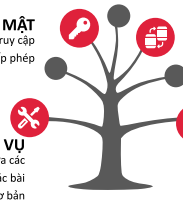
HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

NHẬP MÔN MẬT MÃ HỌC

GIỚI THIỆU HỌC PHẦN



ĐẢM BẢO TÍNH BÍ MẬT
Thông tin chỉ được phép truy cập bởi đối tượng được cấp phép

ĐẢM BẢO TÍNH TOÀN VẸN
Dữ liệu, thông tin không bị thay đổi, mất mát khi truyền tin

TÍCH HỢP CÁC DỊCH VỤ
Khả năng vận dụng kết hợp giữa các thuật toán mật mã để giải quyết các bài toán đảm bảo an toàn thông tin cơ bản

XÁC THỰC
Đảm bảo thông tin đến từ một nguồn đáng tin cậy

GIỚI THIỆU HỌC PHẦN

THỜI LƯỢNG: 3tc

- 54 tiết lý thuyết (3 tiết/1 buổi x 18 buổi)
- 18 tiết bài tập

ĐÁNH GIÁ KẾT QUẢ HỌC TẬP

- Điểm chuyên cần
  - Đi học đầy đủ, đúng giờ
  - Tham gia xây dựng bài
- Kiểm tra giữa kỳ: thi viết/BTL
- Thi kết thúc học phần: thi viết

GIỚI THIỆU HỌC PHẦN

Cơ sở lý thuyết mật mã, Học viện KTMM
Nguyễn Bình, Hoàng Thu Phương, 2013

Mật mã ứng dụng trong an toàn thông tin
Nguyễn Ngọc Cương, Trần Thị Lượng, 2013

Và các tài liệu khác

- Douglas Stinson, *Cryptography: Theory and Practice 3th*, CRC Press/Star Educational Books Distributors, 2015
- A.Menezes, P.Van Oorschot and S. Vanstone: *Handbook of applied cryptography*. CRC Press, 1996
- ...

HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

NỘI DUNG

HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

CHƯƠNG 01

TỔNG QUAN VỀ MẬT MÃ HỌC

BÀI 01 - MỤC TIÊU

- An toàn thông tin là gì?
- Các tính chất (dịch vụ) cơ bản của an toàn thông tin?

- Mật mã có thể được ứng dụng để giải quyết những vấn đề cơ bản nào?
- Có những loại thuật toán mật mã cơ bản nào?
- Mối quan hệ giữa các dịch vụ an toàn thông tin cơ bản và các loại thuật toán mật mã cơ bản như thế nào?

- Định nghĩa hình thức toán học của một Hệ mật là gì?
- Hệ mật đối xứng/bất đối xứng? Hệ mật mã khối/mã dòng?

- Có những ứng dụng cụ thể điển hình nào của mật mã trong thực tế?

TỔNG QUAN VỀ MẬT MÃ HỌC

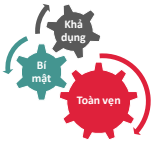
- Một số vấn đề cơ bản trong bảo vệ thông tin
- Sơ đồ hệ thống truyền tin số
- Một số ứng dụng của mật mã trong thực tế
- Các hệ thống mật mã

KN An toàn thông tin

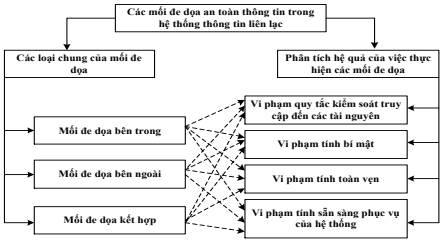
- **An toàn thông tin là gì?**
  - An toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bí mật và tính khả dụng của thông tin

Một số vấn đề cơ bản trong ATTT

- Tránh bị truy nhập
- Tránh bị sử dụng
- Tránh bị tiết lộ
- Tránh bị gián đoạn
- Tránh bị sửa đổi
- Tránh bị phá hoại trái phép



Một số vấn đề trong bảo vệ thông tin



Một số vấn đề trong bảo vệ thông tin

BÍ MẬT THÔNG TIN (CONFIDENTIALITY)
Đảm bảo chỉ những đối tượng đã được cấp quyền mới biết được nội dung thông tin

TOÀN VẸN THÔNG TIN (INTEGRITY)
Bảo đảm thông tin không bị sửa đổi, xuyên tạc bởi những người không có thẩm quyền hoặc đối tượng trái phép (hoặc giúp phát hiện rằng thông tin đã bị sửa đổi)

CHỐNG CHỐI BỎ (NON-REPUDIATION)
Đảm bảo một đối tác bất kỳ trong hệ thống không thể từ chối trách nhiệm về hành động mà mình đã thực hiện

TÍNH SẴN SÀNG (AVAILABLILITY)
Bảo đảm độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn.

