

The ideal cryptographic hash function has four main properties:

- It is easy to compute the hash value for any given message
- Dễ dàng tính toán giá trị băm cho bất kỳ thông điệp nào
- It is infeasible to generate a message that has a given hash
- Không thể tạo lại thông điệp từ một hàm băm đã cho
- It is infeasible to modify a message without changing the hash
- Không thể tùy chỉnh 1 thông điệp mà không làm thay đổi hàm băm
- It is infeasible to find two different messages with the same hash.
- Không thể tìm được 2 thông điệp khác nhau có cùng hàm băm