# **Đinh Văn Hiếu – 20221201**

# Bài 1: Nhập 2 dòng văn bản’

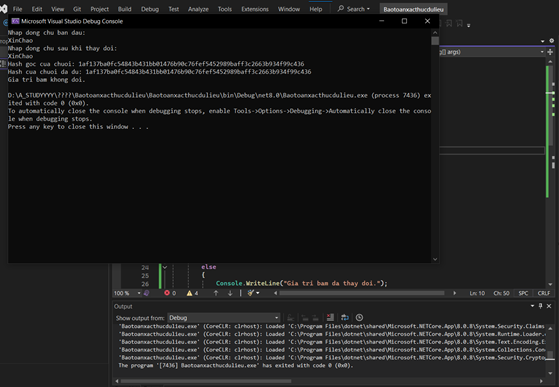
## Trường hợp 1:

**Văn bản 1: XinChao**

**Văn Bản 2: XinChao**

* **Hash goc cua chuoi:** 1af137ba0fc54843b431bb01476b90c76fef5452989baff3c2663b934f99c436
* **Hash cua chuoi da thay doi:** 1af137ba0fc54843b431bb01476b90c76fef5452989baff3c2663b934f99c436

**Giá trị băm không thay đổi.**



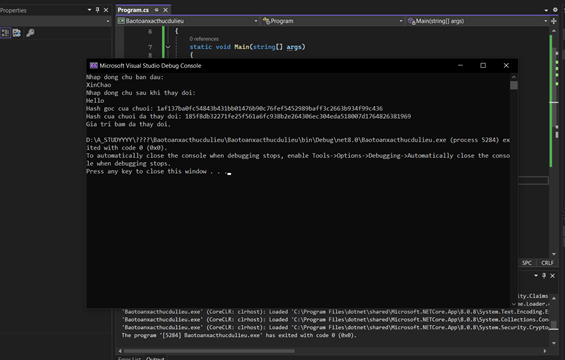
## Trường hợp 2:

**Văn bản 1: XinChao**

**Văn Bản sau khi thay đổi: Hello**

* **Hash goc cua chuoi:** 1af137ba0fc54843b431bb01476b90c76fef5452989baff3c2663b934f99c436
* **Hash cua chuoi da thay doi:** 185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

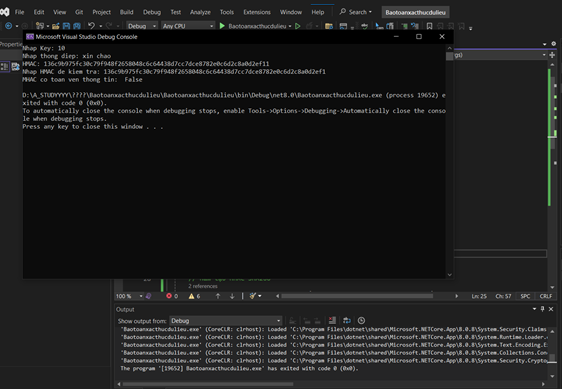
**Giá trị băm đã thay đổi.**



# Bài 2:

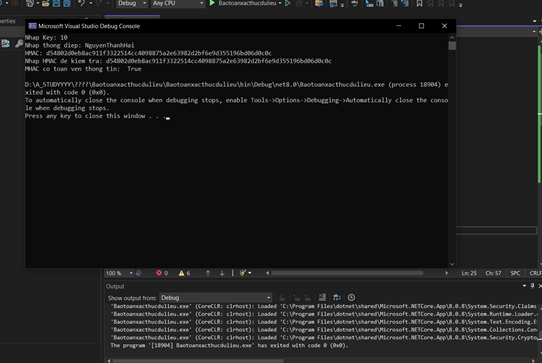
## Trường hợp 1:

* Nhập Key: 10
* Nhập thông điệp: xin chao
* HMAC: 136c9b975fc30c79f948f2658048c6c64438d7cc7dce8782e0c6d2c8a0d2ef11
* Nhap HMAC de kiem tra: 136c9b975fc30c79f948f2658048c6c64438d7cc7dce8782e0c6d2c8a0d2ef1
* (MHAC thiếu 1 số 1 ở cuối chuỗi)
* MHAC không toan vẹn thông tin.

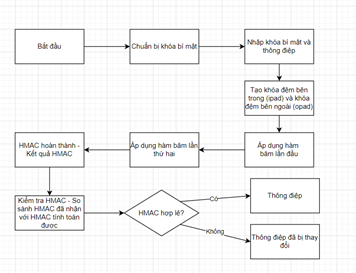


## Trường hợp 2:

* Nhap Key: 10
* Nhap thong diep: NguyenThanhHai
* HMAC: d54802d0eb8ac911f3322514cc4098875a2e63982d2bf6e9d355196bd06d0c0c
* Nhap HMAC de kiem tra: d54802d0eb8ac911f3322514cc4098875a2e63982d2bf6e9d355196bd06d0c0c
* MHAC có toan vẹn thông tin .



* Sơ đồ thuật toán:



**Mô tả thuật toán:**

 **Bắt đầu**: Thuật toán bắt đầu bằng cách yêu cầu người dùng nhập vào thông điệp và khóa bí mật.

 **Chuẩn bị khóa bí mật**:

* Nếu khóa bí mật dài hơn độ dài block của hàm băm (ví dụ SHA-256 có block size là 64 byte), nó sẽ được băm lại để có độ dài phù hợp.
* Nếu khóa bí mật ngắn hơn độ dài block, nó sẽ được bổ sung thêm các byte đệm 0x00 để đạt đủ độ dài.

 **Tạo khóa đệm**:

* Khóa bí mật được XOR (phép toán OR độc quyền) với hai hằng số:
  + ipad (inner padding) là một dãy các byte có giá trị 0x36.
  + opad (outer padding) là một dãy các byte có giá trị 0x5c.

 **Hàm băm lần đầu**:

* Áp dụng hàm băm (SHA-256) lên kết quả của key ⊕ ipad nối với thông điệp.

 **Hàm băm lần thứ hai**:

* Áp dụng hàm băm (SHA-256) lần nữa lên kết quả của key ⊕ opad nối với kết quả băm lần đầu.

 **Kết quả HMAC**:

* Kết quả cuối cùng chính là giá trị HMAC.

 **Kiểm tra HMAC**:

* Khi kiểm tra HMAC, chúng ta tính toán HMAC của thông điệp dựa trên khóa bí mật và so sánh với giá trị HMAC đã được cung cấp trước đó.

 **Kết luận**:

* Nếu HMAC tính toán khớp với HMAC cung cấp, thì thông điệp chưa bị thay đổi, đảm bảo tính toàn vẹn và xác thực.
* Nếu HMAC không khớp, thông điệp đã bị thay đổi hoặc HMAC không đúng, báo hiệu thông điệp không an toàn.

# Bài 3:

