MẬT MÃ ỨNG DỤNG TRONG AN TOÀN THÔNG TIN

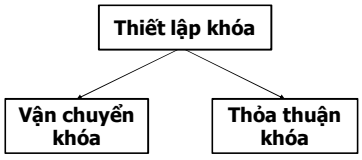
Bài 08. Thiết lập khóa

1. Một số khái niệm, định nghĩa
2. Vận chuyển khóa dựa trên mã hóa đối xứng
3. Thỏa thuận khóa dựa trên các kỹ thuật đối xứng
4. Vận chuyển khóa dựa trên mã hóa khóa công khai
5. Thỏa thuận khóa dựa trên kỹ thuật phi đối xứng
6. Một số kỹ thuật khác

1. Một số khái niệm, định nghĩa
2. Vận chuyển khóa dựa trên mã hóa đối xứng
3. Thỏa thuận khóa dựa trên các kỹ thuật đối xứng
4. Vận chuyển khóa dựa trên mã hóa khóa công khai
5. Thỏa thuận khóa dựa trên kỹ thuật phi đối xứng
6. Một số kỹ thuật khác

Một số khái niệm, định nghĩa

- **Thiết lập khóa** (**key establishment**) là một tiến trình hoặc giao thức mà nhờ nó một bí mật chung được thiết lập để dùng cho hai hoặc nhiều hơn các bên, cho việc sử dụng mật mã tiếp sau.



1. Một số khái niệm, định nghĩa
2. Vận chuyển khóa dựa trên mã hóa đối xứng
3. Thỏa thuận khóa dựa trên các kỹ thuật đối xứng
4. Vận chuyển khóa dựa trên mã hóa khóa công khai
5. Thỏa thuận khóa dựa trên kỹ thuật phi đối xứng
6. Một số kỹ thuật khác

Vận chuyển khóa dựa trên mã hóa đối xứng

- **Một số giao thức**:

Giao thức \ Thuộc tính	Kiểu máy chủ	Sử dụng tem thời gian	Số thông báo
Cập nhật khóa điểm-tới-điểm	Không có	Tùy chọn	1-3
Giao thức không dùng khóa của Shamir	Không có	Không	3
Chia sẻ khóa Needham-Schroeder	KDC	Không	5

Cập nhật khóa điểm – điểm dựa trên mã hóa đối xứng

- **Một số ký hiệu:**
  - r_A, t_A và n_A, tương ứng là ký hiệu một số ngẫu nhiên, tem thời gian và số tuần tự được sinh bởi A
  - E là một thuật toán mã hóa khóa đối xứng
- Giao thức này sử dụng một khóa đối xứng dài hạn K được chia sẻ giữa A và B.

7

Cập nhật khóa điểm – điểm dựa trên mã hóa đối xứng

- **Vận chuyển khóa một lần chuyển:**

$$A \rightarrow B: E_K(r_A, t_A^*, B^*) \quad (1)$$

- Phần có dấu * là tùy chọn

8

Cập nhật khóa điểm – điểm dựa trên mã hóa đối xứng

- **Vận chuyển khóa với quá trình hỏi - đáp:**

$$A \leftarrow B: n_B \quad (1)$$
$$A \rightarrow B: E_K(r_A, n_B, B^*) \quad (2)$$

- Phần có dấu * là tùy chọn

9

Cập nhật khóa sử dụng hàm KDF và hàm một chiều

- **Giao thức trao đổi khóa có xác thực số 2:**
  - Cho phép thiết lập khóa phiên và xác thực lẫn nhau giữa 2 bên, xác thực khóa

10

Cập nhật khóa sử dụng hàm KDF và hàm một chiều

- **Thiết lập**
  - A và B chia sẻ các khóa đối xứng thời hạn dài là K, K'.
  - h_k là một mã xác thực thông điệp MAC
  - h'_k là hàm một chiều

11

Cập nhật khóa sử dụng hàm KDF và hàm một chiều

- **Hoạt động của giao thức**

$$A \rightarrow B: r_A \quad (1)$$
$$A \leftarrow B: T, h_K(T) \quad (2)$$
$$A \rightarrow B: (A, r_B), h_K(A, r_B) \quad (3)$$

A và B tính khóa chung: $W = h'_{K'}(r_B)$

trong (2) T=(B, A, r_A, r_B).

12

Cập nhật khóa sử dụng hàm KDF và hàm một chiều

❑Các hoạt động của giao thức

1. *A* chọn và gửi cho *B* một số ngẫu nhiên r_A.
2. *B* chọn một số ngẫu nhiên r_B và gửi cho *A* các giá trị (*B*, *A*, r_A, r_B), cùng với một MAC trên những đại lượng này được sinh ra nhờ *h* với khóa *K*.
3. Khi nhận được thông báo (2), *A* kiểm tra rằng các định danh là đúng, r_A đã nhận được trùng với r_A ở trong (1) và kiểm tra MAC.
4. *A* gửi tới *B* các giá trị (*A*, r_B), cùng với MAC trên nó $h_K(A, r_B)$.
5. Khi nhận được (3), *B* kiểm tra rằng MAC là đúng, và rằng giá trị đã nhận được r_B trùng với giá trị mà đã được gửi đi trước đó.
6. Cả *A* và *B* tính khóa phiên như là $W = h'_{K'}(r_B)$

13

Giao thức không dùng khóa của Shamir

❑Thiết lập tham số hệ thống

1. Chọn một số nguyên tố lớn p.
2. *A* và *B* chọn ngẫu nhiên $\boldsymbol{a}, \boldsymbol{b} \in [1, \mathrm{p} - 2]$ **nguyên tố cùng nhau** với $\boldsymbol{p} - \mathbf{1}$ và **giữ bí mật**. A và B tính $\boldsymbol{a}^{-1}$ và $\boldsymbol{b}^{-1}\ mod\ p - 1$.

14

Giao thức không dùng khóa của Shamir

❑Hoạt động của giao thức

$A \rightarrow B: \beta_A = K^a mod\ p$ (1)

$A \leftarrow B: \beta_B = (\beta_A)^b\ mod\ p$ (2)

$A \rightarrow B: \beta = (\beta_B)^{a^{-1}}\ mod\ p$ (3)

B tính $(\beta)^{b^{-1}} mod\ p$ để nhận được khóa chung là K.

15

Giao thức thiết lập khóa Needham-Schroeder

Điều kiện:

- Alice và Trung tâm chia sẻ khóa K_{AT};
- Bob và Trung tâm chia sẻ K_{BT};

Yêu cầu:

- Alice và Bob thiết lập khóa chia sẻ K

16

Giao thức thiết lập khóa Needham-Schroeder

Thực hiện:

1. A → T: Alice, Bob, N_A;
2. T → A: {N_A, K, Bob, {K, Alice}K_{BT}}K_{AT};
3. A → B: {K, Alice}K_{BT};
4. B → A: {N_B}K;
5. A → B: {$N_B - 1$}K.

17