Secure Hash Algorithm-512 (SHA-512)\_ Thuật toán băm an toàn:

1. Tổng quan:

* được phát triển bởi Viện Nghiên cứu Quốc giaTiêu chuẩn và Công nghệ
* thành viên của gia đình SHA-2
* phiên bản mới nhất của thuật toán băm an toàn
* dựa trên sơ đồ Merkle-Damgard
* kích thước tin nhắn tối đa -1 bit
* kích thước khối 1024 bit
* kích thước thông báo tóm tắt 512 bit
* số vòng 80
* kích thước từ 64 bit

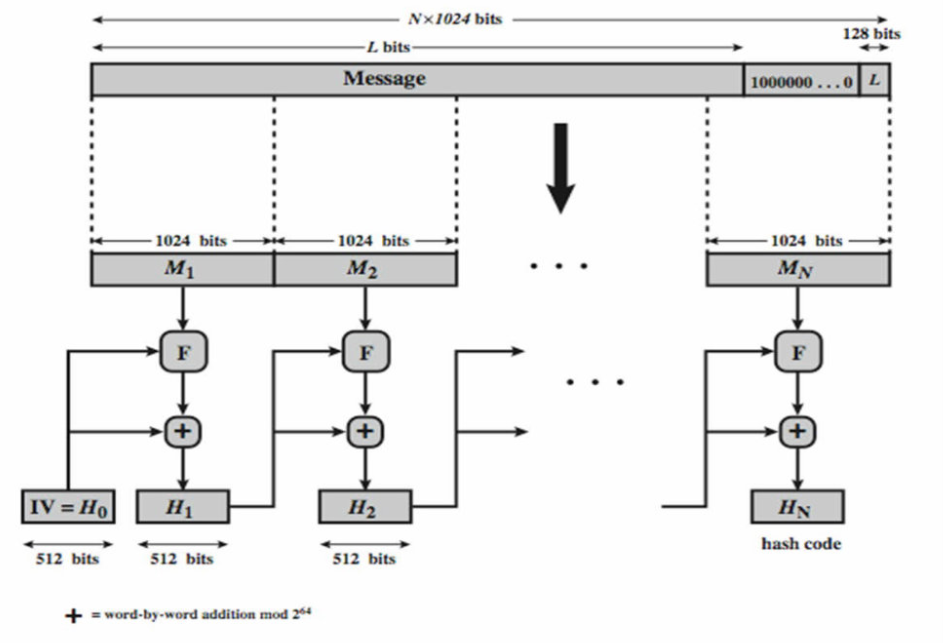
2. Phân tích mật mã SHA-512

SHA-512 cũng là nằm trong SHA-2, nó có khả năng nhận đầu với với số lương hai lũy thừa một trăm hai mươi tám bit, SHA-512 trải qua nhiều hơn 25% vòng lặp so với SHA-256 vì vậy nó có độ trễ so với SHA-256. Trên bộ xử lý 64 bit, mỗi vòng có cùng số lượng thao tác, nhưng có thể xử lý gấp đôi dữ liệu mỗi vòng, vì các hướng dẫn xử lý các từ 64 bit thay vì các từ 32 bit. SHA-512 có thể nhanh hơn bao nhiêu trong điều kiện tối ưu. Tất nhiên là có phí bộ nhớ, độ trễ chỉ dẫn và các yếu tố khác liên quan; trên bộ xử lý Intel Ivy Bridge, thông báo SHA-512 nhanh hơn 1,54 lần và trên AMD Piledriver nó nhanh hơn 1,48 lần. Đối với các tin dữ liệu cần băm có độ dài nhỏ ít hơn 448 bit SHA-512 sẽ chậm hơn khoảng 1,25 lần.

