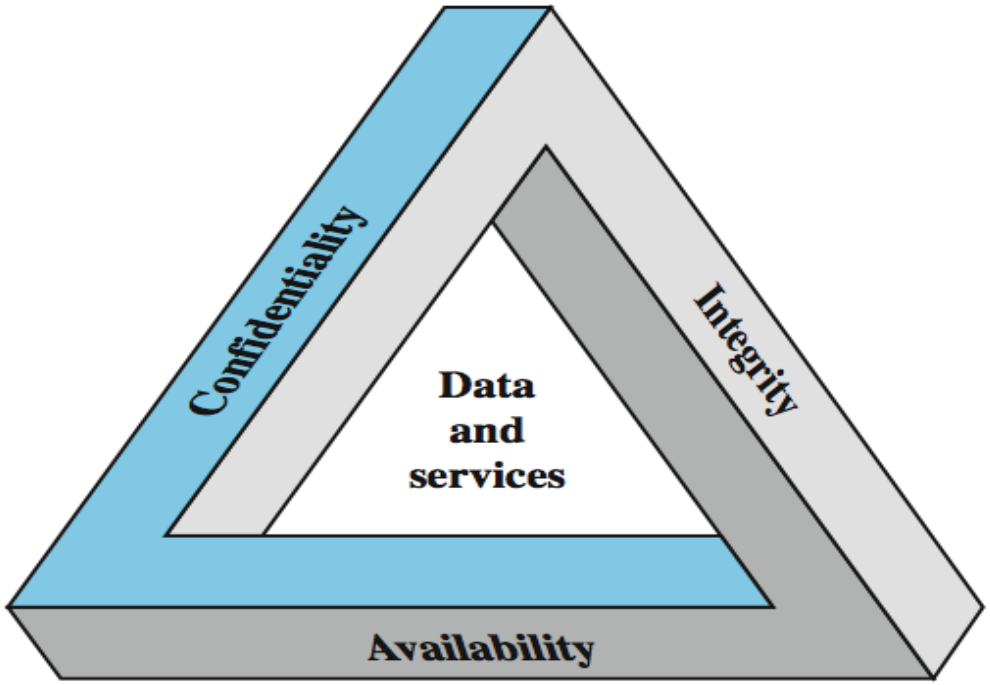
Chương 1:
GIỚI THIỆU TỔNG QUAN

3. Các mối đe dọa 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 quy định của tổ chức nhằm đảm bảo tính an toàn bảo mật của hệ thống

Chương 1:
GIỚI THIỆU TỔNG QUAN

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



Chương 1:
GIỚI THIỆU TỔNG QUAN

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 những người có thẩm quyền.

Chương 1:
GIỚI THIỆU TỔNG QUAN

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

Thêm vào đó sự chính xác của thông tin còn được đánh giá bởi:

- **Tính xác thực** (Authentication): - Đảm bảo rằng dữ liệu nhận được chắc chắn 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.

Chương 1:
GIỚI THIỆU TỔNG QUAN

5. Các chiến lược an toàn hệ thống

- **Giới hạn quyền hạn tối thiểu** (Last Privilege): theo nguyên tắc này bất kỳ một đối tượng nào cũng chỉ có những quyền hạn nhất định đối với tài nguyên mạng**.**
- **Bảo vệ theo chiều sâu** (Defence In Depth): Không nên dựa vào một chế độ an toàn dù cho chúng rất mạnh, mà nên tạo nhiều cơ chế an toàn để tương hỗ cho nhau.
- **Nút thắt** (Choke Point): Tạo ra một "cửa khẩu" hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là "cửa khẩu" này.

Chương 1:
GIỚI THIỆU TỔNG QUAN

5. Các chiến lược an toàn hệ thống

- **Điểm nối yếu nhất** (Weakest Link): Chiến lược này dựa trên nguyên tắc: "Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất".
- **Tính toàn cục:** Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ.
- **Tính đa dạng bảo vệ**: Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau. Nếu không, chỉ cần có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

Chương 1:
GIỚI THIỆU TỔNG QUAN

6. Các mức bảo vệ trên mạng

- **Quyền truy nhập:** Là lớp bảo vệ trong cùng nhằm kiểm soát các tài nguyên của mạng và quyền hạn trên tài nguyên đó.
- **Đăng ký tên /mật khẩu**: Thực ra đây cũng là kiểm soát quyền truy nhập, nhưng không phải truy nhập ở mức thông tin mà ở mức hệ thống.
- **Mã hóa dữ liệu**: Dữ liệu bị biến đổi từ dạng nhận thức được sang dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhận (giải mã).
- **Bảo vệ vật lý:** ngăn chặn các truy nhập vật lý vào hệ thống

Chương 1:
GIỚI THIỆU TỔNG QUAN

6. Các mức bảo vệ trên mạng

Tường lửa (Fire Walls)

⬇

Bảo vệ vật lý (Physical Walls)

⬇

Mã hóa dữ liệu (Data Encryption)

⬇

Đăng ký và mật khẩu

⬇

Quyền truy nhập (Access Rights)

⬇

Thông tin (Informations)

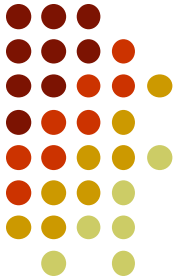
Mức độ bảo vệ

Chương 1:
GIỚI THIỆU TỔNG QUAN

6. Các mức bảo vệ trên mạng

- **Tường lửa:** Ngăn chặn thâm nhập trái phép và lọc bỏ các gói tin không muốn gửi hoặc nhận vì các lý do nào đó để bảo vệ một máy tính hoặc cả mạng nội bộ (intranet).
- **Quản trị mạng:** Công tác quản trị mạng máy tính phải được thực hiện một cách khoa học đảm bảo các yêu cầu sau: *-Toàn bộ hệ thống hoạt động bình thường trong giờ làm việc*; *-Có hệ thống dự phòng khi có sự cố về phần cứng hoặc phần mềm xảy ra*; *-Backup dữ liệu quan trọng theo định kỳ; -Bảo dưỡng mạng theo định kỳ; -Bảo mật dữ liệu, phân quyền truy cập, tổ chức nhóm làm việc trên mạng.*

Chương 1:
GIỚI THIỆU TỔNG QUAN



7. Các phương pháp bảo mật

Các phương pháp quan trọng như:

- ✓ **Viết mật mã:** đảm bảo tính bí mật của thông tin truyền thông
- ✓ **Xác thực quyền:** được sử dụng để xác minh, nhận dạng quyền hạn của các thành viên tham gia.

