**Họ Tên: Trịnh Xuân Chinh**

**Lớp: TH24.09**

Kiểm tra

Câu 1: Nêu các giá trị của hàm băm trong an toàn dữ liệu

Các hàm băm mật mã có nhiều ứng dụng trong an toàn thông tin. Nó được sử dụng nhiều trong chữ ký số, mã xác thực thông điệp (MAC) và các hình thức xác thực khác. Ngoài ra, chúng cũng có thể được sử dụng như các hàm băm thông thường, để lập chỉ mục dữ liệu trong bảng băm, lấy đặc trưng của dữ liệu, phát hiện dữ liệu trùng lặp hoặc làm tổng kiểm tra để phát hiện lỗi các dữ liệu ngẫu nhiên

Đảm bảo tính toàn vẹn và xác thực

Đảm bảo tính toàn vẹn là đảm bảo thông tin, dữ liệu nhận được được chính xác giống như khi nó được gửi (tức là không bị sửa đổi, chèn, xóa hay phát lại). Đặc biệt, khi hai bên thực hiện truyền thông trên một kênh truyền thông không an toàn, đòi hỏi một phương pháp để hai bên truyền thông có thể xác thực lẫn nhau..

Xác thực và toàn vẹn thông báo có thể được thực hiện bằng nhiều cách trong đó có cả việc sử dụng mật mã khóa đối xứng nhưng đơn giản nhất là sử dụng hàm MAC và hàm băm.

**Nâng cao hiệu quả chữ ký số**

Hầu như tất cả các lược đồ [chữ ký số](https://bitcoinvietnamnews.com/digital-signature-la-gi) đều yêu cầu tính toán bản tóm lược của thông điệp bằng các hàm băm mật mã. Điều này cho phép việc tính toán và tạo chữ ký được thực hiện trên một khối dữ liệu có kích thước tương đối nhỏ và cố định thay vì trên toàn bộ văn bản dài. Tính chất toàn vẹn thông điệp của hàm băm mật mã được sử dụng để tạo các lược đồ chữ ký số an toàn và hiệu quả.

**Xác minh mật khẩu**

Việc xác minh mật khẩu thường dựa vào các hàm băm mật mã. Mật khẩu người dùng nếu được dưới dạng bản rõ có thể dẫn đến những lỗ hổng bảo mật nghiêm trọng khi tệp mật khẩu bị xâm phạm. Do đó, để làm giảm nguy cơ này, chúng ta thường chỉ lưu trữ giá trị băm của mỗi mật khẩu. Để xác thực người dùng, mật khẩu do người dùng nhập vào được băm và so sánh với giá trị băm được lưu trữ tương ứng. Mật khẩu ban đầu không thể được tính toán lại từ giá trị băm được lưu trữ trong cơ sở dữ liệu.

Câu 2: Nêu phương thức hoạt động của MD5

MD5 chuyển một đoạn thông tin [chiều dài](https://vi.wikipedia.org/wiki/Chi%E1%BB%81u_d%C3%A0i) thay đổi thành một kết quả chiều dài không đổi 128 bit. Mẩu tin đầu vào được chia thành từng đoạn 512 bit; mẩu tin sau đó được [độn](https://vi.wikipedia.org/w/index.php?title=%C4%90%E1%BB%99n_(m%E1%BA%ADt_m%C3%A3_h%C3%B3a)&action=edit&redlink=1) sao cho chiều dài của nó chia chẵn cho 512. Công việc độn vào như sau: đầu tiên một bit đơn, 1, được gắn vào cuối mẩu tin. Tiếp theo là một dãy các số zero sao cho chiều dài của mẩu tin lên tới 64 bit ít hơn so với bội số của 512. Những bit còn lại được lấp đầy bằng một số nguyên 64-bit đại diện cho chiều dài của mẩu tin gốc.

Thuật toán MD5 chính hoạt động trên trạng thái 128-bit, được chia thành 4 từ [32-bit](https://vi.wikipedia.org/wiki/32-bit), với ký hiệu A, B, C và D. Chúng được khởi tạo với những hằng số cố định. Thuật toán chính sau đó sẽ xử lý các khối tin 512-bit, mỗi khối xác định một trạng thái. Quá trình xử lý khối tin bao gồm bốn giai đoạn giống nhau, gọi là vòng; mỗi vòng gồm có 16 tác vụ giống nhau dựa trên hàm phi tuyến F, [cộng mô đun](https://vi.wikipedia.org/w/index.php?title=C%E1%BB%99ng_m%C3%B4_%C4%91un&action=edit&redlink=1), và dịch trái.