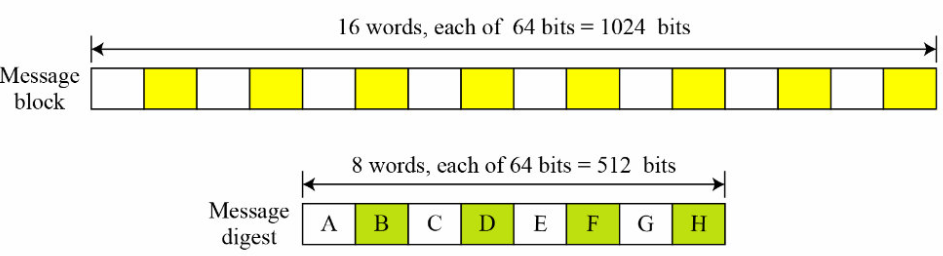
SHA-512 có tốc độ chỉ bằng 60% SHA-256 nhưng có một lợi thế đó là đôi khi chúng ta muốn một quá trình sinh khóa chậm để kéo dài khóa, điều này thường được sử dụng để giảm thiểu các cuộc tấn công BruceForce và các cuộc tấn công có thể dự đoán trước các khóa yếu như mật khẩu.

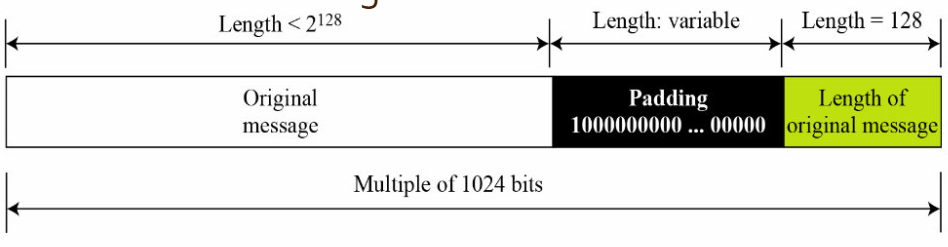
1. Processing of SHA-512\_Xử lý SHA-512

* thêm phần đệm và cố định 128 bit trường chiều dài
* chia thông điệp tăng cường thành khối
* sử dụng một từ 64-bit có nguồn gốc từ khối tin nhắn hiện tại
* sử dụng 8 hằng số dựa trên căn bậc hai của 8 số nguyên tố đầu tiên (2-19)
* cập nhật bộ đệm 512 bit
* sử dụng hằng số tròn dựa trên khối lập phương căn của 80 số nguyên tố đầu tiên (2-409)
* SHA-512 Xử lý một đĩa đơn

Hình. SHA-512 Xử lý một đĩa đơn khối 1024 bit

1. Message block and digest word\_Khối tin nhắn và tiêu hóa từ

* hoạt động trên các từ
* mỗi khối bao gồm mười sáu 64 bit (1024 bit) từ
* thông báo tóm tắt có tám bit 64 (512bit) các từ có tên A,B,C,D,E,F,G,H
* mở rộng 80 từ từ mười sáu 64bit từ

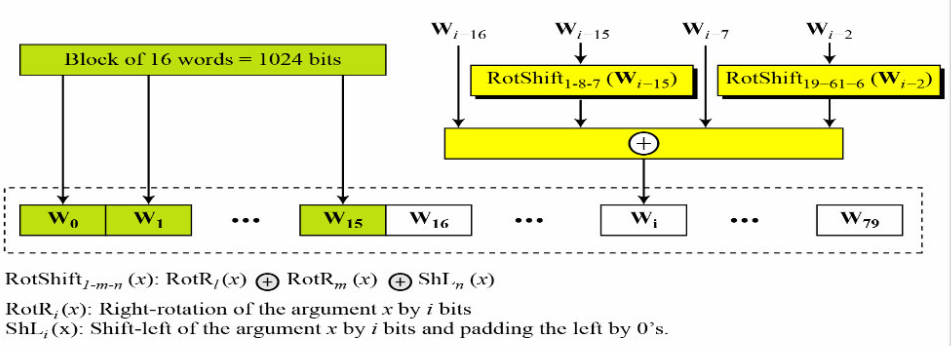
Hình. Một khối tin nhắn và tiêu hóa như lời nói