Chương 1:
GIỚI THIỆU TỔNG QUAN

8. 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.*

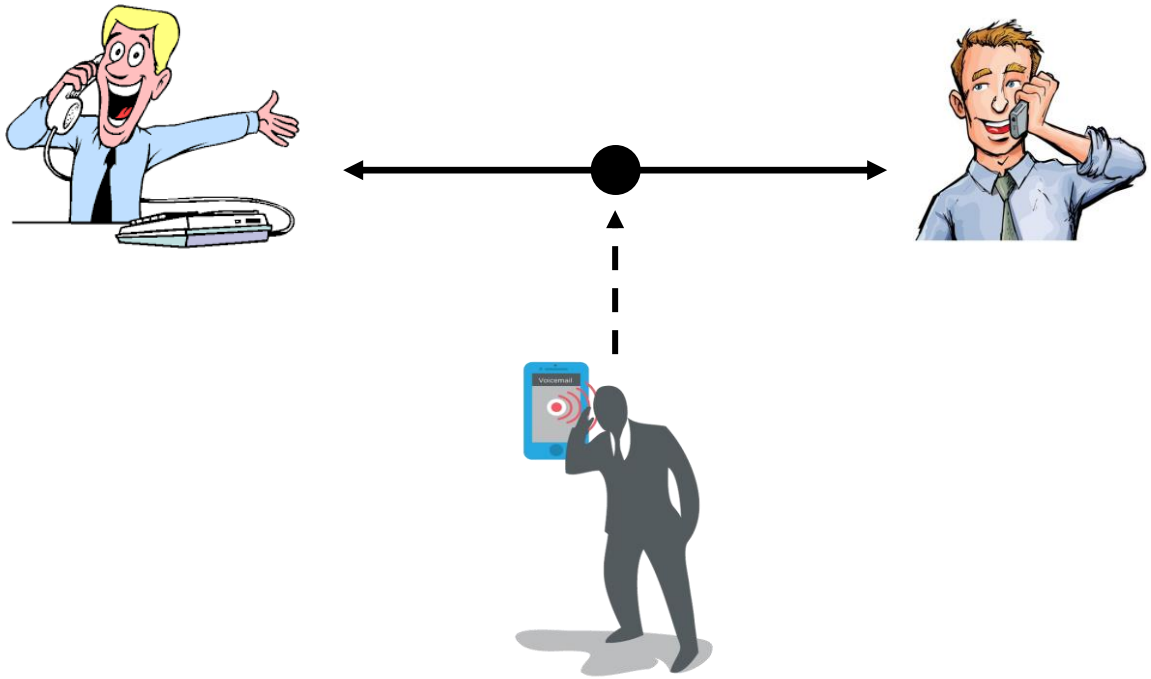
- ✓ Lập mã **bao gồm 2 quá trình:** *mã hóa* và *giải mã*. Các sản phẩm của lĩnh vực này là các hệ mã mật, các hàm băm, các hệ chữ ký điện tử, các cơ chế phân phối, quản lý khóa và các giao thức mật mã.
- ✓ Phá mã: Nghiên cứu các phương pháp phá mã hoặc tạo mã giả. Sản phẩm của lĩnh vực này là các phương pháp phá mã, các phương pháp giả mạo chữ ký, các phương pháp tấn công các hàm băm và các giao thức mật mã.

Chương 1:
GIỚI THIỆU TỔNG QUAN

8. An toàn thông tin bằng mật mã

Cách hiểu truyền thống: *giữ bí mật nội dung* trao đổi.

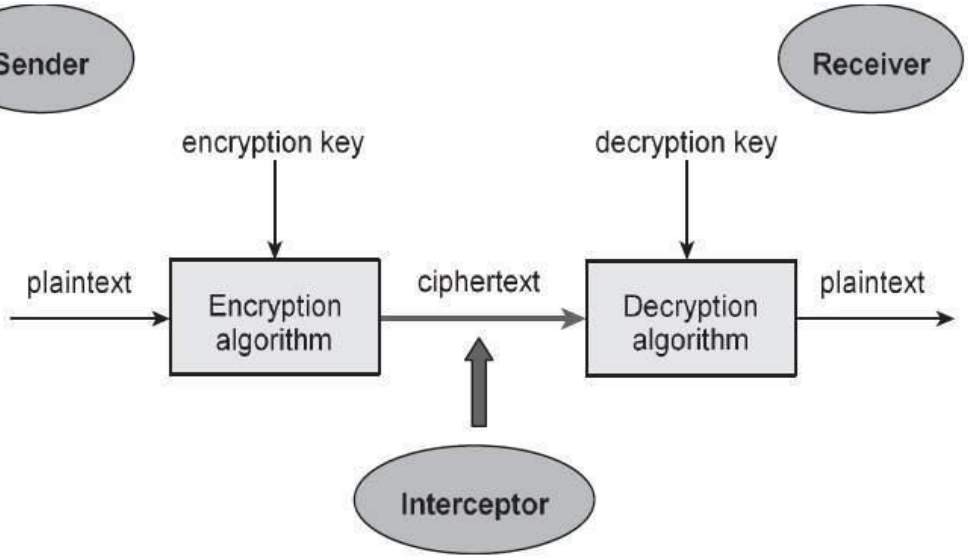
GỬI và NHẬN trao đổi với nhau trong khi TRUNG GIAN tìm cách "nghe lén".



Chương 1:
GIỚI THIỆU TỔNG QUAN

8. 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 hóa các thông báo trước khi gửi chúng đi và tiến hành giải mã chúng lúc nhận được.



Chương 1:
GIỚI THIỆU TỔNG QUAN

8. An toàn thông tin bằng mật mã

- Có 2 phương pháp mã hóa cơ bản: thay thế và hoán vị:
  - ✓ Phương pháp mã hóa thay thế: là phương thức mã hóa 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 khóa.
  - ✓ Phương thức mã hóa hoán vị: là phương thức mã hóa mà các từ mã của bản rõ được sắp xếp lại theo một phương thức nhất định.

Chương 1:
GIỚI THIỆU TỔNG QUAN

9. 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.

Chương 1:
GIỚI THIỆU TỔNG QUAN

9. Hệ mật mã

- **Khái niệm cơ bản:**
  - ✓ Bản rõ (Plain Text) X được gọi là bản tin gốc. Bản rõ có thể được chia nhỏ có kích thước phù hợp.
  - ✓ Bản mã (Cipher Text) Y là bản tin gốc đã được mã hóa. Ở đây người 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 (Coding) là thuật toán E để 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 thể tìm được bản rõ.

Chương 1:
GIỚI THIỆU TỔNG QUAN

9. Hệ mật mã

- **Khái niệm cơ bản:**
  - ✓ Khóa K (key) là thông tin tham số dùng để mã hóa, chỉ có người gửi và người nhận biết. Khóa độc lập với bản rõ và có độ dài phù hợp với yêu cầu bảo mật.
  - ✓ Mã hóa (Encoding) là quá trình chuyển bản rõ thành bản mã, thông thường bao gồm việc áp dụng thuật toán mã hóa và một số quá trình xử lý thông tin kèm theo.
  - ✓ Giải mã (Decoding) chuyển bản mã thành bản rõ, đây là quá trình ngược lại của mã hóa.

