AN TOÀN THÔNG TIN

Giảng viên: Th.s Phạm Minh Thái

Email: pmthai@uneti.edu.vn

Tổ Mạng Máy Tính và Công Nghệ Đa Phương Tiện

Khoa Công nghệ Thông tin

CHƯƠNG 2: MÃ HÓA ĐỐI XỨNG CỔ ĐIỂN

2.1. Mô hình mã hóa đối xứng.

2.2. Các hệ mã hóa thay thế cổ điển.

2.3. Các kỹ thuật mã hóa hoán vị cổ điển.

2.4. Mã hóa kết hợp.

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: mã hóa và giải mã. Sản phẩm là các hệ mã mật, hàm băm, chữ ký điện tử, 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 là các phương pháp phá mã, giả mạo chữ ký, tấn công.

Phương thức mã hóa cơ bản

- Phương thức mã hóa thay thế: 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: các từ mã của bản rõ được sắp xếp lại theo một phương thức nhất định.

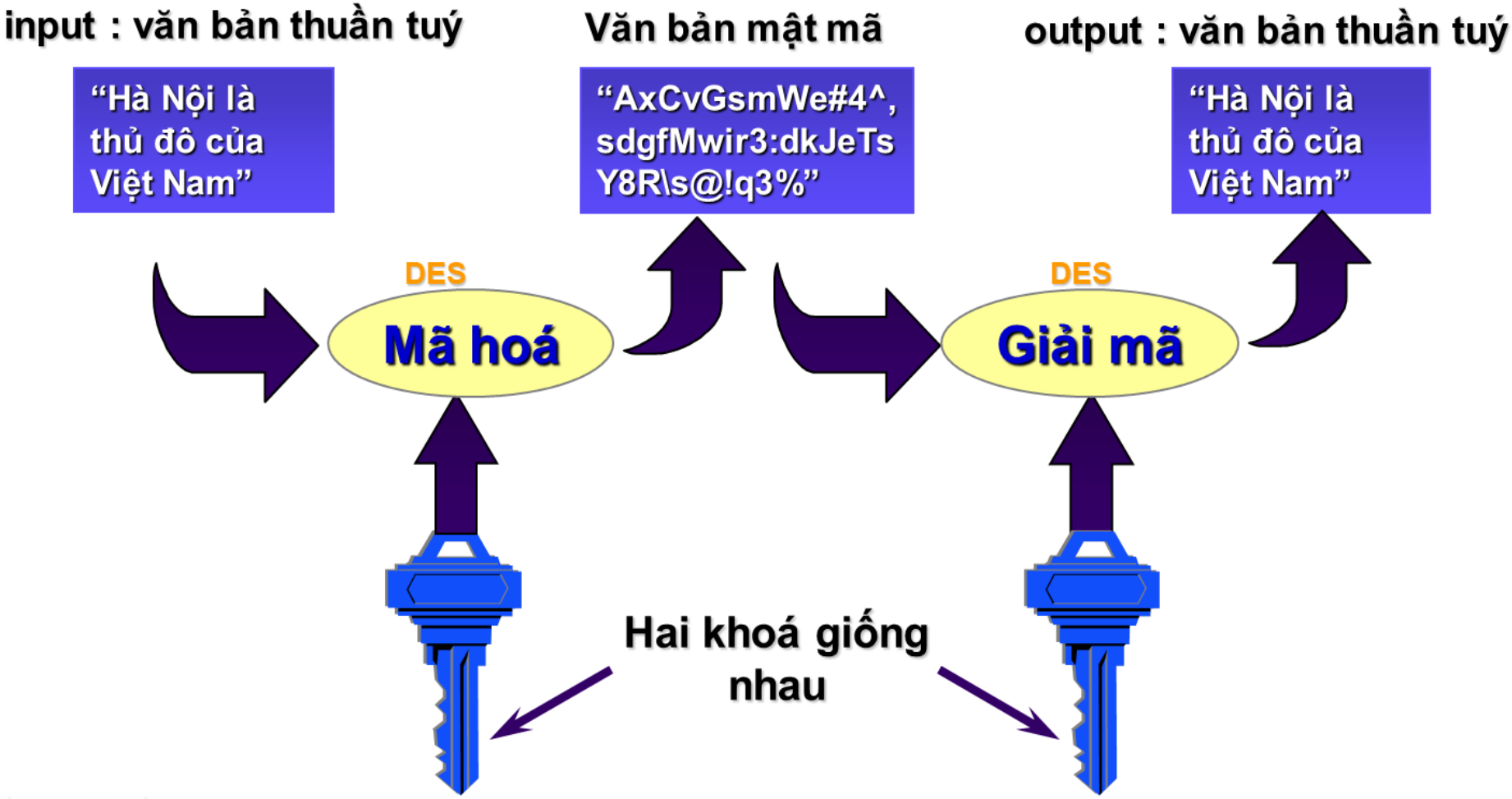
Vai trò của hệ mật mã

- 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.

Khái niệm cơ bản trong hệ mật mã

- Bản rõ X: 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 (xét phương pháp mã hóa không làm thay đổi kích thước của bản rõ => chúng có cùng độ dài).
- Mã: là thuật toán E - chuyển bản rõ thành bản mã. (Cần thuật toán mã hóa mạnh, dù biết thuật toán, nhưng không biết khóa => không tìm được bản rõ).
- Khoá K: là thông tin tham số dùng để mã hoá, chỉ có người gửi và người nhận biết. Khóa độc lập với bản rõ, độ dài phù hợp yêu cầu bảo mật.

2.1 Mô hình mã hóa đối xứng



Mã đối xứng

- Mã đối xứng là mã một khoá - khoá riêng - khoá thỏa thuận.
- Người gửi và người nhận chia sẻ khoá chung.
- Mọi thuật toán mã cổ điển đều là khoá riêng.
- Là kiểu duy nhất trước khi phát minh ra khoá mã công khai vào những năm 1970.
- Và đến nay vẫn được sử dụng rộng.

2.2. Các hệ mã hóa thay thế cổ điển.

- Hệ mã hóa Caesar
- Hệ mã hóa đơn bảng
- Hệ mã hóa Playfair
- Hệ mã hóa Vigenere
- Hệ mã hóa khóa tự động
- Hệ mã hóa độn một lần

Hệ mã hóa Caesar

