CHƯƠNG 1

TỔNG QUAN VỀ AN TOÀN THÔNG TIN VÀ MẬT MÃ HỌC

Nguồn tài liệu: Handbook of Applied Cryptography

Katz Jonathan, Menezes Alfred J, Van Oorschot Paul C, Vanstone Scott A

CRC Press

Giới thiệu chung

- Mã hóa có lịch sử lâu đời

  CEASAR cipher có 100 năm trước C.N

- Sự bùng nổ của máy tính những năm 1960s

  Yêu cầu càng cao của bảo vệ thông tin

- Phát triển nhảy vọt nhất trong ngành mật mã

  Mật mã khóa công khai (Public-key) vào 1978

Giới thiệu chung

- Cống hiến quan trọng của Public-key:

  Chữ ký số (Digital signature)

- Hiện tại tốc độ phát triển nhanh chóng của việc:
  - Tìm kiếm các mô hình public-key mới
  - Cải thiện các kỹ thuật mã hóa đang có
  - Lý thuyết về bảo mật

Đối tượng quan tâm của an toàn thông tin

- Privacy/ Confidentiality

  Giữ bí mật thông tin chỉ người có thẩm quyền mới biết

- Data integrity

  Đảm bảo thông tin không bị chỉnh sửa khi không có thẩm quyền hoặc phương pháp chưa biết

- Entity authentication/ identification

  Xác thực một thực thể, đối tượng

Đối tượng quan tâm của an toàn thông tin

- Message authentication

  Xác thực nguồn tin/dữ liệu

- Signature

  Phương pháp gắn thêm thông tin với thực thể

- Authorization

  Cấp quyền cho ai đó làm hoặc không làm

Đối tượng quan tâm của an toàn thông tin

- Validation

Phương pháp cấp quyền để sử dựng hoặc thao tác với thông tin hoặc nguồn dữ liệu

- Access control

Giới hạn quyền truy cập nguồn thông tin cho nhóm người

- Certification

Sự tán thành chính thức với thông tin bởi thực thể tin tưởng

Đối tượng quan tâm của an toàn thông tin

- Timestamping

  Lưu trữ thời gian tạo và tồn tại của thông tin

- Witnessing

  Xác thực việc tạo hoặc tồn tại của thông tin bởi thực thể/ người tạo khác

- Receipt

  Ghi nhận thông tin đã được nhận

Đối tượng quan tâm của an toàn thông tin

- Confirmation

  Ghi nhận dịch vụ đã được cung cấp

- Ownership

  Là cách cung cấp một thực thể với quyền sử dụng hoặc chuyển một nguồn dữ liệu cho thực thể khác

- Anonymity

  Ngăn không cho biết một thực thể liên quan đến tiến trình xử lý nào đó

Đối tượng quan tâm của an toàn thông tin

- Non-repudiation

  Ngăn chặn từ chối dịch vụ theo cam kết trước

- Revocation

  Việc rút lại chứng chỉ hoặc quyền

Mật mã học

Định nghĩa:

Mật mã học là nghiên cứu các kỹ thuật toán liên hệ với các khía cạnh của an toàn thông tin như:

- Bảo mật (confidentiality),
- Toàn vẹn dữ liệu (data integrity),
- Xác thực thực thể (entity authentication) và
- Xác thực nguồn gốc dữ liệu (data origin authentication)

Mục tiêu cơ bản của mật mã học

- Bảo mật (Confidentiality)
- Toàn vẹn dữ liệu (Data integrity)
- Xác thực (Authentication)
- Không từ chối dịch vụ (Non-repudation)

Đánh giá một công cụ bảo mật

- Mức độ bảo mật
- Chức năng
- Phương pháp vận hành
- Khả năng thực hiện
- Tính dễ cài đặt

Ký hiệu và thuật ngữ cơ bản về mã hóa

- $\mathcal{A}$: Bảng ký tự mã (Alphabet of definition)

  VD: $\mathcal{A}$ = {0,1}, hay

  $\mathcal{A}$ = {A,B,…,Z}

- $\mathcal{M}$: Không gian các tin cần mã hóa, chứa xâu các ký tự từ bảng ký tự mã hóa $\mathcal{A}$

- $\mathcal{C}$: Không gian các tin được mã hóa, là xâu các ký tự từ bảng ký tự mã hóa với $\mathcal{M}$ hoặc khác.

- $\mathcal{K}$: Không gian khóa, mỗi phần từ của $\mathcal{K}$ gọi là một khóa

Ký hiệu và thuật ngữ cơ bản về mã hóa

- Mỗi phần tử $e \in \mathcal{K}$ xác định duy nhất một tương ứng 1-1 từ $\mathcal{M}$ vào $\mathcal{C}$ ký hiệu là E_e gọi là hàm hay biến đổi mã hóa
- Mỗi phần tử $\mathrm{d} \in \mathcal{K}$ xác định duy nhất một tương ứng 1-1 từ $\mathcal{C}$ vào $\mathcal{M}$ ký hiệu là D_d gọi là hàm hay biến đổi giải mã
- Một hệ mật mã hay lược đồ mã hóa:

Gồm tập $\{E_e: e \in \mathcal{K}\}$ các biến đổi mã hóa và tương ứng $\{D_d: d \in \mathcal{K}\}$ các biến đổi giải mã và có tính chất $\forall e \in \mathcal{K}$ xác định duy nhất một $\mathrm{d} \in \mathcal{K}$ sao cho $D_d = E_e^{-1}$. Khi đó (e,d) gọi là cặp khóa.

Kênh truyền thông

- Một kênh truyền thông: là cách truyền tải dữ liệu từ một thực thể đến thực thể khác
- Phân loại:
  - Kênh bảo mật/ an toàn: Kẻ địch không có khả năng thâm nhập để đọc và chỉnh sửa thông tin
  - Kênh không an toàn: Kẻ địch có thể thâm nhập để đọc và chỉnh sửa thông tin

Định nghĩa về phá mã

Định nghĩa

Một hệ mật mã được gọi là có thể phá được nếu một bên thứ 3 không biết trước cặp khóa (e,d) về hệ thống có thể khôi phục tin gốc từ mã hóa của tin đó trong một khoảng thời gian thích hợp.

Chú ý: Do phương pháp tìm kiếm vét cạn (exhaustive search) nên không gian khóa phải có kích thước đủ lớn

Phân loại hệ mật mã

- Hệ mật mã khóa đối xứng (Symmetric-key encryption)

***Định nghĩa**: Một hệ mật mã gồm* $\{E_e: e \in \mathcal{K}\}$ *và* $\{D_d: d \in \mathcal{K}\}$ *tương ứng gọi là hệ mật mã khóa đối xứng nếu ở mỗi cặp (e, d) thì ta dễ dàng tìm được d khi biết e và ngược lại.*

Phân loại hệ mật mã

- Hệ mật mã khối (Block cipher)

Định nghĩa*: Là một hệ mật mã mà quá trình mã hóa chia tin gốc thành các khối có kích thước bằng nhau để mã hóa trên từng khối đó.*

Phân loại hệ mật mã

- Hệ mật mã dòng (Stream cipher)

***Định nghĩa**: Là một hệ mật mã khối mà kích thước mỗi khối bằng 1.*

$$\begin{cases} m = (m_1 m_2 m_3 \dots) \\ c = (c_1 c_2 c_3 \dots) \\ e = (e_1 e_2 e_3 \dots) \end{cases} \Rightarrow E_{e_i}(m_i) = c_i,\ D_{d_i}(c_i) = m_i$$

Phân loại hệ mật mã

- Hệ mật mã khóa công khai (Public-key encryption)

***Định nghĩa**: Một hệ mật mã gồm* $\{E_e: e \in \mathcal{K}\}$ *và* $\{D_d: d \in \mathcal{K}\}$ *tương ứng gọi là hệ mật mã khóa công khai nếu ở mỗi cặp (e, d) thì e được cho công khai trong khi d giữ bí mật ở đó sẽ không khả thi để tìm d từ e.*

Nội dung bài kiểm tra 1

- Xác định các đối tượng của ATTT
- Mục tiêu của mật mã học
- Cách đánh giá một công cụ bảo mật
- Định nghĩa và phân loại về các hệ mật mã
- Các thuật ngữ cơ bản liên quan đến hệ mật mã và an toàn thông tin
- Tính toán với hệ mật mã cổ điển: Shift-cipher, Hill, thay thế, chuyển vị, Vigenere.