Chương 1:
GIỚI THIỆU TỔNG QUAN

9. Hệ mật mã

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

Một hệ mật mã là bộ 5 thành phần (**P, C, K, E, D**) thỏa đk:

- **P**: là không gian bản rõ, gồm 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 khóa, là tập hữu hạn các khóa có thể có.

Đối với mỗi k ∈ **K** có một quy tắc mã e_k: P → C và một quy tắc giải mã tương ứng d_k ∈ **D.**

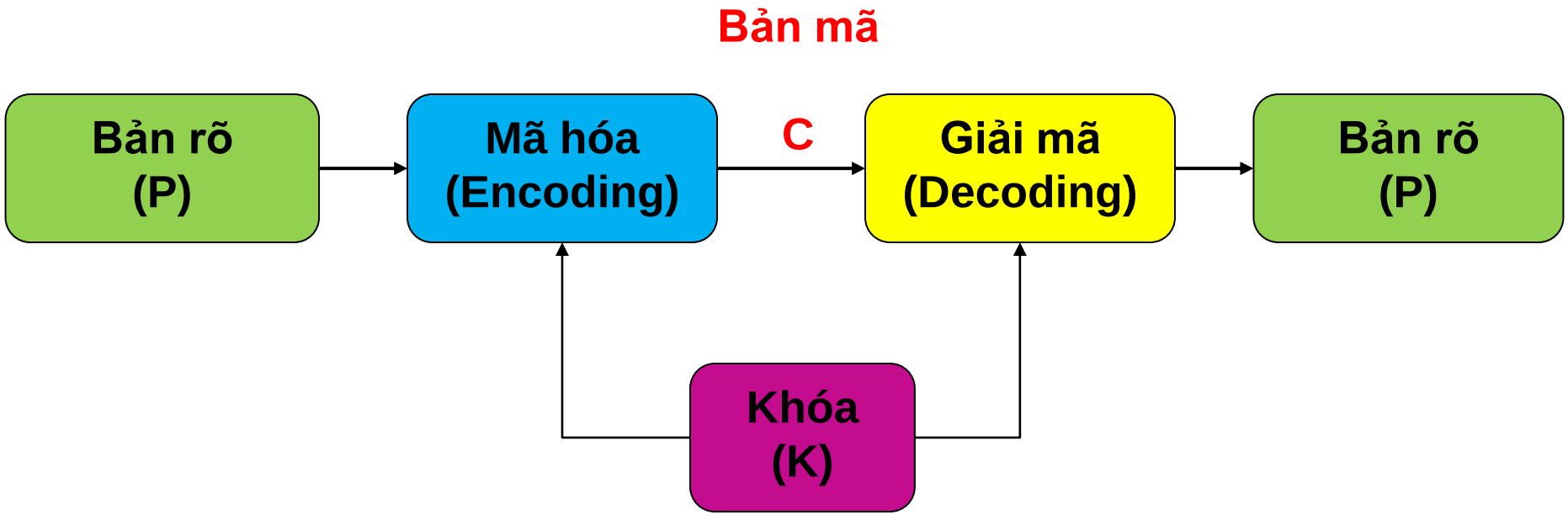
Với mỗi e_k: P → C và d_k: C → P là những hàm mà:

$$d_k(e_k(x)) = x \text{ với mọi bản rõ } x \in P$$

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

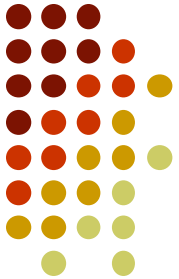
Chương 1:
GIỚI THIỆU TỔNG QUAN

Mô hình hệ mật mã



Quá trình mã hóa và giải mã thông tin

Chương 1:
GIỚI THIỆU TỔNG QUAN



10. Phân loại hệ mật mã

- Hệ mật đối xứng (hay còn gọi là hệ mật mã khóa bí mật) – Symmetric key cryptosystem: là những hệ mật dùng chung một khóa cả trong quá trình mã hóa và giải mã dữ liệu. Do đó khóa phải được bí mật tuyệt đối. Một số thuật toán nổi tiếng trong mã hóa đối xứng là: DES, Triple DES (3DES), RC4, AES…
- Hệ mật mã bất đối xứng (hay còn gọi là hệ mật mã khóa công khai) – Public key cryptosytem: Các hệ mật này dùng một khóa để mã hóa và sau đó dùng một khóa khác để giải mã. Các khóa này tạo nên từng cặp chuyển đổi ngược nhau và không có khóa nào có thể suy được từ khóa kia.

Chương 1:
GIỚI THIỆU TỔNG QUAN

10. Phân loại hệ mật mã

Trong hệ mật mã bất đối xứng, khóa dùng để mã hoá có thể công khai nhưng khóa dùng để giải mã phải giữ bí mật. Do đó trong thuật toán này có 2 loại khóa: Khóa để mã hóa được gọi là khóa công khai (public key), khóa để giải mã được gọi là khóa bí mật (private key)

