TRUYỀN VÀ BẢO MẬT THÔNG TIN

Bài 1:

Lý thuyết mật mã

VŨ THỊ TRÀ

Nội dung

- Lược sử mật mã & truyền tin
- Sơ đồ Hệ thống mật mã
- Hệ mật mã đối xứng và bất đối xứng
- Một số bài toán an toàn thông tin
- Bảo mật và thám mã
- Tính an toàn của một hệ mật mã

Lược sử mật mã

- **Mật mã sơ khai** ra đời từ ~ > 4000 năm trước công nguyên trong nên văn minh Ai Cập
- Mật mã được sử dụng rộng rãi trên thế giới để giữ bí mật cho việc trao đổi thông tin trong nhiều lĩnh vực như: quân sự, chính trị, ngoại giao, v.v…
- **Nhu cầu:** Trao đổi thông tin, thư từ → Giữ bí mật & bảo vệ thông tin, thư từ → Che dấu nội dung văn bản: Biến dạng văn bản (*mật mã*) + Khôi phục lại nguyên dạng ban đầu của văn bản (*giải mật mã*)

→ Mật mã?

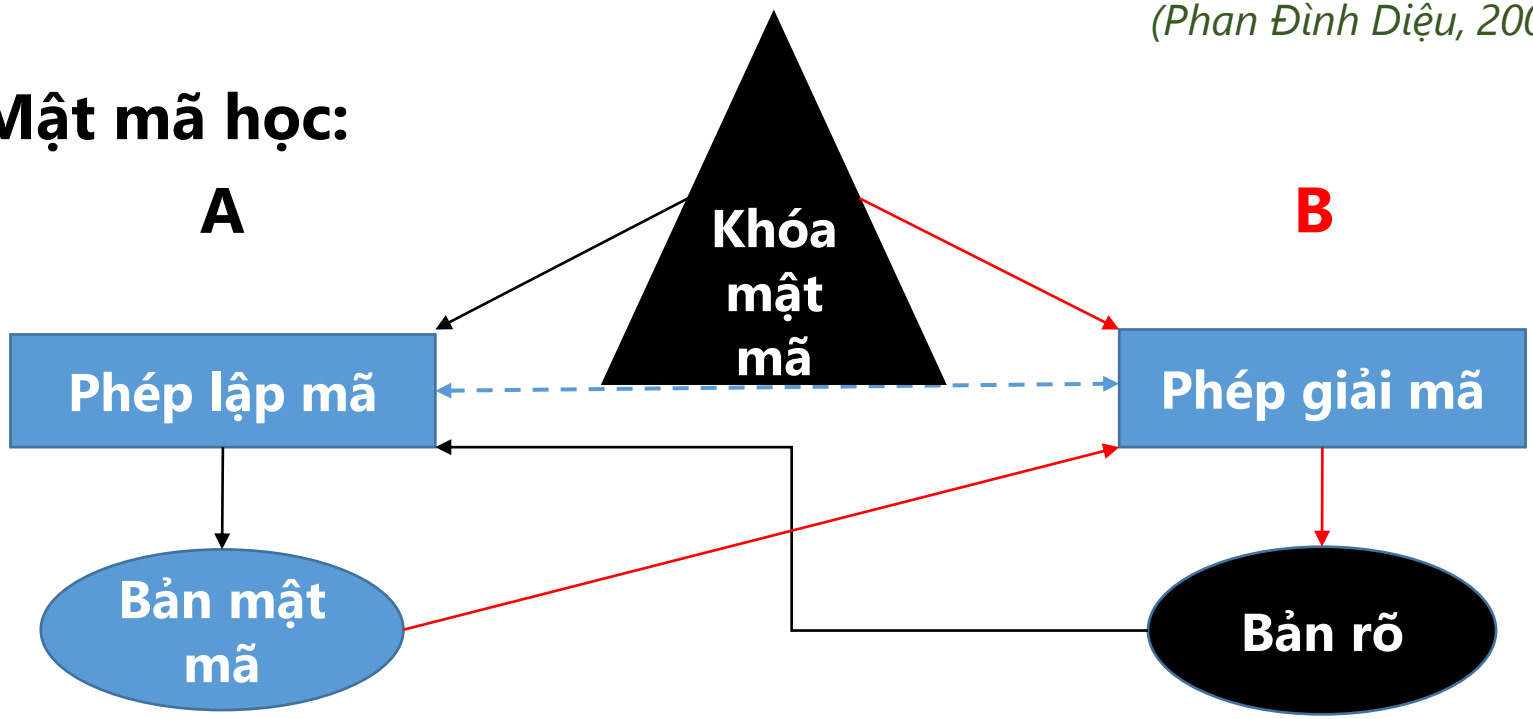
Lược sử mật mã

- **Định nghĩa:**

"Mật mã trước hết là một loại hình hoạt động thực tiễn, nội dung chính của nó là để giữ bí mật thông tin (chẳng hạn dưới dạng một văn bản) từ một người gửi A đến một người nhận B"

(Phan Đình Diệu, 2002)

- **Mật mã học:**



Lược sử mật mã

- **Y2K:** Sự phát triển của các kỹ thuật biểu diễn, truyền và xử lý tín hiệu
  - **Lập và giải mật mã**: thủ công → cơ giới hóa → điện tử hóa: kỹ thuật số - tín hiệu nhị phân, hàm số học → kỹ thuật tính toán - công cụ phát triển khoa học về mật mã
  - Bản mật mã tiêu chuẩn: *"Bí mật"* = *"Ngẫu nhiên"*+ *"Phức tạp"*
- **1948:** C.Shannon đưa ra khái niệm *"Bí mật hoàn toàn"* → **Lý thuyết xác suất về mật mã**
  - Bit ngẫu nhiên: qui luật sinh ra dãy bit ngẫu nhiên, *giả ngẫu nhiên*
  - *Dãy bit ngẫu nhiên* nếu xác suất xuất hiện bít 0 hay bít 1 trong toàn dãy đó cũng như các dãy con bất kỳ của nó đều = 1/2