- Mã thế được biết sớm nhất.
- Được sáng tạo bởi Julius Ceasar.
- Đầu tiên được sử dụng trong quân sự.
- Thay mỗi chữ bằng chữ thứ ba tiếp theo.
- Ví dụ:

meet me after the toga party

=> PHHW PH DIWHU WKH WRJD SDUWB

(thay m = chữ thứ 3 sau m = “n, o, p”; e =“f, g, h”;…)

Caesar Cipher

- Có thể định nghĩa qua phép dịch chuyển

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Về toán học, nếu gán số cho mỗi chữ

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Mã Caesar được định nghĩa như sau:

  $c = E(p) = (p + k) \bmod (26)$

  $p = D(c) = (c - k) \bmod (26)$

- p là số thứ tự của chữ trong bản rõ, c là số thứ tự của chữ tương ứng trong bản mã; k là khoá (*có 26 giá trị khác nhau của k, nên có 26 khoá khác nhau*).

Hệ mã hóa đơn bảng

- Không chỉ là dịch chuyển bảng chữ.
- Có thể tạo các bước nhảy các chữ tùy ý.
- Mỗi chữ của bản rõ được ánh xạ đến một chữ ngẫu nhiên khác nhau của bản mã.
- Như vậy độ dài khoá là 26.
- Ví dụ:

  Plain: abcdefghijklmnopqrstuvwxyz

  Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

  Plaintext: ifwewishtoreplaceletters

  Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

Hệ mã hóa Playfair

- Mỗi chữ có thể được mã bằng một trong 7 chữ khác nhau tùy vào chữ cặp đôi cùng nó trong bản rõ.
- Là ma trận gồm các chữ 5 x 5 dựa trên một từ khoá.
- Viết các chữ của từ khoá vào ma trận.
- Nếu còn trống, viết các chữ khác vào các ô còn lại.
- Ví dụ: sử dụng từ MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Mã hóa và giải mã

- Bản rõ được mã hoá 2 chữ cùng một lúc.
- Nếu một cặp nào đó là chữ lặp => chèn thêm một từ lọc X.
- Nếu hai chữ ở cùng hàng => mã hóa mỗi chữ bằng chữ ở phía bên phải nó.
- Nếu hai chữ ở cùng cột => mã mỗi chữ bằng chữ ở phía bên dưới nó.
- Trong các trường hợp khác: mỗi chữ được mã bởi chữ cùng hàng với nó và cùng cột với chữ cùng cặp với nó.