Câu 3: Trình bày thuật toán MD5

-Input: xâu đầu vào x có độ dài tối đa 2^64

-Output: chuỗi băm 128 bit -Sơ đồ thuật toán:

Trước tiên thông điệp được đệm vào dãy padding 100...00. Chiều dài của dãy padding được chọn sao cho thông điệp cuối cùng có thể chia làm N block 512 bit M1,M2,...,MN.Quá trình tính giá trị băm của thông điệp là quá trình lũy tiến. Trước tiên block M1 kết hợp với giá trị khởi tạo H0 thông qua hàm F để tính giá trị hash H1. Sau đó block M2 đượckết hợp với H1 để cho ra giá trị hash là H2. Block M3 kết hợp với H2 cho ra giá trị H3. Cứ như vậy cho đến block MN thì có giá trị băm của toàn bộ thông điệp là HN.

H0 là một dãy 128 bit được chia thành 4 từ 32 bit, ký hiệu 4 từ 32 bit trên là abcd. Với a, b, c, d là các hằng số như sau (viết dưới dạng thập lục phân):  
a = 01234567  
b = 89abcdef  
c = fedbca98  
d = 76543210  
  
-Cấu trúc của hàm F như sau:

Tại mỗi bước lũy tiến, các giá trị abcd của giá trị hash Hi-1 được biến đổi qua 64 vòng từ 0 đến 63. Tại vòng thứ j sẽ có 2 tham số là Kj và Wj đều có kích thước 32 bit. Các tham số Kj được tính từ công thức: Kj là phần nguyên của số 2^32 abs(sin(i)) với i biểu diễn theo rad.  
Giá trị block Mi 512 bit được biến đổi qua một hàm message schedule cho ra 64 giá trị W0, W1,…, W63 mỗi giá trị 32 bit. Block Mi 512 bit được chia thành 16 block 32 bit ứng với các giá trị W0, W1, …, W15 (16×32=512). Tiếp theo, 16 giá trị này được lặp lại 3 lần tạo thành dãy 64 giá trị.  
Sau vòng cuối cùng, các giá trị abcde được cộng với các giá trị abcd của Hi-1 để cho ra các giá trị abcd của Hi. Phép cộng ở đây là phép cộng modulo 232.  
Tiếp theo tìm hiểu cấu trúc của một vòng. Việc biến đổi các giá trị abcd trong vòng thứ i được thể hiện trong hình bên dưới.  
  
Note:Phép + trong sơ đồ trên là phép cộng modul 2^32  
Ở đây c lấy giá trị của b, d lấy giá trị của c, a lấy giá trị của d.  
Giá trị b được tính qua hàm:  
t = a + f(b,c,d) + Wi + Ki  
b = b + ROTL(t,s)  
Trong đó : Hàm f(x,y,z):  
f (x,y,z) = (x ^ y) v (\_x ^ z) nếu vòng từ 0 đến 15  
f (x,y,z) = (z ^ x) v (\_z ^ y) nếu vòng từ 16 đến 32  
f (x,y,z) = x xor y xor z nếu vòng từ 32 đến 48  
f (x,y,z) = y xor (x v \_z) nếu vòng từ 49 đến 63  
Hàm ROTL(t, s): t được dịch vòng trái s bit, với s là các hằng số cho vòng thứ i như sau:

Câu 4: Nêu quy trình mã hóa SHA512

SHA-2 bao gồm bốn giải thuật SHA-224, SHA-256, SHA-384 và SHA-512. Ba thuật giải SHA-256, SHA-384 và SHA-512 được xuất bản lần đầu năm 2001 trong bản phác thảo FIPS PUB 180-2. Năm 2002, FIPS PUB 180-2, bao gồm cả SHA-1 được chấp nhận thành chuẩn chính thức. Năm 2004, FIPS PUB 180-2 được bổ sung thêm một biến thể - SHA-224, với mục đích tạo ra một biến thể SHA-2 có độ dài khóa trùng với DES ba lần với 2 khóa ([2TDES](https://vi.wikipedia.org/w/index.php?title=TDES&action=edit&redlink=1)) - 112 bit. Những biến thể SHA-2 này được đăng ký [Bằng sáng chế Hoa Kỳ số 6,829,355](http://www.google.com/patents?vid=6.829).