Một số thuật toán mã hóa công khai nổi tiếng như: Diffle-Helman, RSA…

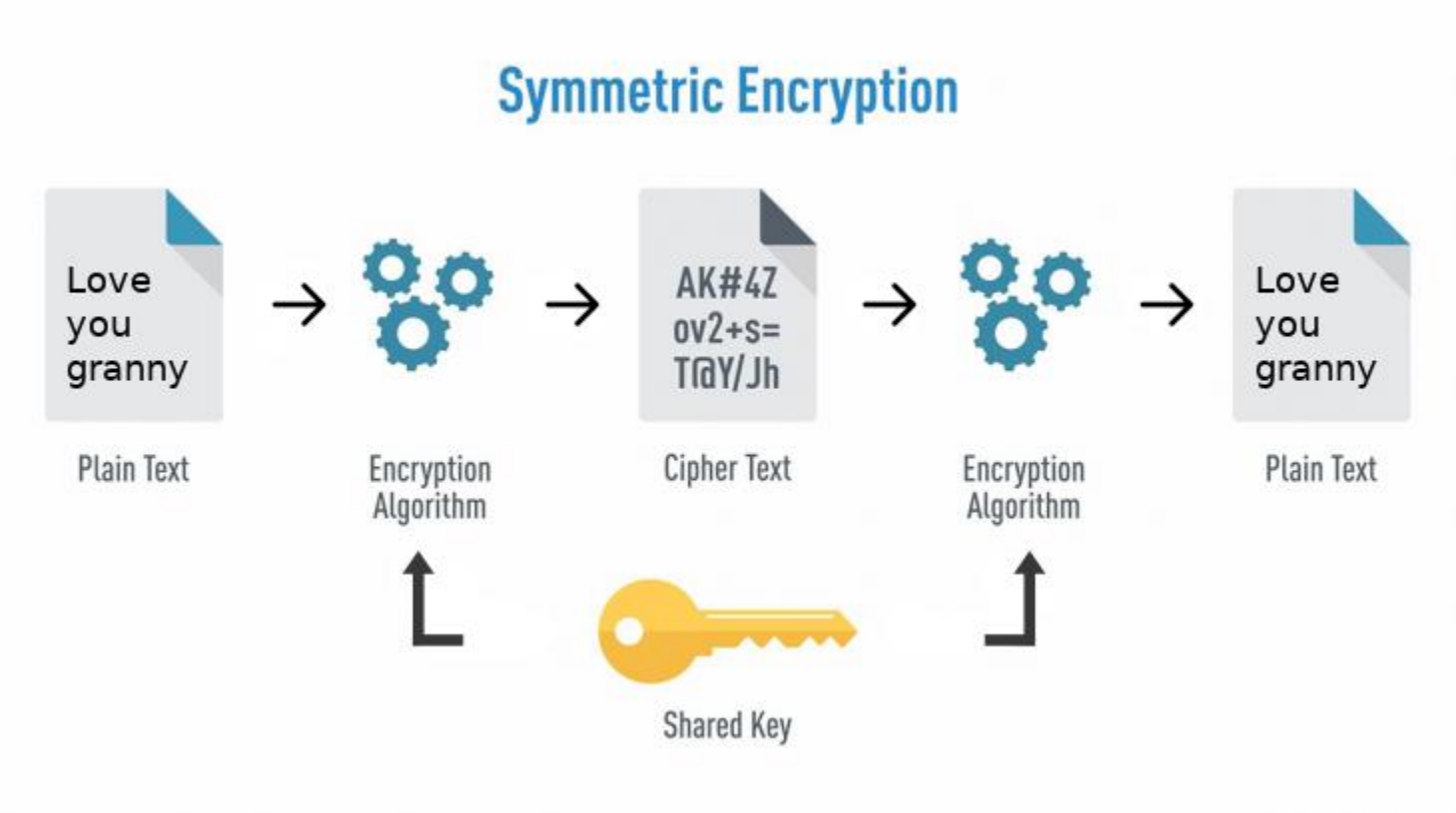
Chương 1:
GIỚI THIỆU TỔNG QUAN

10. Các phương pháp mã hóa

- **Có 3 phương pháp chính cho việc mã hóa và giải mã**
  - ✓ Sử dụng khóa đối xứng
  - ✓ Sử dụng khóa bất đối xứng
  - ✓ Sử dụng hàm băm một chiều

Chương 1:
GIỚI THIỆU TỔNG QUAN

10.1. Mã hóa đối xứng



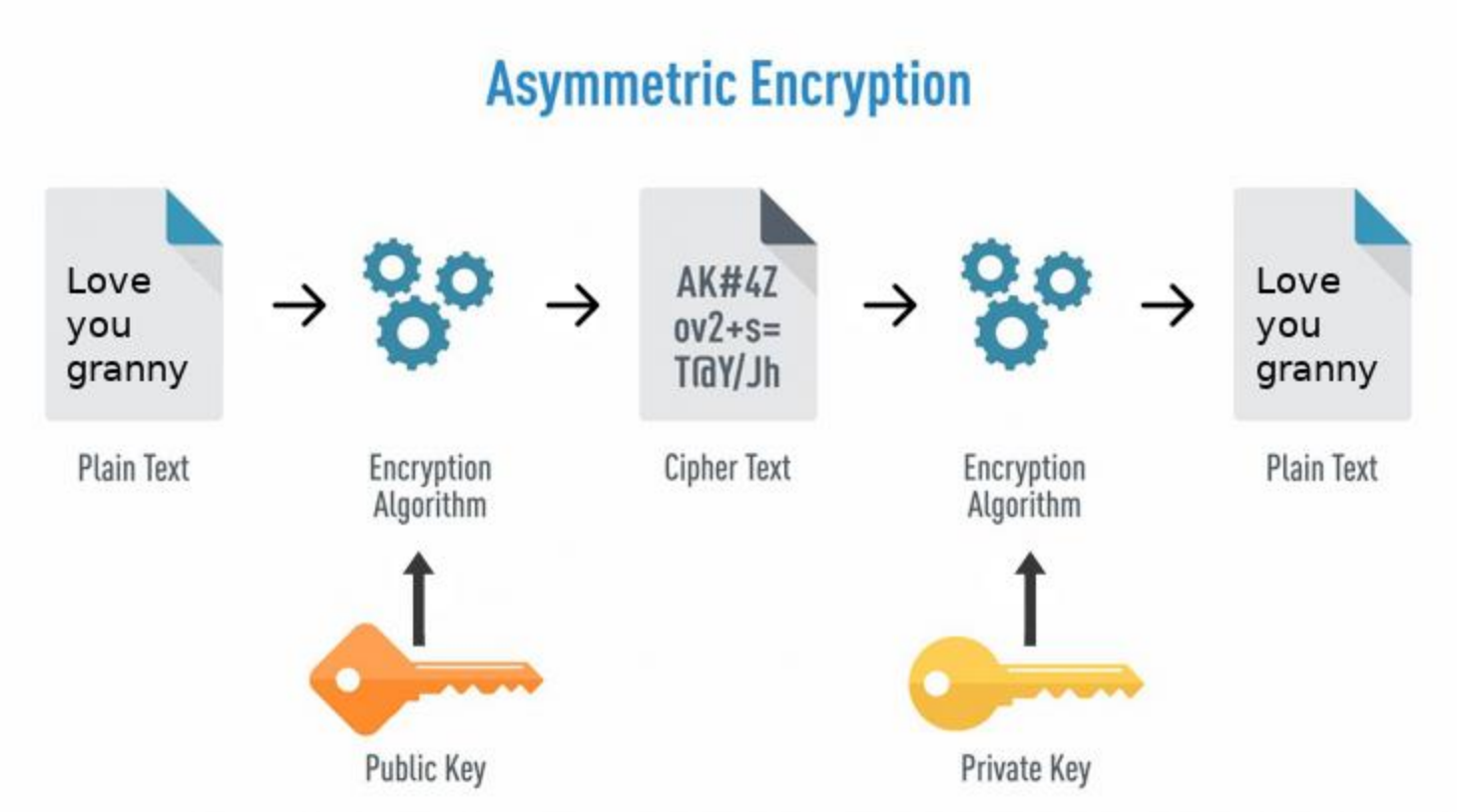
Chương 1:
GIỚI THIỆU TỔNG QUAN

10.1. Mã hóa đối xứng

- Các khóa giống nhau được sử dụng cho việc mã hóa và giải mã.
- Thuật toán mã hóa sử dụng khóa đối xứng thường được biết đến là DES (Data Encryption Standard).
- Các thuật toán mã hóa đối xứng khác được biết đến như:
  - Triple DES, DESX, GDES, RDES – 168 bit key.
  - RC2, RC4, RC5 – variable length up to 2048 bits.
  - IDEA – basic of PGP -128 bit key.

