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.

2.3 Các kỹ thuật mã hóa hoán vị cổ điển

2.3.1. Hệ mã hóa hàng rào

2.3.2. Hệ mã hóa hàng

Hệ mã hóa hàng rào

- Dịch chuyển vị trí tương đối giữa các chữ trong bản rõ.
- Dấu bản rõ bằng cách thay đổi thứ tự các chữ.
- Không thay đổi các chữ thực tế được dùng.
- Có thể nhận biết được vì có cùng phân bố tần suất như bản gốc.

Mã Rail Fence

- Viết các chữ của bản tin theo đường chéo trên một số dòng.
- Sau đó đọc theo dòng => nhận được bản mã.
- Số dòng chính là khoá của mã. Vì khi biết số dòng, tính được số chữ trên mỗi dòng. Viết bản mã theo các dòng, lấy bản rõ bằng cách viết lại theo các cột.
- Ví dụ: viết bản tin "meet me after the toga party"

m		e		m		a		t		r		h		t		g		p		r		y
	e		t		e		f		e		t		e		o		a		a		T	

=> cho bản mã: MEMATRHTGPRYETEFETEOAAT

Hệ mã hóa hàng

- Viết các chữ của bản tin theo các dòng trên số cột xác định.
- Thay đổi thứ tự các cột theo một dãy số khoá cho trước, đọc lại chúng theo cột => bản mã.
- Ví dụ:

Key:	4	3	1	2	5	6	7
Plaintext:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

2.4 Mã hóa kết hợp

- Mã dùng hoán vị hoặc dịch chuyển không an toàn vì các đặc trưng của ngôn ngữ.
- Sử dụng một số mã liên tiếp => mã khó hơn.
- Tích hai hoán vị sẽ tạo nên hoán vị phức tạp hơn.
- Tích hai phép dịch chuyển tạo nên dịch chuyển phức tạp hơn.
- Phép thế được nối tiếp bằng phép dịch chuyển tạo nên mã mới khó hơn rất nhiều.

2.4 Mã hóa kết hợp

- Mã cổ điển chỉ sử dụng một trong hai phương pháp thay thế hoặc hoán vị.
- Mã dùng hoán vị hoặc dịch chuyển không an toàn vì các đặc trưng tần xuất của ngôn ngữ không thay đổi
- Để làm cho mã khó thám mã hơn => áp dụng một số mã liên tiếp nhau.
- Mã hoá cổ điển dễ bị giải mã: đoán chữ dựa trên thống kê tần xuất xuất hiện các chữ cái trên mã, so sánh với bảng thống kê quan sát của bản rõ.
- Dùng mã hoá cổ điển: mã hoá và giải mã phải thống nhất về cơ chế

Máy quay

- Trước khi có mã hiện đại, máy quay là mã tích thông dụng nhất.
- Được sử dụng rộng rãi trong chiến tranh thế giới thứ hai
- Tạo nên mã thế rất đa dạng và phức tạp.
- Sử dụng một số lõi hình trụ, mỗi lõi ứng với một phép thế, khi quay sẽ thay đổi sau khi mỗi chữ được mã.
- 26 x 26 x 26 = 17576 bảng chữ

Hagelin Rotor Machine

Dấu tin - Steganography

- **Là lựa chọn dùng kết hợp hoặc đồng thời với mã**
- **Dấu sự tồn tại của bản tin**
  - Trong bản tin dài chỉ dùng một tập con các chữ/từ được đánh dấu bằng cách nào đó.
  - Sử dụng mực không nhìn thấy.
  - Dấu trong các file âm thanh hoặc hình ảnh.
- **Có nhược điểm: chỉ dấu được lượng thông tin nhỏ các bít.**

Kết luận - Summary

- **Đã xét:**
  - Các thuật ngữ và kỹ thuật mã cổ điển.
  - Các mã thế đơn bảng chữ.
  - Thám mã sử dụng tần suất của các chữ.
  - Mã Playfair.
  - Mã thế đa bảng chữ.
  - Mã hoán vị (đổi chỗ).
  - Tích các mã và máy quay.
  - Dấu tin.