Chủ đề 2:

Hệ thống Mã hóa đối xứng

Mở đầu

- Hệ thống mã hóa đối xứng (symmetric cryptosystem)
  - Hệ thống mã hóa quy ước (conventional cryptosystem)
  - Hệ thống mã hóa trong đó quy trình mã hóa và giải mã đều sử dụng chung một khoá - *khóa bí mật (secret key)*.
  - Việc bảo mật thông tin phụ thuộc vào việc bảo mật khóa.

Hệ thống mã hóa đối xứng

Các phương pháp truyền thống

- Các phương pháp truyền thống sử dụng:
  - Phép thay thế (substitution): thay thế 1 từ/ký tự bằng 1 từ/ký tự khác
  - Phép thay đổi vị trí (transposition): các ký tự được thay đổi vị trí
- Việc thay thế/thay đổi vị trí có thể được thực hiện:
  - Đơn ký tự (mono-alphabetic)
  - Đa ký tự (poly-alphabetic)

Phương pháp mã hóa dịch chuyển

Shift Cipher:

- Một trong những phương pháp lâu đời nhất được sử dụng để mã hóa
- Thông điệp được mã hóa bằng cách dịch chuyển xoay vòng từng ký tự đi *k* vị trí trong bảng chữ cái
- Trường hợp với *k*=3 gọi là phương pháp *mã hóa Caesar*.

Phương pháp mã hóa dịch chuyển

Cho $P = C = K = \mathbf{Z}_n$

Với mỗi khóa $k \in K$, định nghĩa:

$e_k(x) = (x + k) \bmod n$ và $d_k(y) = (y - k) \bmod n$ với $x, y \in \mathbf{Z}_n$

$E = \{e_k, k \in K\}$ và $D = \{d_k, k \in K\}$

- Phương pháp đơn giản,
- Thao tác xử lý mã hóa và giải mã được thực hiện nhanh chóng
- Không gian khóa $K = \{0, 1, 2, \ldots, n\text{-}1\} = Z_n$
- Dễ bị phá vỡ bằng cách thử mọi khả năng khóa k

Phương pháp mã hóa dịch chuyển

- Ví dụ:
  - Mã hóa một thông điệp được biểu diễn bằng các chữ cái từ A đến Z (26 chữ cái), ta sử dụng Z_{26}.
  - Thông điệp được mã hóa sẽ không an toàn và có thể dễ dàng bị giải mã bằng cách thử lần lượt 26 giá trị khóa k.
  - Tính trung bình, thông điệp đã được mã hóa có thể bị giải mã sau khoảng 26/2 = 13 lần thử khóa

- Cho bản mã

JBCRCLQRWCRVNBJENBWRWN

- Lần lượt thử các khóa k = 0, 1, 2, … 25

jbcrclqrwcrvnbjenbwrwn
iabqbkpqvbqumaidmavqvm
hzapajopuaptlzhclzupul
gyzozinotzoskygbkytotk
fxynyhmnsynrjxfajxsnsj
ewxmxglmrxmqiweziwrmri
dvwlwfklqwlphvdyhvqlqh
cuvkvejkpvkogucxgupkpg
btujudijoujnftbwftojof
astitchintimesavesnine

- Cho bản mã

  JBCRCLQRWCRVNBJENBWRWN

- Lần lượt thử các khóa k = 0, 1, 2, … 25

  jbcrclqrwcrvnbjenbwrwn
  iabqbkpqvbqumaidmavqvm
  hzapajopuaptlzhclzupul
  gyzozinotzoskygbkytotk
  fxynyhmnsynrjxfajxsnsj
  ewxmxglmrxmqiweziwrmri
  dvwlwfklqwlphvdyhvqlqh
  cuvkvejkpvkogucxgupkpg
  btujudijoujnftbwftojof
  astitchintimesavesnine ← *k*=9

Phương pháp mã hóa thay thế

Substitution Cipher:

- Phương pháp mã hóa nổi tiếng
- Được sử dụng phổ biến hàng trăm năm nay
- Thực hiện việc mã hóa thông điệp bằng cách hoán vị các phần tử trong bảng chữ cái hay tổng quát hơn là hoán vị các phần tử trong tập nguồn *P*

Phương pháp mã hóa thay thế

Cho $P = C = Z_n$

K là tập hợp tất cả các hoán vị của n phần tử $0,1,\ldots,n-1$. Như vậy, mỗi khóa $\pi \in K$ là một hoán vị của n phần tử $0,1,\ldots,n-1$.

Với mỗi khóa $\pi \in K$, định nghĩa:

$e_\pi(x) = \pi(x)$ và $d_\pi(y) = \pi^{-1}(y)$ với $x, y \in \mathbf{Z}_n$

$E = \{e_\pi, \pi \in K\}$ và $D = \{D_\pi, \pi \in K\}$

Phương pháp mã hóa thay thế

- Đơn giản, thao tác mã hóa và giải mã được thực hiện nhanh chóng
- Không gian khóa K gồm $n!$ phần tử
- Khắc phục hạn chế của phương pháp Shift Cipher: việc tấn công bằng cách vét cạn các giá trị khóa $k \in K$ là không khả thi

Thật sự an toàn???

Phương pháp mã hóa thay thế

AO VCO JO IBU RIBU

AO VCO JO IBU

?A H?A ?A

MA HOA VA UNG DUNG

Tấn công dựa trên tần số xuất hiện của ký tự trong ngôn ngữ

Phương pháp mã hóa thay thế

L FDPH L VDZ L FRQTXHUHG

L FDPH L VDZ L FRQTXHUHG

i ?a?e i ?a? i ?????e?e?

i came i saw i conquered

Phương pháp mã hóa thay thế

- Phân tích tần số
  - Ký tự: E > T > R > N > I > O > A > S
  - Nhóm 2 ký tự (digraph): TH > HE > IN > ER > RE > ON > AN > EN
  - Nhóm 3 ký tự (Trigraph): THE > AND > TIO > ATI > FOR > THA > TER > RES

Một số phương pháp khác

- Phương pháp Affine
- Phương pháp Vigenere
- Phương pháp Hill
- Phương pháp mã hoá hoán vị
- Phương pháp mã hoá bằng phép nhân
- Phương pháp DES (Data Encryption Standard)
- Phương pháp chuẩn mã hoá nâng cao AES

Tham khảo tài liệu MaHoa&UngDung_Ch02.pdf

Chiến lược mã hoá

- Mã hoá đối xứng được thực hiện theo 2 chiến lược:

1. Block Ciphers
   - Mã hoá từng block dữ liệu (thông thường 1 block là 64 bits hoặc 128 bits)
2. Stream Ciphers
   - Mã hoá từng bit hoặc từng byte dữ liệu

Các thuật toán Mã hoá đối xứng phổ biến

Algorithm	Type	Key Size	Features
DES	Block Cipher	56 bits	Most Common, Not strong enough
TripleDES	Block Cipher	168 bits (112 effective)	Modification of DES, Adequate Security
Blowfish	Block Cipher	Variable (Up to 448 bits)	Excellent Security
AES	Block Cipher	Variable (128, 192, or 256 bits)	Replacement for DES, Excellent Security
RC4	Stream Cipher	Variable (40 or 128 bits)	Fast Stream Cipher, Used in most SSL implementations