Chương 1:
GIỚI THIỆU TỔNG QUAN

10.2. Mã hóa bất đối xứng



Chương 1:
GIỚI THIỆU TỔNG QUAN

10.2. Mã hóa bất đối xứng

- Các khóa dùng cho mã hóa và giải mã khác nhau nhưng cùng một mẫu và là cặp đôi duy nhất (khóa private/public)
- Khóa private chỉ được biết đến bởi người nhận
- Khóa public được biết đến bởi nhiều người hơn, nó được sử dụng bởi những người đáng tin cậy đã được xác thực.
- Thuật toán mã hóa sử dụng khóa bất đối xứng thường được biết đến là RSA (Rivest, Shamir, Adleman 1978)

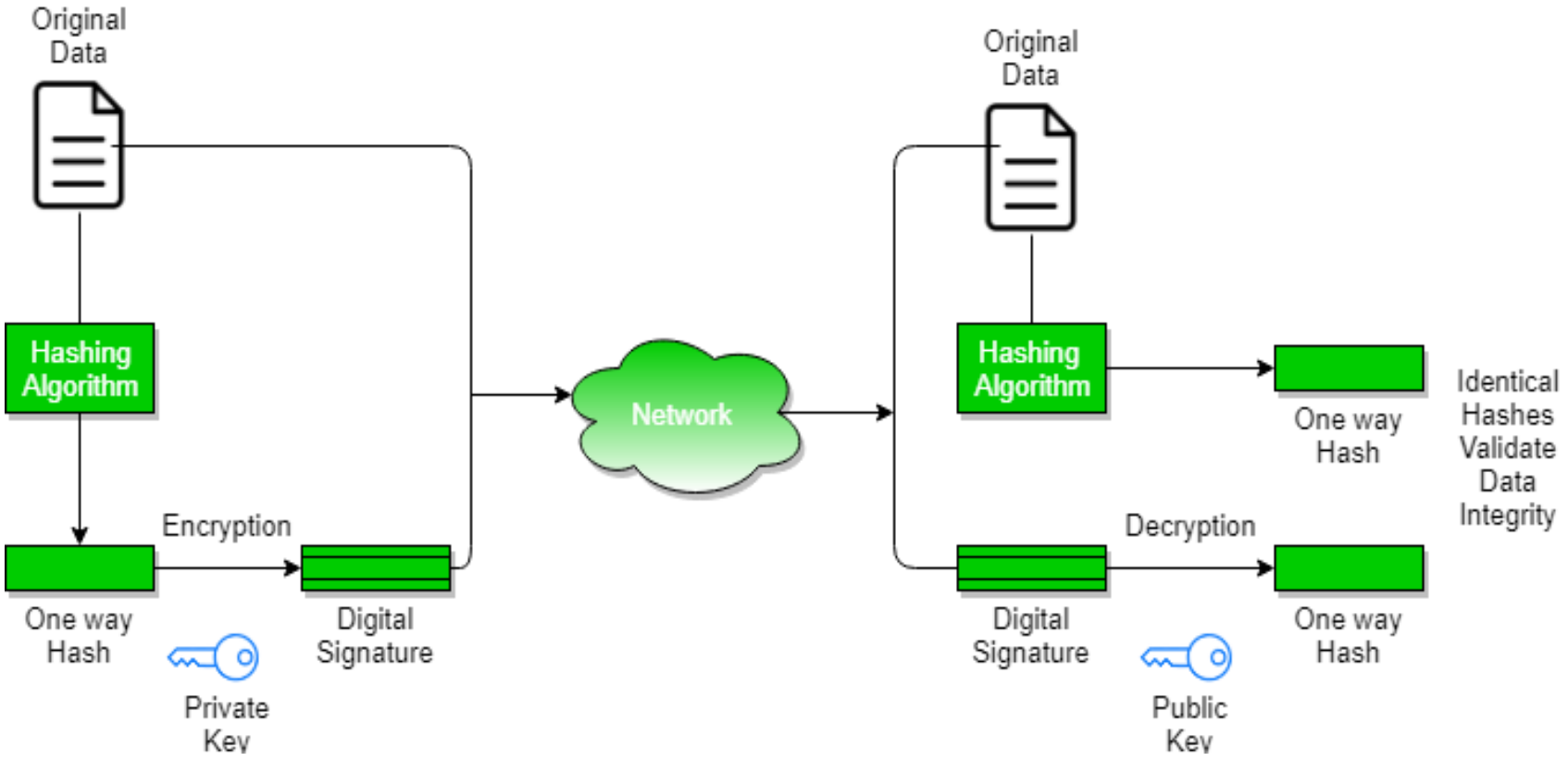
Chương 1:
GIỚI THIỆU TỔNG QUAN

10.3. Hàm băm

- Một hàm băm H nhận được một thông báo *m* với một độ dài bất kỳ từ đầu vào và đưa ra một xâu bít *h* có độ dài cố định ở đầu ra *h = H(m).*
- Hàm băm là một hàm một chiều, điều đó có nghĩa là ta không thể tính toán được đầu vào *m* nếu biết đầu ra *h.*
- Thuật toán sử dụng hàm băm thường được biết đến là MD5.

Chương 1:
GIỚI THIỆU TỔNG QUAN

10.4. Chữ ký số



Chương 1:
GIỚI THIỆU TỔNG QUAN

11. Xác thực quyền

Tức là xác minh quyền hạn của các thành viên tham gia trong hệ thống truyền thông.

- Phương pháp phổ biến:
  - ✓ Sử dụng Password: để xác thực người sử dụng.
- Sử dụng **Kerberos**: phương thức mã hóa và xác thực trong AD của công nghệ Window.
- Sử dụng **Secure Remote Password** (SRP) là một giao thức để xác thực đối với các truy cập từ xa.
- Sử dụng Hardware Token, SSL/TLS để mã hóa xác thực trong VPN, Web.
- Ngoài ra còn có X.509 Public Key, PGP Public Key, SPKI Public Key, XKMS Public Key, XML Digital Signature.

Chương 1:
GIỚI THIỆU TỔNG QUAN

12. 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 ta phải có phương pháp bảo vệ mà chỉ dựa trên sự bí mật của khóa, 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 rất nhiều so với giá trị của thông tin đã được mã hóa thì thuật toán đó tạm thời được coi an toàn
    - ✓ Nếu thời gian cần thiết dùng để phá vỡ thuật toán quá lâu.
    - ✓ Nếu lượng dữ liệu cần thiết để phá vỡ một thuật toán quá lớn so với lượng dữ liệu đã được mã hóa bởi nó.

