CHƯƠNG VII

Vấn đề phân phối khoá và thoả thuận khoá

Bài 7.1. Quản trị khoá trong các mạng truyền tin.

Trong các chương trước, ta đã làm quen với các phương pháp lập mật mã và các bài toán quan trọng khác liên quan đến việc truyền tin bảo mật trên các mạng truyền tin công cộng nói chung. Ta cũng đã thấy rằng các hệ mật mã khoá công khai có nhiều ưu

việt hơn các hệ mật mã khoá đối xứng trong việc làm nền tảng cho các giải pháp an toàn thông tin, và đặc biệt nếu đối với các hệ mật mã khoá đối xứng việc thực hiện đòi hỏi những kênh bí mật để chuyển khoá hoặc trao đổi khoá giữa các đối tác, thì về nguyên tắc, đối với các hệ mật mã khoá công khai, không cần có những kênh bí mật như vậy, vì các khoá công khai có thể được truyền hoặc trao đổi cho nhau một cách công khai qua các kênh truyền tin công cộng.

Tuy nhiên, trên thực tế, để bảo đảm cho các hoạt động thông tin được thật sự an toàn, không phải bất cứ thông tin nào về các khoá công khai của một hệ mật mã, của một thuật toán kiểm thử chữ ký, của một giao thức xác nhận thông báo hay xác nhận danh tính, v.v... cũng được phát công khai một cách tràn lan trên mạng công cộng, mà dẫu là công khai nhưng người ta cũng mong muốn là những ai cần biết thì mới nên biết mà thôi. Do đó, dẫu là dùng các hệ có khoá công

khai, người ta cũng muốn có những giao thức thực hiện việc trao đổi khoá giữa những đối tác thực sự có nhu cầu giao lưu thông tin với nhau, kể cả trao đổi khoá công khai. Việc trao đổi khoá giữa các chủ thể trong một cộng đồng nào đó có thể được thiết lập một cách tự do giữa bất cứ hai người nào khi có nhu cầu trao đổi thông tin, hoặc có thể được thiết lập một cách tương đối lâu dài trong một thời hạn nào đó trong cả cộng đồng với sự điều phối của một cơ quan được

uỷ thác (mà ta ký hiệu là TA-trusted authority).

Việc trao đổi khoá trong trường hợp thứ nhất ta gọi đơn giản là *thoả thuận khoá*, còn trong trường hợp thứ hai ta gọi là *phân phối khoá* , TA là nơi thực hiện việc phân phối, cũng tức là nơi quản trị khoá.

Việc thoả thuận khoá nói chung không cần có sự tham gia của một TA nào và chỉ có thể xẩy ra khi các hệ bảo mật mà ta sử dụng là hệ có khoá công khai, còn việc phân phối khoá thì có

thể xẩy ra đối với các trường hợp sử dụng các hệ khoá đối xứng cũng như các hệ có khoá công khai. Việc phân phối khoá với vai trò quản trị khoá của một TA là một việc bình thường, đã tồn tại từ rất lâu trước khi có các hệ mật mã khoá công khai.

Ta sẽ bắt đầu với việc giới thiệu một vài hệ phân phối khoá như vậy, rồi tiếp sau sẽ giới thiệu một số hệ phân phối hoặc trao đổi khoá khi dùng các sơ đồ an toàn và bảo mật có khoá công khai.