Bài 4.0 Mở đầu về chữ ký số

Trong cách thức truyền thống, thông báo được truyền đi trong giao dịch thường dưới dạng các văn bản viết tay hoặc đánh máy được kèm thêm chữ ký (viết tay) của người gửi ở bên dưới văn bản.

Chữ ký đó là bằng chứng xác nhận thông báo đúng là của người ký, tức là của chủ thể giao dịch, và nếu tờ giấy mang văn bản không bị cắt, dán, tẩy, xoá, thì tính toàn vẹn của thông báo

cũng được chứng thực bởi chữ ký đó.

Chữ ký viết tay có nhiều ưu điểm quen thuộc như dễ kiểm thử, không sao chép được, chữ ký của một người là giống nhau trên nhiều văn bản, nhưng mỗi chữ ký gắn liền với một văn bản cụ thể, v.v...

Khi chuyển sang cách thức truyền tin bằng phương tiện hiện đại, các thông báo được truyền đi trên các mạng truyền tin số hoá, bản thân các thông báo cũng được biểu diễn dưới dạng số hoá,

tức dưới dạng các dãy bit nhị phân, "chữ ký" nếu có cũng ở dưới dạng các dãy bit, thì các mối quan hệ tự nhiên kể trên không còn giữ được nữa.

Chẳng hạn, "chữ ký" của một người gửi trên những văn bản khác nhau phải thể hiện được sự gắn kết trách nhiệm của người gửi đối với từng văn bản đó thì tất yếu phải khác nhau chứ không thể là những đoạn bit giống nhau như các chữ ký giống nhau trên các văn bản thông thường.

Chữ ký viết tay có thể được kiểm thử bằng cách so sánh với nguyên mẫu, nhưng "chữ ký" điện tử thì không thể có "nguyên mẫu" để mà so sánh, việc kiểm thử phải được thực hiện bằng những thuật toán đặc biệt.

Một vấn đề nữa là việc sao chép một văn bản cùng chữ ký. Nếu là văn bản cùng chữ ký viết tay thì dễ phân biệt bản gốc với bản sao, do đó khó mà dùng lại được một văn bản có chữ ký thật. Còn với văn bản điện tử cùng chữ ký điện tử thì có thể nhân

bản sao chép tuỳ thích, khó mà phân biệt được bản gốc với bản sao, cho nên nguy cơ dùng lại nhiều lần là có thực, do đó cần có những biện pháp để tránh nguy cơ đó.

Một "chữ ký", nếu muốn thể hiện được trách nhiệm của người gửi trên toàn văn bản, thì phải mang được một chút gắn bó nào đó với từng bit thông tin của văn bản, vì vậy, theo hình dung ban đầu, độ dài của chữ ký cũng phải dài theo độ dài của văn bản; để có được "chữ ký ngắn" như

trong trường hợp viết tay người ta phải dùng một kỹ thuật riêng gọi là *hàm băm* mà ta sẽ trình bày ở cuối chương.

Bây giờ, trước hết ta sẽ giới thiệu định nghĩa về sơ đồ chữ ký (điện tử).