Lược sử mật mã

- **1950s**: Mật mã truyền thống → **Mật mã máy tính**
- **1960s: Lý thuyết về độ phức tạp tính toán**
  - Bảo đảm bí mật: nếu mọi thuật toán thám mã nếu có đều phải được thực hiện với độ phức tạp tính toán cực lớn
  - Tiêu chuẩn bí mật: dựa theo độ phức tạp tính toán với tốc độ tăng vượt quá hàm mũ, hoặc thuộc lớp **NP-khó**

"Bản mật mã đối với anh là bí mật, nếu từ bản mật mã đó để tìm ra bản rõ anh phải thực hiện một tiến trình tính toán mà độ phức tạp của nó vượt qua mọi năng lực tính toán (kể cả mọi máy tính) của anh ta"

(Phan Đình Diệu, 2002)

Lược sử mật mã

- **1976:** Diffie & Hellman đưa ra khái niệm về *mật mã khóa công khai*
- **1978:** Rivest, Shamir & Adleman tìm ra **hệ mã khóa công khai** và một *sơ đồ chữ ký điện tử* mà tính bảo mật và an toàn của chúng được bảo đảm = độ phức tạp của một bài toán số học phân tích số nguyên thành tích các thừa số nguyên tố.

Lược sử mật mã

- **1970s:** phát minh các hệ mật mã có *khóa công khai*, *mà* cơ sở lý thuyết là sự tồn tại của *các hàm một phía* (one-way function)

  Các hệ mật mã có khóa công khai

  - đã làm thay đổi bản chất việc tổ chức các hệ truyền thông tin bảo mật, làm dễ dàng cho việc bảo mật trên các hệ truyền thông công cộng
  - là cơ sở cho việc phát triển nhiều giao thức an toàn thông tin:
    - ✓ Xác nhận nguồn tin và định danh người gửi, chứ ký điện tử
    - ✓ Trao đổi khóa trong tổ chức truyền tin bảo mật và trong xác nhận
    - ✓ Trong các giao dịch ngân hàng, thương mại điện tử, phát hành và mua bán bằng tiền điện tử, v.v...