Chương 1:
GIỚI THIỆU TỔNG QUAN

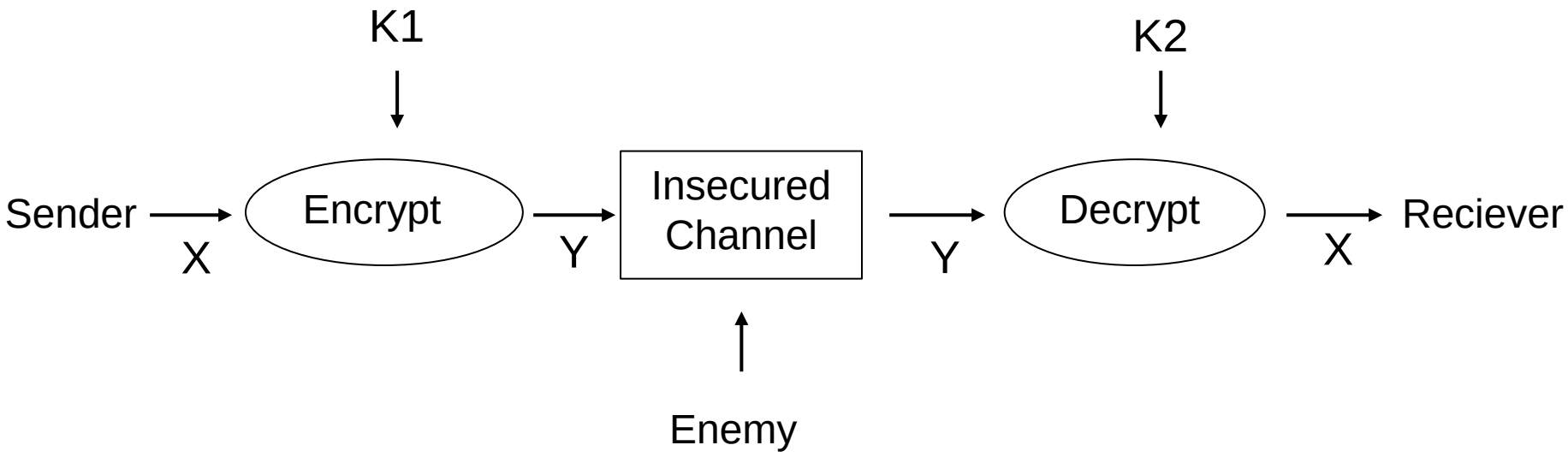
12. Tiêu chuẩn đánh giá hệ mật mã

- Bản mã C không được có các đặc điểm gây chú ý, nghi ngờ.

- **Tốc độ mã và giải mã**: Hệ mật mã tốt thì thời gian mã và giải mã phải nhanh.
- **Phân phối khóa**: Một hệ mật mã phụ thuộc vào khóa, khóa này được truyền công khai hay truyền bí mật. Phân phối khóa bí mật thì chi phí sẽ cao hơn. Đây cũng là tiêu chí để lựa chọn một hệ mã.

