Chapter 04A: Hàm Hash.

Đặc điểm:

Giá trị của hàm Hash là giá trị có độ dài xác định dù cho độ dài tin nhắn như thế nào.

Hàm Hash dùng để xác định toàn vẹn dữ liệu.

Hash functions dùng để chức năng khác:

Phát hiện xâm nhập hay virus.

Tạo one-way password file.

Collision Resistant Attacks:

Bằng cách nào đó tìm ra H(x)=H(y); có xác suất khi thực hiện 2m/2.

SHA1: là 160bits.