Lược sử mật mã

*"Cơ sở quan trọng của **lý thuyết mật mã hiện đại** là sự tồn tại của các hàm một phía, nhưng ngay có thật tồn tại các hàm một phía hay không vẫn là một bài toán chưa có câu trả lời! Ta chỉ mới đang có một số hàm một phía theo sự hiểu biết của con người hiện nay, nhưng chưa chứng minh được có một hàm cụ thể nào đó chắc chắn là hàm một phía!"*

(Phan Đình Diệu, 2002)

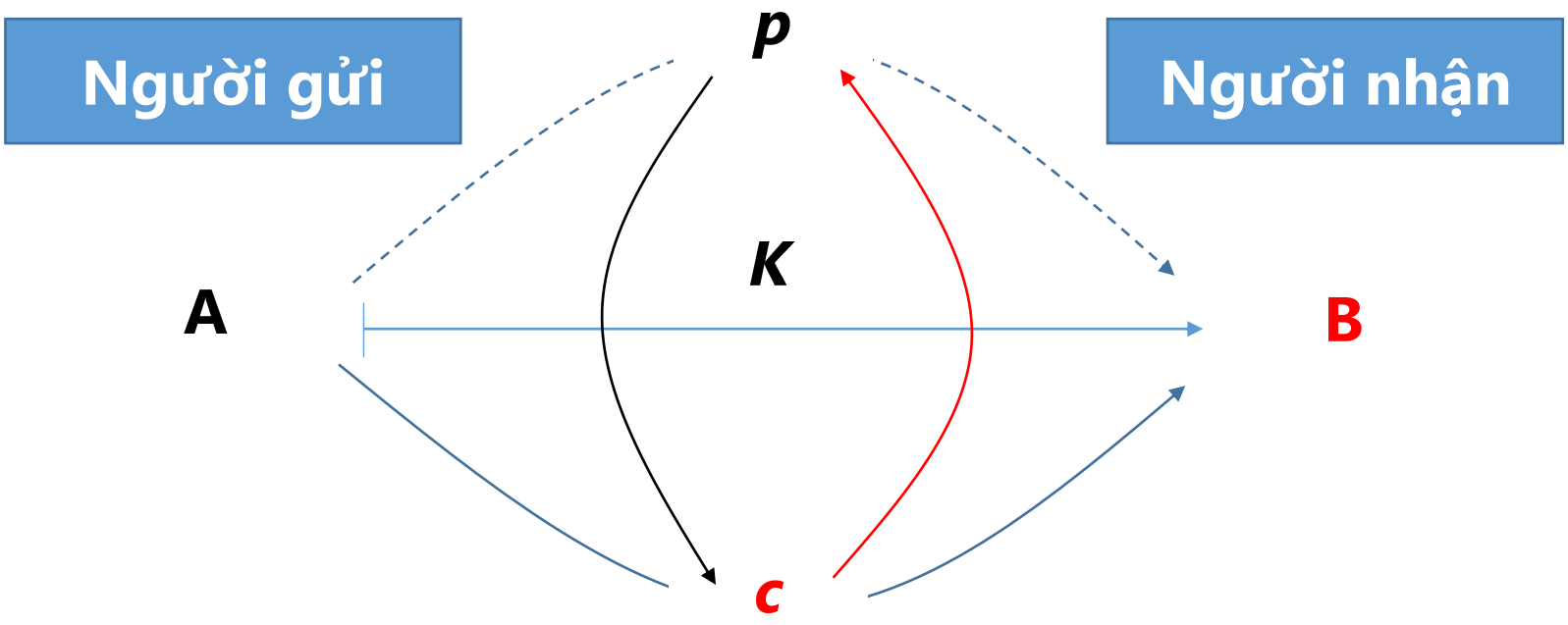
Lược sử mật mã

- **Suốt mấy nghìn năm lịch sử,** các thông báo, thư từ được truyền đưa và trao đổi với nhau chủ yếu là các văn bản (dạng các dãy ký tự trong một ngôn ngữ).
  - **Thuật toán lập mật mã** thường đơn giản là chuyển dịch, thay thế và hoán vị các ký tự
  - **Khóa mật mã**: số vị trí đối với phép chuyển dịch, bảng xác định các cặp ký tự t.ứ trong phép thay thế, hoán vị, v.v...
- Do bản thân hoạt động mật mã là bí mật, nên các tài liệu về mật mã đến nay được phổ biến vẫn ít, ...

V/v "Phát minh" Hệ mật mã

- **1600s:** Hệ mật mã Vinegere – phép chuyển dịch + thay thế
- **1929:** Hệ mật mã Hill – phép thay thế trên một nhóm ký tự
- Những câu chuyện kỳ thú của lịch sử mật mã được thuật lại bởi David Kahn trong
  - "*The Codebreakers . The Story of Secret Writing*" (1967)
  - "*Những người mã thám" , 3 tập* (1987)

Mật mã & Hệ truyền tin



Định nghĩa: Sơ đồ hệ thống mật mã

Một sơ đồ hệ thống mật mã là một bộ năm

$$S = (P, C, K, E, D) \qquad (1)$$

thỏa mãn các điều kiện sau:

P *là một tập hữu hạn các ký tự bản rõ,*

C *là một tập hữu hạn các ký tự bản mã,*

K *là một tập hữu hạn các khóa mật mã,*

E *là một ánh xạ từ* $K \times P$ *vào* C*, được gọi là phép lập mật mã,*

D *là một ánh xạ từ* $K \times C$ *vào* P*, được gọi là phép giải mã.*

Với mỗi $K \in K$*, ta định nghĩa* $e_K: P \rightarrow C$, $d_K: C \rightarrow P$ *là 2 hàm cho bởi:*

$$\forall x \in P : e_K(x) = E(K,x) ; \quad \forall y \in C : d_K(y) = D(K,y)$$

e_K *và* d_K *được gọi là các hàm lập mã và giải mã tương ứng với khóa mật mã* K*. Các hàm này sẽ phải thỏa mãn hệ thức:*

$$\forall x \in P : d_K(e_K(x)) = x$$

(Phan Đình Diệu, 2002)

Định nghĩa: Sơ đồ hệ thống mật mã

- **Qui ước:**
  - Danh sách (1) thỏa mãn các điều kiện trên đây là một *sơ đồ hệ thống mật mã*
  - Khi đã chọn cố định một khóa K, thì danh sách ($\mathcal{P}$, $\mathcal{C}$, e_K, d_K) là một *hệ mật mã* thuộc sơ đồ đó.

Mở rộng thuật toán: Hệ mã theo khối

- Xác định **độ dài khối** (chẳng hạn k), **mở rộng** không gian khóa từ $\mathbf{K}$ thành $\mathbf{K}^k$. Với mỗi $K=K_1,\ldots,K_k \in \mathbf{K}^k$, ta mở rộng e_k và d_k thành các thuật toán $e_k: \mathbf{P}^k \rightarrow \mathbf{C}^k$ và $d_k: \mathbf{C}^k \rightarrow \mathbf{P}^k$ như sau:

  với mọi $x=x_1,\ldots,x_k \in \mathbf{P}^k$ và $y=y_1,\ldots,y_k \in \mathbf{C}^k$ *ta có*

  $$e_K(x_1\ldots x_k)=e_{K_1}(x_1)\ldots e_{K_k}(x_k)\ ;\ d_K(y_1\ldots y_k)=d_{K_1}(y_1)\ldots d_{K_k}(y_k)$$