XÁC THỰC (AUTHENTICATION)
Xác thực các đối tác trong liên lạc, xác thực nguồn gốc của một thông báo

Thuật toán mật mã cơ bản

Có những loại thuật toán mật mã cơ bản nào?

- Mã hóa khóa bí mật, mã hóa khóa công khai
- Hàm băm, mã xác thực thông điệp (MAC)
- Chữ kí số

Quan hệ giữa Dịch vụ ATTT & Thuật toán

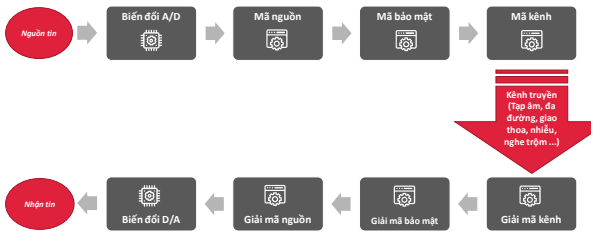
Mối quan hệ giữa các dịch vụ an toàn thông tin và các kỹ thuật (thuật toán) mật mã cơ bản?

	Dịch vụ	Kỹ thuật
	Đảm bảo tính bí mật	Mã hóa
	Đảm bảo tính toàn vẹn	Chữ ký số, hàm băm, MAC
	Xác thực	Chữ ký số, MAC
	Chống chối bỏ	Chữ ký số

TỔNG QUAN VỀ MẬT MÃ HỌC

- Một số vấn đề cơ bản trong bảo vệ thông tin
- Sơ đồ hệ thống truyền tin số
- Một số ứng dụng của mật mã trong thực tế
- Các hệ thống mật mã

Sơ đồ hệ thống truyền tin số



TỔNG QUAN VỀ MẬT MÃ HỌC

- Một số vấn đề cơ bản trong bảo vệ thông tin
- Sơ đồ hệ thống truyền tin số
- Một số ứng dụng của mật mã trong thực tế
- Các hệ thống mật mã

Một số ứng dụng của mật mã trong thực tế

Ứng dụng trong thực tiễn
- Ứng dụng trong đời sống thông tin, KT-XH
- Ứng dụng trong an ninh, quốc phòng

Ứng dụng của một số thành phần mật mã

Ứng dụng trong các giao thức bảo mật
- Mã hóa mật khẩu và xác thực đăng nhập trên Linux
- SSH, SSL, SET, ...

TỔNG QUAN VỀ MẬT MÃ HỌC

- Một số vấn đề cơ bản trong bảo vệ thông tin
- Sơ đồ hệ thống truyền tin số
- Một số ứng dụng của mật mã trong thực tế
- Các hệ thống mật mã

Định nghĩa hình thức của hệ mật

Một số khái nhiệm/ký hiệu liên quan

- $\mathcal{P}$ là tập hữu hạn các bản rõ có thể
- $\mathcal{C}$ là tập hữu hạn các bản mã có thể
- $\mathcal{K}$ là tập hữu hạn các khoá có thể
- $\mathcal{E}_k: \mathcal{P} \to \mathcal{C}$ là quy tắc mã hóa với khóa $k \in \mathcal{K}$. Tập $\{\mathcal{E}_k: k \in \mathcal{K}\}$ ký hiệu là $\mathcal{E}$, còn tập $\{E_k(x): x \in \mathcal{P}\}$ ký hiệu là $E_k(\mathcal{P})$.
- $\mathcal{D}_k: \mathcal{C} \to \mathcal{P}$ - là quy tắc giải mã với khóa $k \in \mathcal{K}$. Tập $\{\mathcal{D}_k: k \in \mathcal{K}\}$ ký hiệu là $\mathcal{D}$.
- Với mỗi $k \in \mathcal{K}$ sẽ được mô tả dưới dạng $k = (k_e, k_d)$, trong đó: k_e - là khóa dùng cho mã hóa, k_d - là khóa dùng cho giải mã. Khi đó $\mathcal{E}_k$ được hiểu là hàm $\mathcal{E}_{k_e}$, $\mathcal{D}_k$ được hiểu là hàm $\mathcal{D}_{k_d}$

