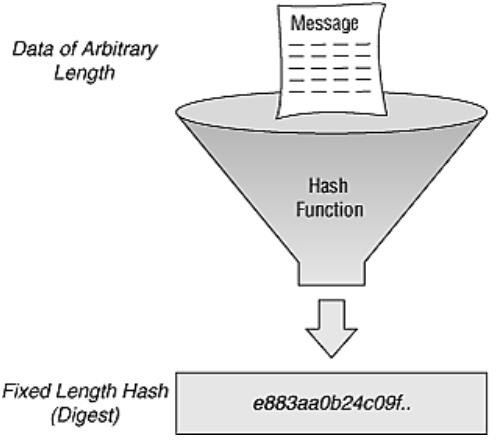
I.Kiến trúc về hàm băm

1.Định nghĩa

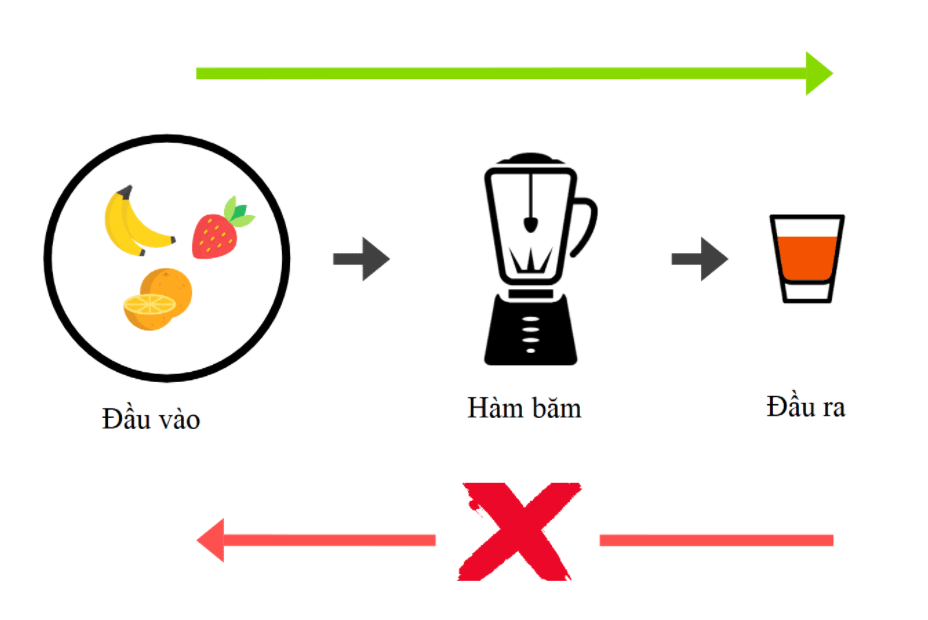
Hàm băm (hash function) là một hàm toán học h có tối thiểu 2 thuộc tính:

* Nén (Compression): h là một ánh xạ từ chuỗi đầu vào x có chiều dài bất kỳ sang một chuỗi đầu ra h(x) có chiều dài cố định n bit.
* Dễ tính toán (Ease of computation): cho trước hàm h và đầu vào x, việc tính toán h(x) là dễ dàng.[1]



2 .Tính chất cơ bản của hàm băm

* Tính một chiều:



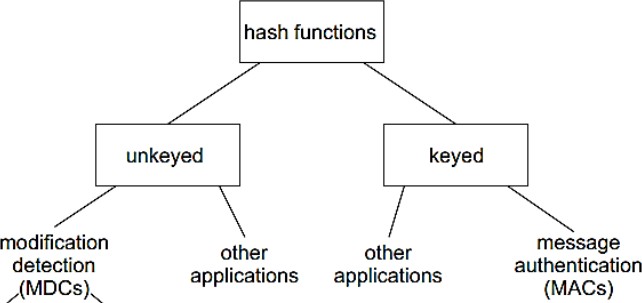
* Tính duy nhất:

**3.**Ngoài ra, với mục đích đảm bảo an toàn cho dữ liệu, các hàm băm mật mã phải có khả năng chịu được tất cả các loại tấn công mã hóa đã biết. Trong lý thuyết mật mã, mức độ an toàn của hàm băm mật mã đã được xác định bằng các thuộc tính sau:

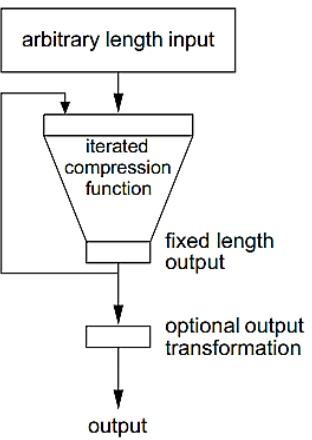
* **Tính kháng tiền ảnh thứ nhất**. Tính chất yêu cầu rằng với một giá trị băm h bất kỳ, sẽ khó tìm thấy bất kỳ thông điệp m nào sao cho h = hash (m). Khái niệm này có liên quan đến tính chất một chiều của hàm băm.
* **Tính kháng tiền ảnh thứ hai**. Với đầu vào m1, sẽ khó tìm được đầu vào m2 khác sao cho hash(m1) = hash (m2).
* **Tính kháng va chạm.** Rất khó để tìm thấy hai thông điệp khác nhau m1 và m2 sao cho hash (m1) = hash (m2). Một giá trị như vậy được gọi là va chạm của hàm băm mật mã.

4.Phân loại hàm băm theo khóa sử dụng

* Hàm băm không khóa (unkeyed): đầu vào chỉ là thông điệp
* Hàm băm có khóa (keyed): đầu vào gồm thông điệp và khóa



5.Mô hình xử lí dữ liệu



Thông điệp đầu vào với độ dài tùy ý (arbitrary length input) đi qua hàm nén lặp nhiều vòng 11 (iterated compression function) để tạo chuỗi đầu ra có kích thước cố định (fixed length output). Chuỗi này đi qua một khâu chuyển đổi định dạng tùy chọn (optional output transformation) để tạo ra chuỗi băm kết quả (output)