Ví dụ: Cho chuỗi Plaintext P: "THUONG MAI DIEN TU". Sử dụng hệ mã hóa Playfair, keyword "MINH".

➢Bước 1: **loại bỏ J**, thêm keyword "MINH", thêm lần lượt các chữ cái khác vào ma trận => được ma trận X

M	I	N	H	A
B	C	D	E	F
G	K	L	O	P
Q	R	S	T	U
V	W	X	Y	Z

➢ Bước 2: Tách chuỗi P theo cặp, thêm X vào các cặp trùng (tiếp tục tách - nếu có)

=> được: **TH UO NG MA ID IE NT UX**

➢ Bước 3: Áp dụng nguyên tắc

- TH1: nếu 2 chữ nằm cùng hàng, thay bởi các chữ bên phải
- TH2: nếu 2 chữ nằm cùng cột, thay bởi các chữ bên dưới
- TH3: trường hợp khác, mỗi chữ cái thay bởi chữ cái khác cùng hàng, trên cột chữ cái cùng cặp.

=> được: ***TH => YE (TH2) UO => TP (TH3) NG => ML (TH3) MA => IM (TH1) ID => NC (TH3) IE => HC (TH3) NT => HS (TH3) UX => SZ (TH2)***

Cipher Text: **YETPMLIMNCHCHSSZ**

Hệ mã hóa Vigenere

- Mã thế đa bảng đơn giản nhất là mã Vigenere.
- Thực chất quá trình mã hoá Vigenere là việc tiến hành đồng thời dùng nhiều mã Ceasar cùng một lúc trên bản rõ với nhiều khoá khác nhau.
- „Giả sử khoá là một chữ có độ dài d được viết dạng K = K1K2…Kd, trong đó Ki nhận giá trị nguyên từ 0 đến 25
- Tần suất các chữ trong bản mã dãn tương đối đều.

Ví dụ: Cho chuỗi Plaintext: "meetmeatsunset".
Sử dụng hệ mã hóa Vigenere, keyword "CIPHER".

- Giả sử d = 6, từ khóa là CIPHER, từ khóa này tương ứng với dãy số: k =(2, 8, 15, 7, 4, 17)
- Bản rõ: **meetmeatsunset**. Chuyển các ký tự rõ thành mã trên Z_{26} rồi cộng với từ khóa.

Bản rõ	12	4	4	19	12	4	0	19	18	20	13	18	4	19
Khóa	2	8	15	7	4	17	2	8	15	7	4	17	2	8
Bản mã	14	12	19	0	16	21	2	1	7	1	17	9	6	1

- Bản mã tương ứng: **OMTAQVCBHBRJGB**

Hệ mã hóa khóa tự động

- Lý tưởng có khoá dài như bản tin => đề xuất khoá tự động sinh cho bằng độ dài bản tin.
- Từ khoá được nối tiếp bằng chính bản rõ để tạo thành khoá => dùng mã vigenere để mã hóa bản rõ.
- Biết từ khoá có thể khôi phục được một số chữ ban đầu => tiếp tục sử dụng chúng để giải mã cho văn bản còn lại.

Hệ mã hóa khóa tự động (t)

- Ví dụ: cho từ khoá deceptive

  key: deceptivewearediscoveredsav

  plaintext: wearediscoveredsaveyourself

  ciphertext:

  ZICVTWQNGKZEIIGASXSTSLVVWLA

Hệ mã hóa độn một lần/bộ đệm một lần

- Là hệ mã hóa thay thế không thể phá được.
- Khóa ngẫu nhiên, độ dài bằng độ dài văn bản, chỉ sử dụng một lần.
- Giữa nguyên bản và bản mã không có bất kỳ quan hệ nào về thống kê.
- Với bất kỳ nguyên bản và bản mã nào cũng tồn tại một khóa tương ứng.
- Khó khăn ở việc tạo khóa và đảm bảo phân phối khóa an toàn.