Định nghĩa hình thức của hệ mật

Một số khái nhiệm/ký hiệu liên quan

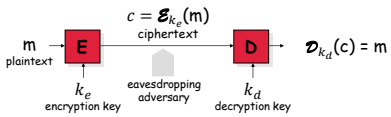
- **Định nghĩa hệ mật:** Một hệ mật là bộ 5 $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ thoả mãn các điều kiện sau:
  1) $\forall x \in \mathcal{P}, k \in \mathcal{K}$ ta có:
  $$\mathcal{D}_k(\mathcal{E}_k(x)) = x;$$
  2)
  $$\mathcal{C} = \bigcup_{k \in \mathcal{K}} \mathcal{E}_k(\mathcal{P})$$
- **Ghi chú:**
  - Mã hóa: $y = \mathcal{E}_{k_e}(x)$
  - Giải mã: $x = \mathcal{D}_{k_d}(y)$

Các hệ thống mật mã

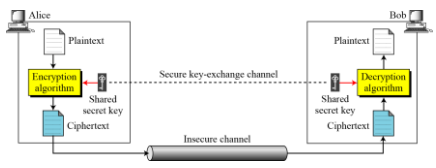
Quá trình chung của hệ mật

Mã hóa đối xứng/bất đối xứng

Mã hóa đối xứng: biết được khóa mã hóa dễ dàng suy ra được khóa giải mã (thông thường $k_e = k_d$)

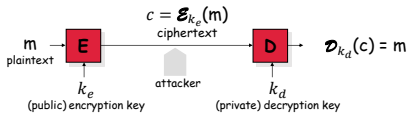


Mã hóa đối xứng/bất đối xứng



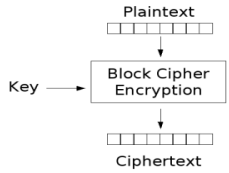
Mã hóa đối xứng/bất đối xứng

Mã hóa bất đối xứng: Mỗi bên có một khoá công khai và một khoá bí mật.
- Bên gửi dùng khoá công khai của bên nhận để mã hoá.
- Bên nhận dùng khoá bí mật của mình để giải mã.



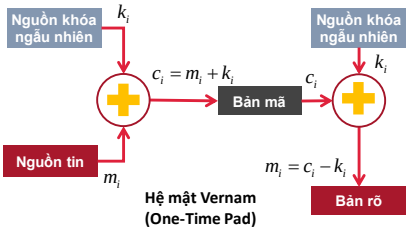
Các hệ thống mật mã

- Mã khối:



Các hệ thống mật mã

Mã dòng:



Ví dụ: Hệ mật Vernam

MÃ HÓA

Bộ kí tự:	chữ cái latin
Khóa ngẫu nhiên:	**PWKAX**
Thông điệp:	**HELLO**

Rõ	H (7)	E (4)	L (11)	L (11)	O (14)
Khóa	P (15)	W (22)	K (10)	A (0)	X (23)
Mã	W (22)	A (0)	V (21)	? (?)	? (?)

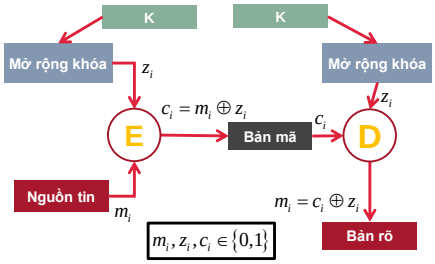
Ví dụ: Hệ mật Vernam

GIẢI MÃ

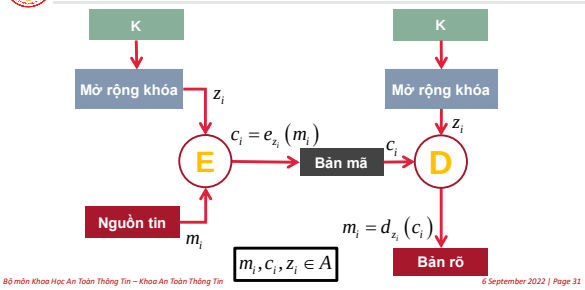
Bộ kí tự:	chữ cái latin
Khóa ngẫu nhiên:	**PWKAX**
Bản mã:	**WAVLL**

Mã	W (22)	A (0)	V (21)	L (11)	L (11)
Khóa	P (15)	W (22)	K (10)	A (0)	X (23)
Rõ	H (7)	E (4)	L (11)	L (11)	O (14)

Mã dòng – Thường gặp



Mã dòng – Trường hợp tổng quát



Mã dòng – Trường hợp tổng quát

- Khối «mở rộng khóa»
  - Là bộ sinh số giả ngẫu nhiên (PRNG)
  - Là quan trọng nhất
  - Quyết định độ an toàn của mã dòng
- Phân loại
  - z_i chỉ phụ thuộc K: «mã dòng đồng bộ»
  - z_i phụ thuộc c_{i-n}, c_{i-n+1}, ..., c_{i-1}: «mã dòng tự đồng bộ»