**TRƯỜNG ĐẠI HỌC HÀNG HẢI VIỆT NAM  
KHOA CÔNG NGHỆ THÔNG TIN**

**-----\*\*\*-----**



**BÁO CÁO BÀI TẬP LỚN**

**HỌC PHẦN: An toàn bảo mật thông tin**

**Đề tài: Mã hóa dữ liệu SHA-1**

**Người hướng dẫn: Nguyễn Thị Hương Thơm**

**Sinh viên thực hiện: Nguyễn Tuấn Vũ – 51275**

**Nguyễn Viết Duy - 51208**

**Phạm Trung Hiếu - 51217**

**Nguyễn Hồng Thanh – 51246**

**Trần Trung Thắng - 51253**

**Hải phòng, tháng 04, năm 2017**

Mục lục

[Chương 1: Giới thiệu về SHA-1 2](#_Toc479186548)

[**1.1 Lịch sử 2**](#_Toc479186549)

[**1.2 Khái niệm 2**](#_Toc479186550)

[**1.3 Ứng dụng 2**](#_Toc479186551)

[**1.4 Giải thuật 3**](#_Toc479186552)

[**1.5 Đánh giá 5**](#_Toc479186553)

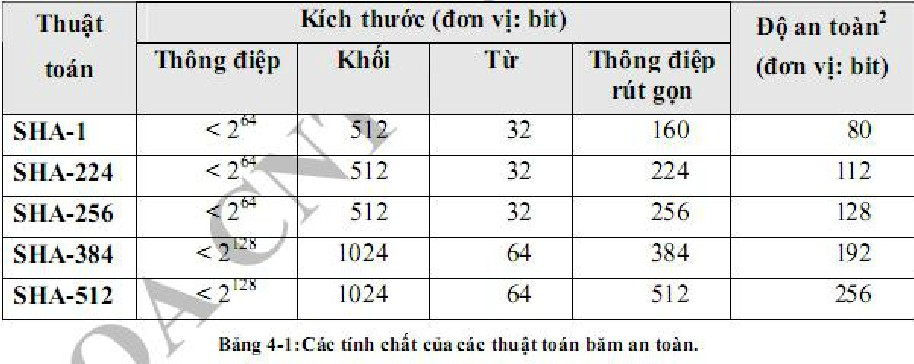
[Chương 2: 6](#_Toc479186554)

# Chương 1: Giới thiệu về SHA-1

* 1. **Lịch sử**

SHA-1 là thuật toán băm 1 chiều dùng trong rất nhiều hệ thống như SSH, SSL, PGP,…Nó được cơ quan an ninh Mỹ phát minh năm 1995 và trở thành chuẩn bảo mật cơ sở phổ biến nhất trên Internet và là thuật toán chữ kí điện tủ duy nhất được Cơ quan Chuẩn Chữ Kí Số của chính phủ Mỹ phê chuẩn.

* 1. **Khái niệm**
* Định nghĩa: Trong mật mã học, SHA-1 là 1 hàm băm mật mã được thiết kế bởi Cơ quan An Ninh Quốc Gia và được công bố bởi NIST hay còn gọi là cục xử lý Thông Tin Tiêu Chuẩn Liên Bang của Mỹ.
* Phân loại các loại mã SHA



* 1. **Ứng dụng**
* Các SHA-1 có thể được sử dụng với các DSA trong thư điện tử, chuyển tiền điện tử, phân phối phần mềm, lưu trữ dữ liệu, và các ứng dụng khác cần đảm bảo tính toàn vẹn dữ liệu và xác thực nguồn gốc dữ liệu. Các SHA-1 cũng có thể sử dụng bất cứ khi nào nó là cần thiết để tạo ra 1 phiên bản đặc của tin nhắn.
* Hàm SHA-1 còn được sử dụng trên Wii của Nintendo để xác minh chữ kí thời gian khởi động.
* SHA-1 và SHA-2 là những thuật toán băm an toàn theo yêu cầu của pháp luật để sử dụng trong 1 số ứng dụng cảu Chính Phủ Hoa Kì, bao gồm cả sử dụng trong các thuật toán mã hóa khác và ác giao thức, để bảo vệ thông tin mật nhạy cảm. Nhưng hiện nay thì Chính Phủ không còn sử dụng SHA-1 nữa nhưng thay vào đó là SHA-2.
* Các hàm băm SHA được dùng làm cơ sở cho mã khối SHACAL.
  1. **Giải thuật**

Gồm 5 bước.

Đầu vào: chuỗi có độ dài tối đa 2^64 bits.

Đầu ra: giá trị băm có độ dài 160 bits.

Bước 1: nhồi thêm dữ liệu

Thông điệp được nhồi thêm các bits sao cho độ dài l = 448 mod 512 hay l = n\*512 + 448(n,l nguyên).

Thông điệp luôn được nhồi thêm dữ liệu.

Số bits nhồi them nằm trong khoảng 1 đến 512.

Phần dữ liệu nhồi them bao gồm 1 bit 1 và theo sau bởi các bit 0.