Hình. Trường đệm và trường độ dài

1. SHA-512 Giá trị ban đầu & Mở rộng từ

|  |  |  |  |
| --- | --- | --- | --- |
| Đệm | Giá trị (trong  thập lục phân) | Đệm 1 | Giá trị (trong  thập lục phân) |
| A0 | 6A09E667F3BCC908 | E0 | 510E527FADE682D1 |
| B0 | BB67AE8584CAA73B | F0 | 9B05688C2B3E6C1F |
| C0 | 3C6EF372FE94F82B | G0 | 1F83D9ABFB41BD6B |
| D0 | A54FF53A5F1D36F1 | H0 | 5BE0CD19137E2179 |

Bảng: Giá trị của các hằng số trong khởi tạo thông báo tóm tắt của SHA-512



Hình. Mở rộng từ trong SHA-512

1. Tính hằng số

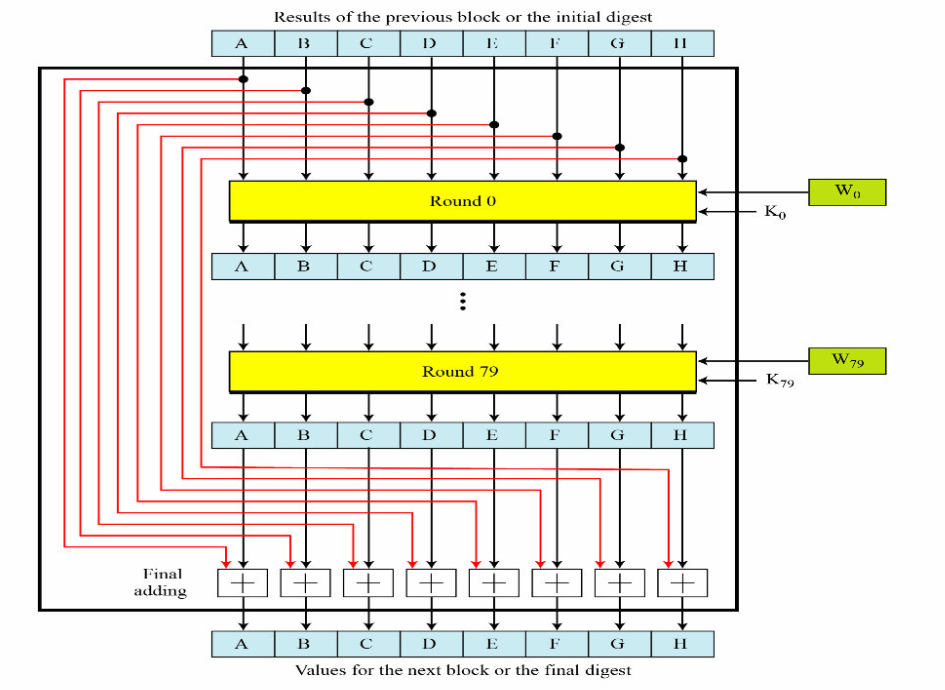
Ví dụ:

Số nguyên tố thứ 8 là 19, với căn bậc hai(19)1/2= 4.35889894354

Chuyển đổi số này

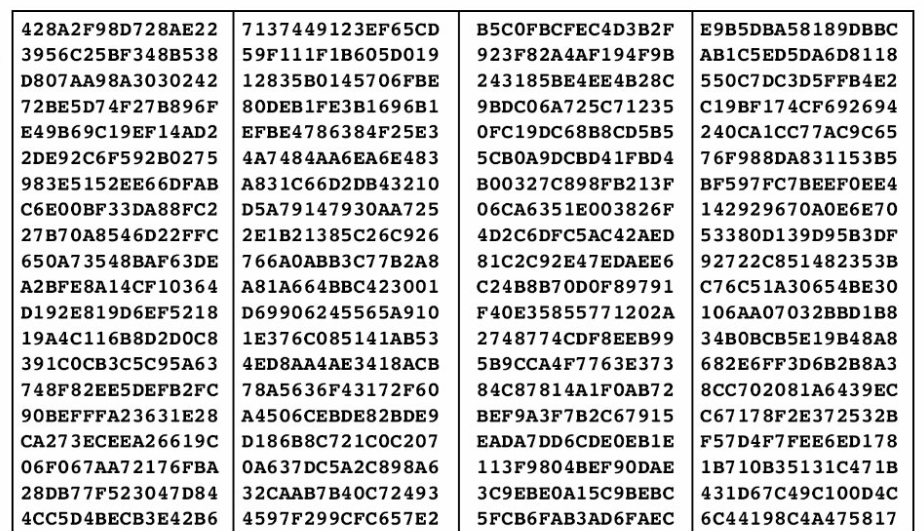
sang nhị phân chỉ với 64 bit trong phân số một phần, chúng tôi nhận được