- Giả sử **bản rõ** là dãy ký tự $X \in \mathbf{P}^*$, cắt X thành từng khối có độ dài k, khối cuối cùng có thể có độ dài $< k$, ta luôn có thể bổ sung vào phần cuối của khối này một số ký tự để nó cũng có độ dài k. Từ đó, ta có giả thuyết $X=X_1\ldots X_m$, trong đó mỗi X_i có độ dài k. Khi đó, bản mật mã X là:

  $$e_K(X) = e_K(X_1\ldots X_m) = e_K(X_1)\ldots e_K(X_m)$$

  Đặt $Y = e_K(X_1)\ldots e_K(X_m) = Y_1\ldots Y_m$ *với* $Y_i = e_K(X_i)$, ta có:

  $$d_K(Y) = d_K(Y_1)\ldots d_K(Y_m) = X_1\ldots X_m = X$$

Hệ mật mã đối xứng & bất đối xứng

- **Hệ mật mã đối xứng:** hệ mật mã có sử dụng một khóa mật mã chung cho cả lập mã và giải mã. Hàm lập mã và giải mã thỏa hệ thức :

$$d_K(e_K(x)) = x \quad \text{với mọi } x \in P^k$$

- **Hệ mật mã bất đối xứng:** hệ mật mã có sử dụng một cặp khóa mật mã $K=(K', K'')$, trong đó K' dành cho việc lập mã và K'' dành cho việc giải mã. Hàm lập mã và giải mã thỏa hệ thức :

$$d_{K''}(e_{K'}(x)) = x \quad \text{với mọi } x \in P^k$$

Trong đó, khóa cần được giữ bí mật là khóa giải mật mã K'', khóa lập mật mã K' có thể công bố công khai khi việc biết K' tìm K'' cực kỳ khó khăn đến mức hầu như ko thể giải được. Hệ có tính chất này được gọi là **hệ mật mã khóa công khai**.

Một số bài toán về an toàn thông tin

- ***Bảo mật***
- ***Toàn vẹn thông tin***
- ***Nhận thực một thực thể***
- ***Nhận thực một thông báo***
- ***Chữ ký***
- ***Ủy quyền***
- ***Cấp chứng chỉ***
- ***Báo nhận***
- ***Làm chứng***
- ***Không chối bỏ được***
- ***Ẩn danh***
- ***Thu hồi***
- ***v.v...***

(Phan Đình Diệu, 2002)

Bảo mật & Mã thám

- **Bảo mật:** là hoạt động che dấu thông tin – nội dung bản rõ dưới một bản mật mã
- **Mã thám:** khám phá bí mật từ các bản mật mã "*lấy trộm*" được
- Khi phép lập mã và giải mã không nhất thiết là bí mật thì việc **thám mã** qui về bài toán tìm khóa mật mã *K* hay khóa giải mã *K'*.
- Mã thám thường tập trung vào việc tìm khóa mật mã (*phá khóa*)

Phân loại bài toán thám mã

- **Chỉ biết bản mã** : chỉ biết 1 bản mã *Y*
- **Khi biết cả bản rõ** : biết 1 bản mã *Y* cùng với 1 bản rõ t.ứ. *X*
- **Khi có bản rõ được chọn** : có thể chọn 1 bản rõ *X*, và biết bản mã t.ứ *Y*
- **Khi có bản mã được chọn** : có thể chọn 1 bản mã *Y*, và biết bản rõ t.ứ *X*

Cấp độ an toàn của hệ mật mã

- **An toàn vô điều kiện**: nếu những hiểu biết về bản mã không thu hẹp được độ bất định về bản rõ. Hệ là bí mật hoàn toàn
- **An toàn được chứng minh**: nếu ta có thể chứng minh được bài toán thám mã khó tương đương với một bài toán khó đã biết (VD: bài toán phân tích một số nguyên thành tích các thừa số nguyên tố, bài toán tìm logarit rời rạc theo một mô đun nguyên tố,...)
- **An toàn tính toán**: nếu mọi pp thám mã đã biết đều đòi hỏi một nguồn năng lượng tính toán vượt mọi khả năng tính toán

Q & A

1. Liệt kê các đặc trưng của một hệ mật mã?
2. Thế nào là một hệ mật mã tiêu chuẩn?