Bước 2: Thêm vào độ dài

Độ dài ban đầu của khối dữ liệu được biểu diễn dưới dạng nhị phân 64 bit và được them vào cuối chuỗi nhị phân kết quả của bước 1.

Độ dài được biểu diễn dưới dạng nhị phân 64 bits không dấu.

Kết quả có được từ 2 bước đầu là khối dữ liệu có độ dài là bội số của 512. Khối dữ liệu được biểu diễn:

Bằng 1 dãy L khối 512 bits.

Bằng 1 dãy N từ (word) 32 bit. Vậy N=L\*16(32\*16=512)

Bước 3: Khởi tạo bộ đệm MD (MD buffet)

1 bộ đệm 160 bit được dùng lưu trữ các giá trị băm trung gian và kết quả. Bộ đệm được biểu diễn bằng 5 thanh ghi 32 bit với các giá trị khởi tạo ở dạng bigiendian (byte có trọng số lớn trong từ nằm ở địa chỉ thấp nhất)

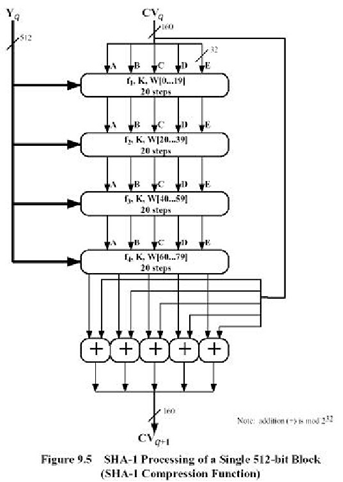
Bước 4: Xử lý các khối dữ liệu 512 bit

Trọng tâm của giải thuật bao gồm 4 vòng lặp thực hiện tất cả 80 bước, 4 vòng lặp có cấu trúc như nhau, chỉ khác nhau ở các hàm logic f1, f2, f3, f4.

Độ dài của khối dữ liệu ban đầu được biểu diễn dưới dạng nhị phân 64 bit và được thao tác sẽ cập nhật gái trị bộ đệm.

Mỗi bước sử dụng 1 hằng số Kt (0 ≤ t ≤ 79)

Đầu ra của 4 vòng (bước 80) được cộng với đầu ra của bước CV(q), CV(q+1).



Bước 5: Xuất kết quả

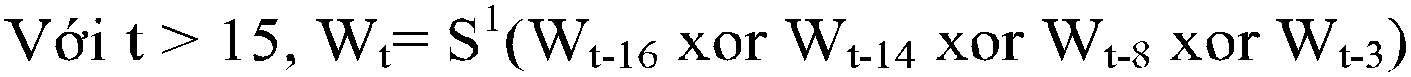
Độ dài của khối dữ liệu ban đầu được biểu diễn dưới dạng nhị phân 64 bit.

Các hàm f:



Từ 16 đến 32 bit từ khối dữ liệu đầu vào, mở rộng thành 80 từ Wt.

Với 0 ≤ t ≤ 15, giá trị Wt lấy trực tiếp từ khối dữ liệu



## Đánh giá

- Ưu điểm:

Bảng băm là 1 cấu trức dung hòa giữa thời gian truy xuất và dung lượng bộ nhớ.

+ Nếu không có sự giới hạn về bộ nhớ: có thể xây dựng bảng băm với mỗi khóa ứng với mỗi địa chỉ với mong muốn thời gian truy xuất tức thời.

+ Nếu dung lượng bộ nhớ có giới hạn: tổ chức 1 số khóa có cùng địa chỉ, tốc độ truy xuất giảm.

Các phép toán trên bảng băm hạn chế số lần so sánh, giảm được thời gian truy xuất.

* Nhược điểm:

Hiện nay vấn đề bảo mật của SHA-1 không còn được tin tưởng sử dụng như trước đó vì:

+ Đầu năm 2005 Rijiman và Oswald đã công bố 1 cuộc tấn công vào phiên bản rút gọn của SHA-1 bằng cách tính ít hơn 2^80 phép tình.

+ 2/2005, 1 cuộc tấn công bởi 3 nhà mật mã học thuộc đại học Shandong (Trung Quốc) đã tìm ra được sự đụng độ trong phiên bản SHA-1 đầy đủ với chỉ 2^69 phép tính , nhanh hơn khoảng 2000 lần so với cách tấn công Brute- Force.

+8/2005, tại hội nghị Mật Mã, họ đã công bố và thuyết trình về việc tấn công này và chỉ ra 1 vụ va chạm tại vòng 58 của SHA-1 chỉ với 2^33 phép tính băm.

+ 18/12/2007, các báo cáo chi tiết kết quả này dược giải thích và xác nhận bởi Martin Cochran.

+ Ngoài ra còn các cuộc nghiên cứu tân công khác nữa.

+ Nhưng nhìn chung thì SHA-1 không có được sự bảo mật tốt nhất như khi nó được công bố vào năm 2004 bởi NIST tại hội nghị Mật Mã năm 2004.

# Chương 2: Cài Đặt

# (thuật toán có trong bản chữ kí RSA)