1. Hàm nén SHA-512



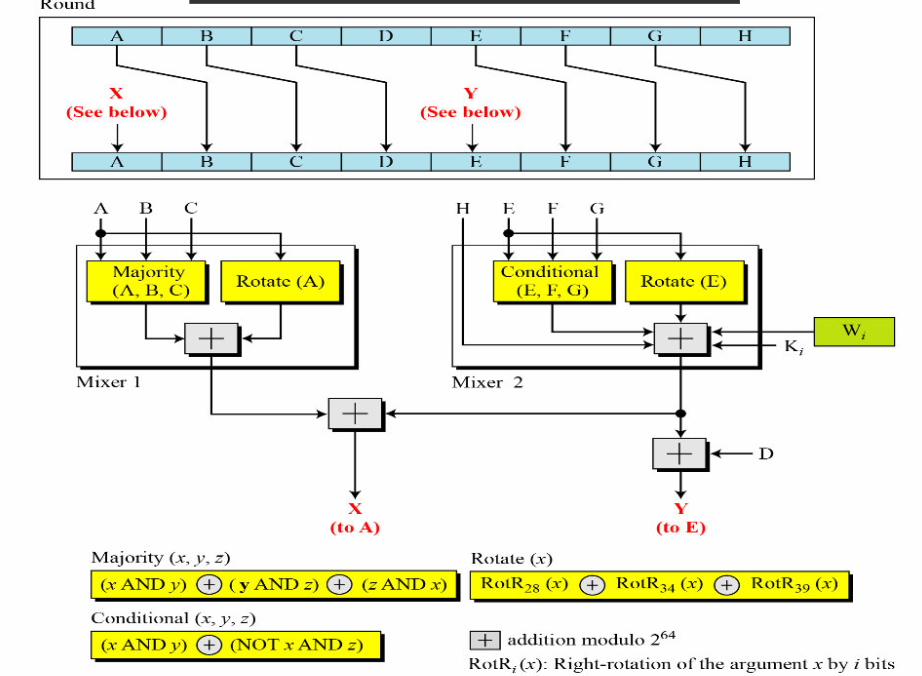
Hình. Chức năng nén trong SHA-512

1. SHA-512 Hằng số tròn (K)

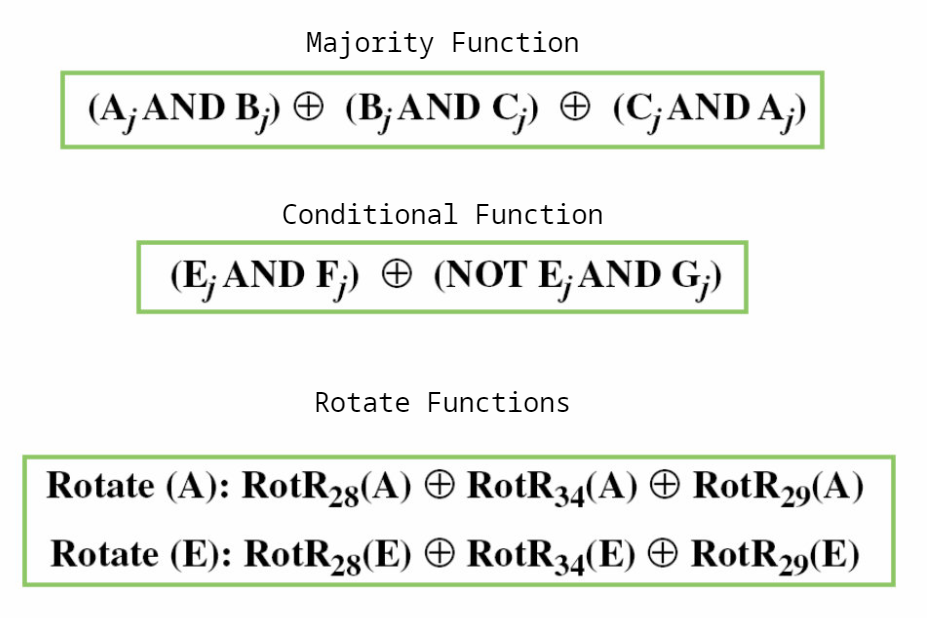


Hình: Danh sách các hằng số làm tròn được sử dụng trong SHA-512

1. Hàm vòng SHA-512



Hình. Cấu trúc của mỗi vòng trong SHA-512



1. Ví dụ sử dụng SHA-512\_1

Ký tự ASCII: “abc”, tương đương với ký tự sau Chuỗi nhị phân 24 bit:

01100001 01100010 01100011 = 616263 trong hệ thập lục phân

Độ dài ban đầu là 24 bit hoặc giá trị thập lục phân là 18. khối tin nhắn 1024 bit, theo hệ thập lục phân, là

6162638000000000 0000000000000000 0000000000000000

0000000000000000

0000000000000000 0000000000000000 0000000000000000

0000000000000000

0000000000000000 0000000000000000 0000000000000000

0000000000000000

0000000000000000 0000000000000000 0000000000000000

0000000000000018

W0 = 6162638000000000 W5 = 0000000000000000

W1 = 0000000000000000 W6 = 0000000000000000

W2 = 0000000000000000 W7 = 0000000000000000

W3 = 0000000000000000 W8 = 0000000000000000

W4 = 0000000000000000 W9 = 0000000000000000

Ví dụ sử dụng SHA-512\_2

Bảng sau đây cho thấy các giá trị ban đầu của các biến này và giá trị của chúng sau mỗi hai vòng đầu tiên.

|  |  |  |  |
| --- | --- | --- | --- |
| a | 6a09e667f3bcc908 | f6afceb8bcfcdd  f5 | 1320f8c9fb872cc0 |
