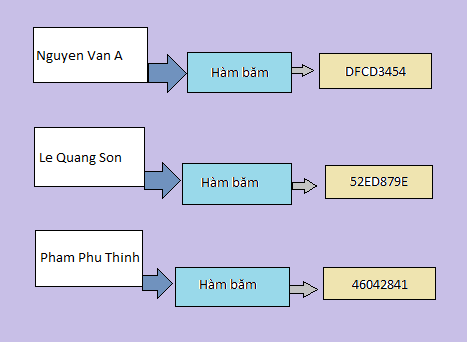
**HASH FUNCTION**

1. **Hash function.**

-Hash function (hàm băm): tạo ra giá trị băm cho các tương ứng với dữ liệu đầu vào.

-giá trị băm được xem như là một khóa để phân biệt giữa các dữ liệu đầu vào.

-Mục đích của hàm băm là từ một dữ liệu đầu vào (input) với dung lượng bất kỳ nó sẽ mã hóa dữ liệu này về một dữ liệu khác với dung lượng nhất định



-Tuy nhiên vẫn còn xảy ra hiện tượng trùng khóa khi sử dụng hàm băm.

-Hàm băm thường được dùng trong bảng băm.

-Bảng băm (hash table): là một loại cấu trúc dữ liệu mà mỗi phần tử trong bảng băm là một cặp (khóa, giá trị).

-Hàm băm (hash function): có thể thự hiện nhanh.

-Độ phức tạp của thuật toán là O(n).

-Hàm băm (hash function): dùng để xây dựng cấu trúc dữ liệu.

🡺

1. **Hàm băm mật mã (cryptographic hash functions).**

-Là một hàm băm có tính bảo mật, có thể sử dụng hàm băm mật mã trong bảo mật thông tin.

-Các hàm băm thông dụng nhất là MD5 và SHA.

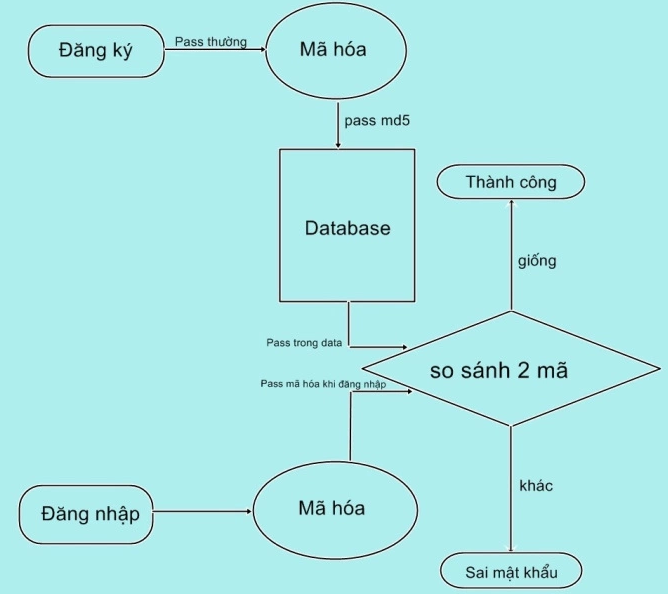
1. MD5:

-MD5 là hàm băm mật mã được sử dụng phổ biến với giá trị hash là 128bit. Được thiết kế bởi Ronald Rivest vào năm 1991.

-MD5 được dùng trong các ứng dụng bảo mật cũng như dùng để kiểm tra tính toàn vẹn của thông tin, lưu trữ mật khẩu.

-Giá trị sau khi băm qua MD5 là di nhất và không thể suy ngược lại giá trị ban đầu hay nói một cách khác là hàm băm MD5 không có phần giải mã.

-Ví dụ: Hệ thống sử dụng MD5 để băm mật khẩu của người dùng trước khi lưu vào database. Khi người dùng đăng nhập thì mật khẩu của người dùng nhập trên giao diện đăng nhập sẽ được băm và so sánh với mật khẩu trong database xem có hợp lệ hay không.



1. SHA.

-SHA là giải thuật băm an toàn. SHA là năm giải thuật được chấp nhận bởi FIPS dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi.

-Năm giải thuật SHA là:

* SHA-1 trả về kết quả 160 bit.
* SHA-224 trả về kết quả 224 bit.
* SHA-256 trả về kết quả 256 bit.
* SHA-384 trả về kết quả 384 bit.
* SHA-512 trả về kết quả 512 bit.
* SHA được phát triển bởi [cục an ninh quốc gia Mĩ](https://vi.wikipedia.org/wiki/C%C6%A1_quan_An_ninh_Qu%E1%BB%91c_gia_Hoa_K%E1%BB%B3" \o "Cơ quan An ninh Quốc gia Hoa Kỳ) (National Security Agency hay NSA) và được xuất bản thành chuẩn của chính phủ [Mĩ](https://vi.wikipedia.org/wiki/Hoa_K%E1%BB%B3" \o "Hoa Kỳ) bởi [viện công nghệ và chuẩn quốc gia Mĩ](https://vi.wikipedia.org/w/index.php?title=NIST&action=edit&redlink=1" \o "NIST (trang chưa được viết)) (National Institute of Standards and Technology hay NIST).
* SHA-224, SHA-256, SHA-384, SHA-512: được gọi chung là SHA-2.
* SHA-1 được sử dụng rộng rãi trong nhiều ứng dụng và giao thức an ninh khác nhau. SHA-1 được xem là giải thuật thay thế cho MD5.
* Hiện nay thì SHA-1 không còn được xem là an toàn nữa. Ba nhà mật mã học người [Trung Quốc](https://vi.wikipedia.org/wiki/Trung_Qu%E1%BB%91c" \o "Trung Quốc) đã phát triển thành công một giải thuật dùng để tìm được hai đoạn dữ liệu nhất định có cùng kết quả băm tạo ra bởi SHA-1.