1. **Các điểm yếu của SHA**

* **SHA0:**

Khi 2 thông điệp muốn mã hóa có giá trị gần như nhau, trong trường hợp này họ phát hiện 142bit trong số 160 bít bằng nhau và các va chạm hoàn toàn của SHA-0 giảm xống còn 62 trong 80 vòng theo nghiên cứu trước đó của thuật toán.

* **SHA1:**

Năm 2005, điểm yếu mật mã đã được phát hiện trong SHA-1. Hàm băm được thiết kế để giảm thiểu xác suất 2 dữ liệu đầu vào khác nhau lại cho đầu ra 2 giá trị băm giống nhau, điều đó có nghĩa là có thể có 2 dữ liệu đầu vào khác nhau cho đầu ra là 2 giá trị băm giống nhau, theo Cryptographic hash collision.

•Khi sử dụng SHA để mã hóa mật khẩu : phương pháp này cũng không khó khăn cho những kẻ tấn công khi chúng có thư viện mật khẩu.

1. **Một số kiểu tấn công:**

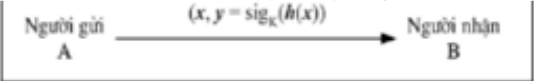
* **Không va chạm yếu:**

HAS là không va chạm yếu nếu cho trước một bức điện x không thể tiến hành về mặt tính toán để tìm ra bức điện x' # x mà h(x') = h(x)

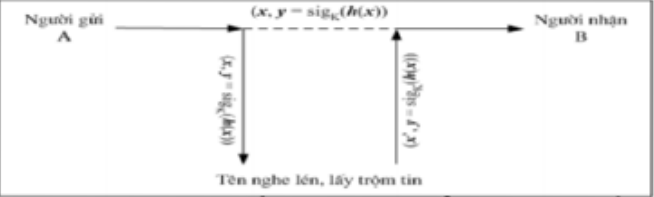
VD :

- Xét một kiểu tấn công như sau :

+ Đáng lẽ : thông tin được truyền từ A -> B



+ Nhưng : trên đường truyền, thông tin bị lấy trộm và bị thay đổi



- Người A gửi cho người B (x,y) với y = sigK (h(x)). Những trên đường truyền, bị lấu trộm. tên trộm bằng cách nào đó tìm được một bản thông điệp x' có h(x') = h(x) mà x'#x, sau đó hắn đưa x' thay thế x rồi truyền cho người B - và người B nhận được vẫn xác thực được thông tin đúng đắn

* **Một số kiểu tấn công khác:**

**• Không va chạm mạnh** :

- SHA là không va chạm mạnh nếu không có khả năng tính toán để tìm ra hai bức thông điệp x và x’ mà x # x’ và h(x) = h(x’).

- VD : xét kiểu tấn công giả mạo như sau : đầu tiên giả mạo tìm ra được hai bức thông điệp x và x' (x' # x) mà có h(x') = h(x) (ta coi bức thông điệ x là hợp lệ

còn x' là giả mạo) tiếp theo, hắn đưa cho ông A và thuyệt phục ông này ký vào bản tóm lược h(x) để nhận được y khi đó (x', y) là bức điện giả mạo nhưng hợp lệ.

**• Hàm một chiều :**

- SHA là một chiều nếu khi cho trước một bản tóm lược thông báo z thì không thể thực hiện về mặt tính toán để tìm ra thông điệp ban đầu x sao cho h(x) = z .

- VD : xét một kiểu tấn công như sau : việc giả mạ các chữ ký trên bản tóm lược z thường xảy ra với các sơ đồ chữ ký số. giả sử tên giả mạo tính chữ ký trên bản tóm lược z, sau đó hắn tìm một bản thông điệp x' được tính ngược từ bản đại diện z , z = h(x'). tên trộm thay thế bản thông điệp x hợp lệ bằng bản thông điệp x' giả mạo, nhưng lại có z = h(x') và hắn ký số trên bản đại diện cho x' bằng đúng chữ ký hợp lệ. nếu làm được như vậy thì (x' y) là bước điện giả mạo hợp lệ.