| b | bb67ae8584caa73b | 6a09e667f3bcc9  08 | f6afceb8bcfcddf5 |
| c | 3c6ef372fe94f82b | bb67ae8584caa7  3b | 6a09e667f3bcc908 |
| D | a54ff53a5f1d36f1 | 3c6ef372fe94f8  2b | bb67ae8584caa73b |
| E | 510e527fade682d1 | 58cb02347ab51f  91 | c3d4ebfd48650ffa |
| F | b05688c2b3e6c1f | 510e527fade682  d1 | 58cb02347ab51f91 |
| G | 1f83d9abfb41bd6b | 9b05688c2b3e6c  1f | 510e527fade682d1 |
| h | 5be0cd19137e2179 | 1f83d9abfb41bd | 9b05688c2b3e6c1f |

Giá trị băm sau đó được tính như

H1,7 = 5be0cd19137e2179 + ceb9fc3691ce8326 = 2a9ac94fa54ca49f

H1,6 = 1f83d9abfb41bd6b + 25c96a7768fb2aa3 = 454d4423643ce80e

H1,5 = 9b05688c2b3e6c1f + 9bb4d39778c07f9e = 36ba3c23a3feebbd

H1,4 = 510e527fade682d1 + d08446aa79693ed7 = 2192992a274fc1a8

H1,3 = a54ff53a5f1d36f1 + 654ef9abec389ca9 = 0a9eeee64b55d39a

H1,2 = 3c6ef372fe94f82b + d67806db8b148677 = 12e6fa4e89a97ea2

H1,1 = bb67ae8584caa73b + 10d9c4c4295599f6 = cc417349ae204131

H1,0 = 6a09e667f3bcc908 + 73a54f399fa4b1b2 = ddaf35a193617aba

Thông báo tóm tắt 512-bit kết quả là

1. Ứng dụng SHA-512

* Được sử dụng như một phần của hệ thống để xác thực video lưu trữ từ quốc tế
* Tòa án hình sự của Rwandan diệt chủng.
* Được đề xuất sử dụng trong DNSSEC
* đang chuyển sang SHA-2 512-bit để bảo mật băm mật khẩu bằng Unix và Linux nhà cung cấp