Chương 1:
GIỚI THIỆU TỔNG QUAN

13. Mô hình truyền tin an toàn và luật Kirchoff

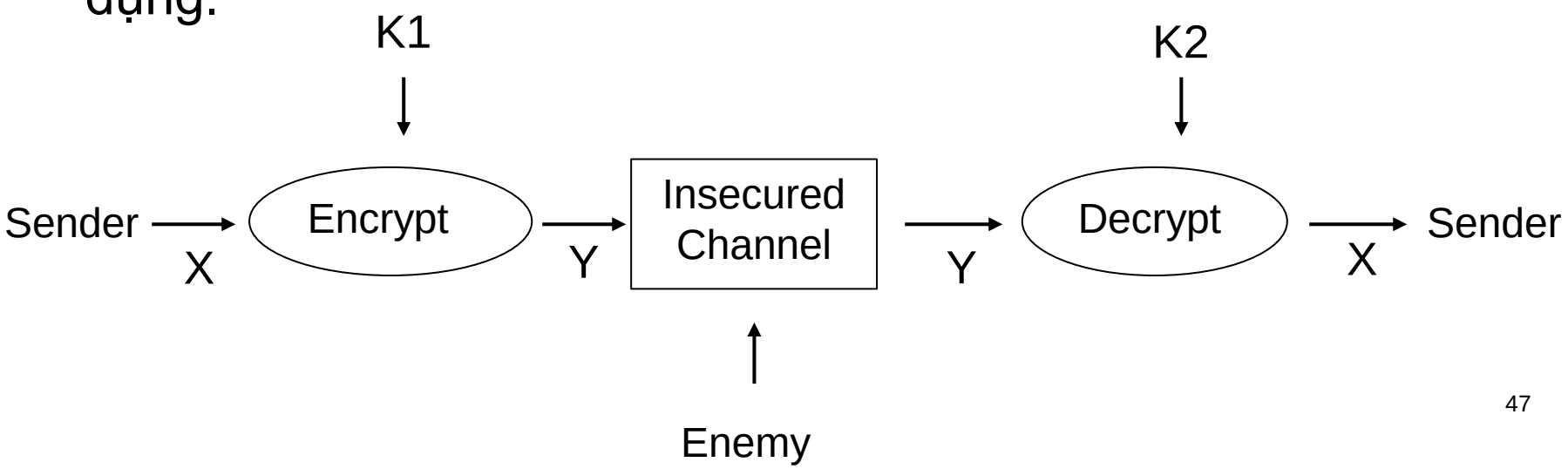


Hình 1.1: Mô hình cơ bản của truyền tin bảo mật

Chương 1:
GIỚI THIỆU TỔNG QUAN

13. Mô hình truyền tin an toàn và luật Kirchoff

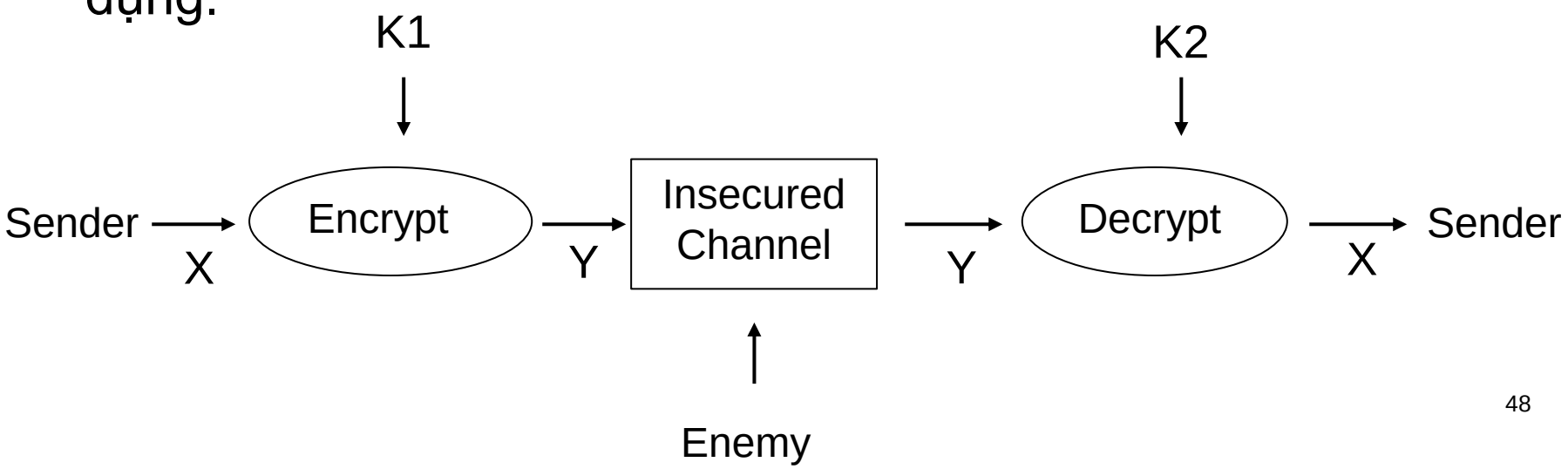
- **Theo luật Kirchoff (1835 - 1903)** (một nguyên tắc cơ bản trong mã hóa) thì: toàn bộ cơ chế mã/giải mã trừ khóa là không bí mật đối với kẻ địch.
- **Ý nghĩa của luật Kirchoff:** sự an toàn của các hệ mã mật không phải dựa vào sự phức tạp của thuật toán mã hóa sử dụng.



Chương 1:
GIỚI THIỆU TỔNG QUAN

13. Mô hình truyền tin an toàn và luật Kirchoff

- **Theo luật Kirchoff (1835 - 1903)** (một nguyên tắc cơ bản trong mã hóa) thì: toàn bộ cơ chế mã/giải mã trừ khóa 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.



Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

Các kỹ thuật mã hóa được sử dụng ngày nay là kết quả của một lịch sử phát triển lâu dài. Từ thời xa xưa, người ta đã sử dụng mật mã để truyền thông tin an toàn.

Sau đây là lịch sử của mật mã học đã dẫn đến các phương pháp tiên tiến và tinh vi được sử dụng trong ngành mã hóa kỹ thuật số hiện đại.

Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

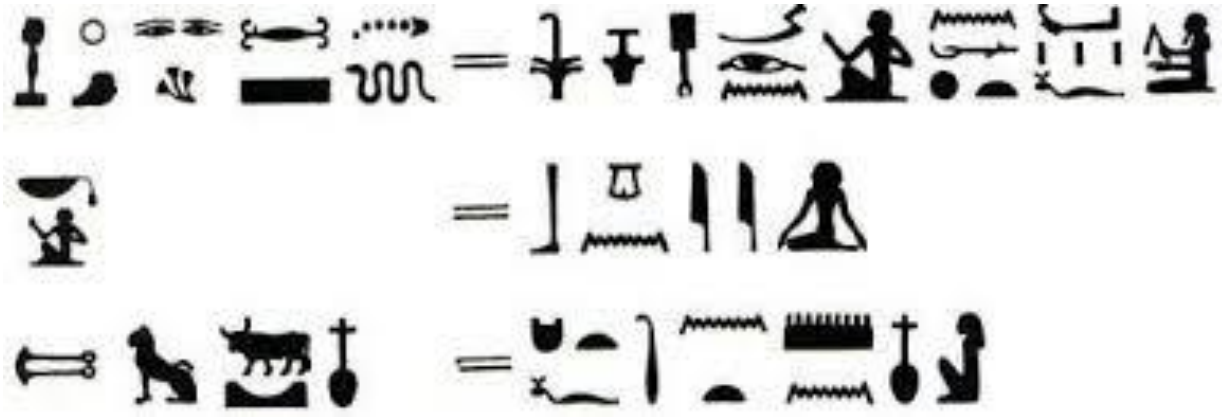
- **Khởi nguồn từ thời cổ đại**

Các kỹ thuật mã hóa sơ khai được biết đến sự tồn tại trong thời cổ đại, khi mà hầu hết các nền văn minh ban đầu dường như đã sử dụng mật mã học ở một mức độ nào đó. Sự thay thế bằng biểu tượng, hình thức mã hóa cơ bản nhất, xuất hiện trong cả hai chữ viết của Ai Cập và Lưỡng Hà cổ đại.

Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

- **Khởi nguồn từ thời cổ đại**



Ví dụ đầu tiên được biết đến về loại mật mã này được tìm thấy trong ngôi mộ của một quý tộc Ai Cập tên là Khnumhotep II, sống khoảng 3900 năm trước.

Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

- **Khởi nguồn từ thời cổ đại**

Ví dụ đầu tiên được biết đến về việc mật mã được sử dụng để bảo vệ thông tin nhạy cảm là vào khoảng 3500 năm trước khi một người ghi chép từ Lưỡng Hà sử dụng mật mã để giấu một công thức men gốm, được sử dụng trên các bảng tính bằng đất sét.

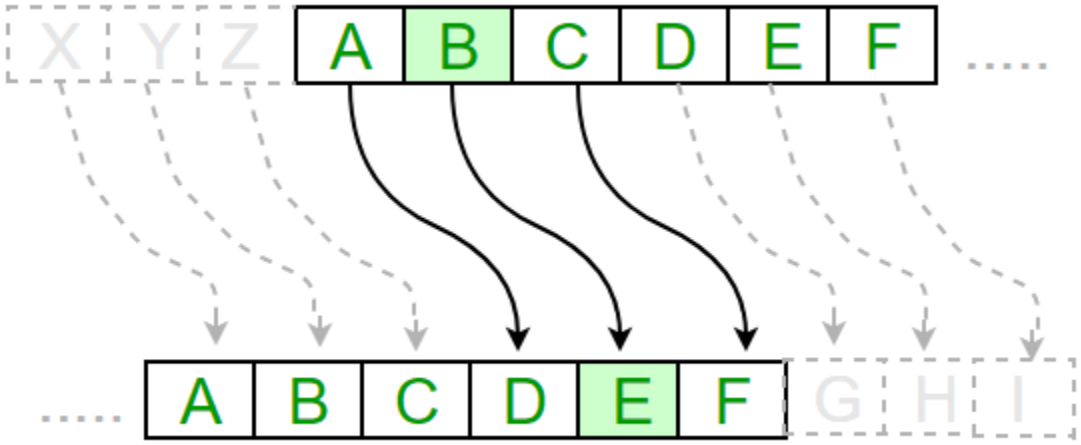
Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

- Sau thời kỳ cổ đại, mật mã đã được sử dụng rộng rãi để bảo vệ thông tin quân sự quan trọng, mật mã vẫn được dùng cho mục đích này cho đến ngày nay.
- Có lẽ mật mã tiên tiến nhất trong thế giới cổ đại được ghi nhận là do người La Mã. Một ví dụ nổi bật của mật mã La Mã, được gọi là mật mã Caesar, trong đó mỗi ký tự trong thông điệp được thay thế bằng một ký tự cách nó một đoạn trong bảng chữ cái Latin. Bằng cách biết cơ chế này và khoảng cách dịch chuyển các chữ cái, người nhận có thể giải mã thành công thông điệp.

Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học



Hệ mã Ceasar (Shift = 3)

Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

- **Phát triển trong thời Trung cổ và Phục hưng**

- Trong suốt thời Trung cổ, mật mã học ngày càng trở nên quan trọng, những mật mã thay thế, với mật mã Caesar làm ví dụ, vẫn là tiêu chuẩn. Tuy nhiên vẫn còn tương đối nguyên thủy.
- Al-Kindi, một nhà toán học Ả Rập nổi tiếng, đã phát triển một kỹ thuật gọi là phân tích tần suất vào khoảng năm 800 sau Công nguyên, cho thấy rằng mật mã thay thế dễ bị giải. Lần đầu tiên, những người làm công việc giải mã các thông điệp được mã hóa được tiếp cận một phương pháp giải mã có hệ thống. Điều này thúc đẩy mật mã học phải tiến xa hơn nữa để duy trì tính hữu ích của nó.

Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

Năm 1465, Leone Alberti đã phát triển mã hóa đa bản thể, được coi là giải pháp chống lại kỹ thuật phân tích tần suất của Al-Kindi. Trong một mật mã đa bản thể, một thông điệp được mã hóa bằng cách sử dụng hai bảng chữ cái riêng biệt. Một là bảng chữ cái dùng để viết thông điệp ban đầu, bảng còn lại là một bảng chữ cái hoàn toàn khác biệt mà qua đó thông điệp ban đầu sẽ được mã hóa. Kết hợp với mật mã thay thế truyền thống, mật mã đa bản thể giúp tăng cường bảo mật cho thông tin được mã hóa. Trừ phi người đọc biết bảng chữ cái mà thông điệp ban đầu dựa vào, kỹ thuật phân tích tần suất sẽ không tác dụng.

Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

Các phương pháp mã hóa thông tin mới cũng được phát triển trong thời kỳ Phục hưng, bao gồm một phương pháp ban đầu của mã hóa nhị phân được phát minh bởi học giả nổi tiếng Sir Francis Bacon vào năm 1623.

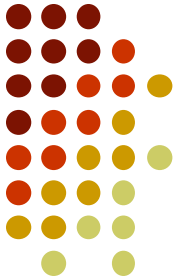
Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

- **Những tiến bộ trong các thế kỷ gần đây**

Khoa học mật mã tiếp tục phát triển mạnh trong nhiều thế kỷ. Một bước đột phá lớn trong mật mã học đã được mô tả bởi Thomas Jefferson trong thập niên 1970. Phát minh của ông được gọi là bánh xe mã hóa gồm 36 vòng chữ cái trên bánh xe chuyển động được sử dụng để thu được kết quả mã hóa phức tạp. Khái niệm này quá tiên tiến nên đã được dùng làm nền tảng cho mật mã quân sự của Mỹ đến cuối Thế chiến thứ hai.

Chương 1:
GIỚI THIỆU TỔNG QUAN



14. Lược sử mật mã học

- **Những tiến bộ trong các thế kỷ gần đây**

Thế chiến II cũng đã chứng kiến ví dụ tuyệt vời về mật mã tương tự, được gọi là máy Enigma. Giống như bánh xe mã hóa, thiết bị này được sử dụng bởi phe Phát Xít, sử dụng các bánh xe quay để mã hóa một thông điệp, làm cho nó hầu như không thể đọc được nếu không có một máy Enigma khác.

Công nghệ máy tính thời kỳ đầu đã được sử dụng để giúp giải mật mã Enigma. Việc giải mã thành công các thông điệp Enigma vẫn được xem là một đóng góp quan trọng vào chiến thắng của phe Đồng Minh.

Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

- **Mật mã học trong kỷ nguyên máy tính**

- Với sự nổi lên của máy tính, mật mã đã phát triển hơn rất nhiều so với kỷ nguyên công nghệ tương tự.
- Mã hóa toán học 128 bit, mạnh hơn rất nhiều so với bất kỳ mật mã cổ đại hay thời trung cổ nào, hiện là tiêu chuẩn cho nhiều thiết bị cảm biến và hệ thống máy tính.
- Bắt đầu từ năm 1990, một dạng mã hóa hoàn toàn mới, với tên gọi mật mã lượng tử, đã và đang được phát triển bởi các nhà khoa học máy tính với hy vọng một lần nữa sẽ nâng cao mức độ bảo vệ của mã hóa hiện đại.

Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

❑ Mật mã học trong kỷ nguyên máy tính

- Gần đây các kỹ thuật mã hóa cũng đã được áp dụng cho tiền điện tử.Tiền điện tử tận dụng một số kỹ thuật mã hóa tiên tiến, bao gồm hàm băm, mật mã khóa công khai và chữ ký số.
- Những kỹ thuật này được sử dụng chủ yếu để đảm bảo tính bảo mật dữ liệu được lưu trữ trên các blockchain và để xác thực giao dịch.
- Một dạng mã hóa đặc biệt được gọi là thuật toán chữ ký điện tử dựa trên đường cong Elliptic (ECDSA), giúp cho Bitcoin và các hệ thống tiền điện tử khác tăng thêm tính bảo mật và đảm bảo rằng tiền chỉ có thể được sử dụng bởi chủ sở hữu hợp pháp.

Chương 1:
GIỚI THIỆU TỔNG QUAN

14. Lược sử mật mã học

Chương 1:
GIỚI THIỆU TỔNG QUAN

Kết luận và lược sử mật mã học

- Mật mã hóa đã đi một chặng đường dài trong 4000 năm qua và không có khả năng sẽ dừng lại sớm. Miễn là có dữ liệu nhạy cảm cần được bảo vệ, mật mã học sẽ tiếp tục phát triển.
- Mặc dù các hệ thống mã hóa được dùng trong các khối blockchain tiền điện tử ngày nay là một số dạng tiên tiến nhất của ngành khoa học mã hóa, chúng cũng là một phần trong chuỗi dài phát triển từ trước đến nay của lịch sử nhân loại.

Chương 1:
GIỚI THIỆU TỔNG QUAN

15. Một số ứng dụng của mã hóa

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

- Bảo mật dữ liệu
- Xác thực toàn vẹn thông tin
- Chữ ký số
- Quản lý khóa