Về giải thuật, các biến thể của SHA-2 không khác nhau. Mặc dù chúng sử dụng giá trị biến và hằng số cũng như độ dài từ, v.v. khác nhau.

Mặc dù Gilbert và Handschuh (2003) đã nghiên cứu và không tìm ra điểm yếu của những biến thể này, chúng vẫn chưa được kiểm chứng kĩ như SHA-1

Ví dụ: SHA-512

SHA512("The quick brown fox jumps over the lazy dog")

= 07e547d9 586f6a73 f73fbac0 435ed769 51218fb7 d0c8d788 a309d785 436bbb64 2e93a252 a954f239 12547d1e 8a3b5ed6 e1bfd709 7821233f a0538f3d b854fee6

Câu 5: So sánh tính an toàn của MD5 và SHA512

Cơ bản của SHA và MD5

- Thuật toán băm an toàn (SHA) là một nhóm các hàm băm mật mã được phát triển bởi Viện tiêu chuẩn và công nghệ quốc gia Hoa Kỳ (NIST). Message Digest (MD5) là một thuật toán băm phổ biến được phát triển bởi Ron Rivest và được sử dụng trong nhiều ứng dụng Internet ngày nay. Nó là một thuật toán băm mật mã có thể được sử dụng để tạo ra giá trị chuỗi 128 bit từ một chuỗi độ dài tùy ý. Giống như MD5, SHA cũng được sử dụng rộng rãi trong các ứng dụng như SSH, SSL, S-MIME (Bảo mật thư mở rộng / đa mục đích) và IPsec.

Độ dài thông báo cho SHA và MD5

- Tiêu chuẩn xử lý thông tin liên bang (Trin 180-2) chỉ định bốn thuật toán băm an toàn - SHA-1, SHA-256, SHA-384 và SHA-512 - tất cả đều là các hàm băm lặp, một chiều có thể xử lý tin nhắn với chiều dài tối đa là 264 - đến 2128 - các bit để tạo ra biểu diễn ngưng tụ 160 đến 512 bit được gọi là thông báo tiêu hóa. Thuật toán MD5 nhận một thông báo có độ dài tùy ý và tạo ra đầu ra một dấu vân tay 128 bit bit hoặc dữ liệu tiêu hóa tin nhắn của tin nhắn đầu vào.

Bảo mật cho SHA và MD5

- Băm MD5 thường được biểu thị dưới dạng số thập lục phân 32 chữ số và được cho là bị phá vỡ bằng mật mã và có thể có va chạm. Mặc dù, nó là một trong những hàm băm mật mã được công nhận, nhưng nó không phù hợp lý tưởng cho các dịch vụ và ứng dụng dựa trên bảo mật hoặc chữ ký số dựa trên khả năng chống va chạm. SHA, mặt khác, được cho là an toàn hơn MD5. Nó lấy một luồng bit làm đầu vào và tạo ra đầu ra có kích thước cố định. Hiện tại có nhiều biến thể an toàn hơn của SHA-1, bao gồm SHA-256, SHA-384 và SHA-512, với các con số phản ánh sức mạnh của thông báo.

Tóm tắt SHA so với MD5

SHA-1 dường như an toàn hơn MD5 về nhiều mặt. Mặc dù đã có một số cuộc tấn công được biết đến được báo cáo trên SHA-1, nhưng chúng ít nghiêm trọng hơn các cuộc tấn công vào MD5. Hiện tại có nhiều hàm băm an toàn hơn và tốt hơn, chẳng hạn như SHA-256, SHA-384 và SHA-512, tất cả đều thực sự an toàn không có lịch sử tấn công nào được báo cáo về chúng. Mặc dù, MD5 là một trong những hàm băm mật mã được công nhận, nhưng nó không phù hợp lý tưởng cho các dịch vụ và ứng dụng dựa trên bảo mật vì nó bị phá vỡ bằng mật mã. Do đó, MD5 được coi là kém an toàn hơn SHA bởi nhiều nhà chức trách về mật mã. Thuật toán SHA chậm hơn một chút so với MD5, nhưng độ dài tiêu hóa thư lớn hơn giúp nó an toàn hơn trước các cuộc tấn công đảo ngược và va chạm mạnh mẽ.