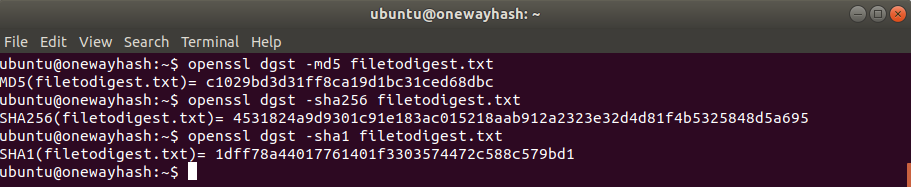
**BÀI 3. TẠO CHUỖI BĂM SỬ DỤNG OPENSSL**

1. Tạo giá trị hàm băm và MAC

Cú pháp: openssl dgst dgsttype filename

Lần lượt thay thế dgsttype bằng một thuật toán hàm băm một chiều cụ thể: -md5, -sha1, -sha256, vv. Và thay thế filename bằng filetodigest.txt. Ta có kết quả như sau

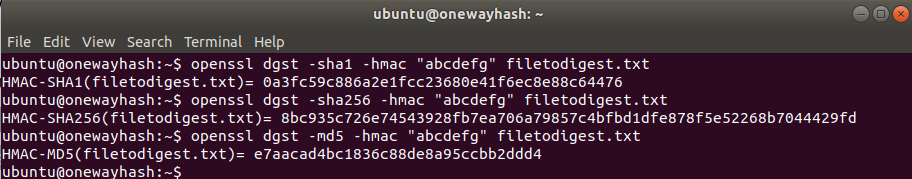
****

1. Keyed hash và HMAC

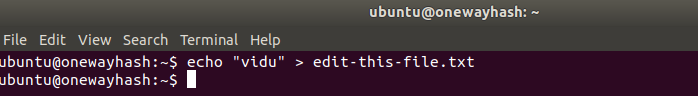
Tạo ra một giá trị băm theo khóa cho một tệp tin sử dụng thuật toán HMAC-MD5.

openssl dgst dgsttype -hmac "abcdefg" filename

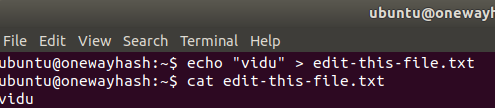
Lần lượt thay thế dgsttype bằng một thuật toán hàm băm một chiều cụ thể: -md5, -sha1, -sha256, vv. Và thay thế filename bằng filetodigest.txt. Ta có kết quả như sau



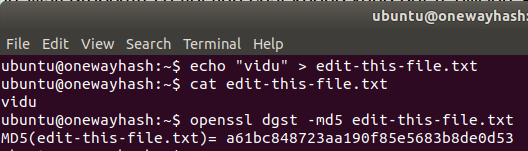
1. Tính ngẫu nhiên hàm băm một chiều
2. Tạo một tệp tin văn bản có tên "edit-this-file.txt" với bất kỳ độ dài nào, với nội dung là “vidu”



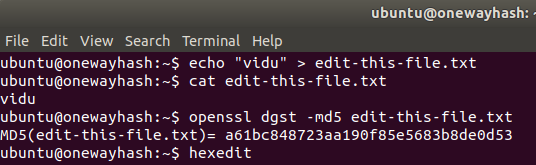
Đọc file này



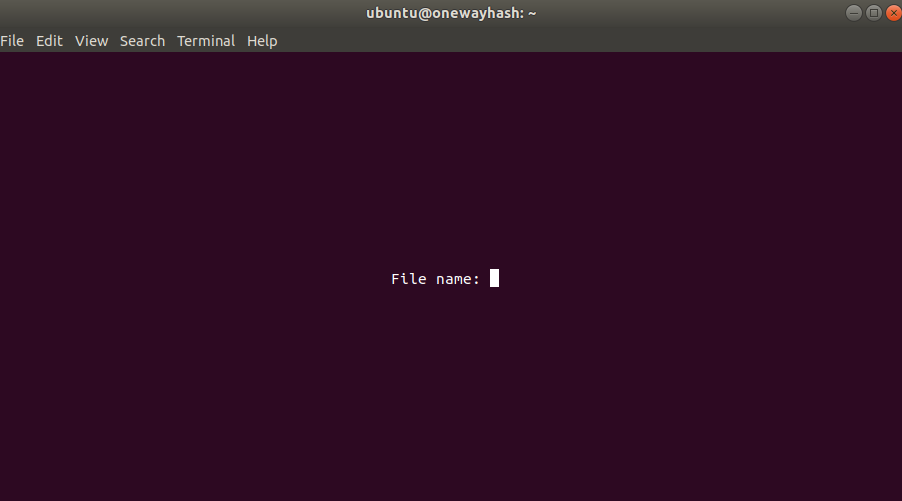
1. Tạo giá trị băm H1 cho tệp tin này bằng cách sử dụng một thuật toán băm cụ thể.



1. Đảo 1 bit trong tập tin này, sử dụng hexedit



Nhấn enter, màn hình yêu cầu nhập tên file như sau

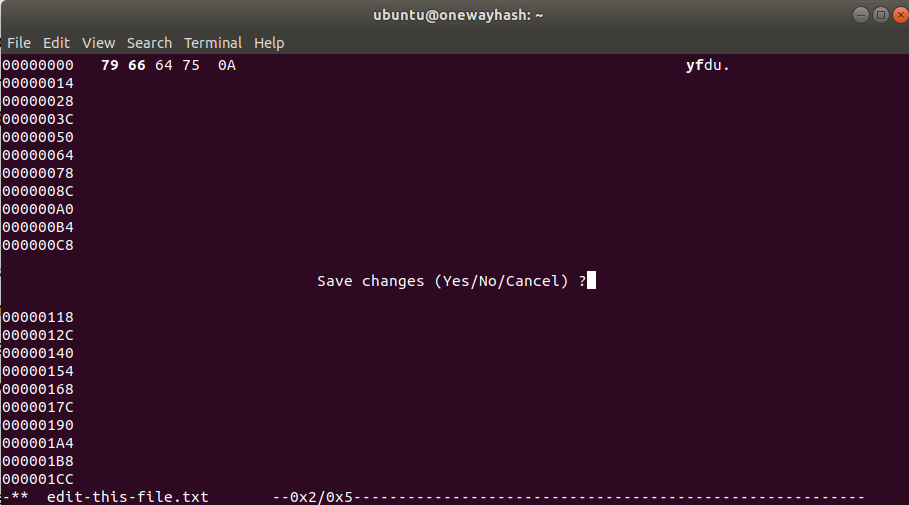


Ta nhập tên file là edit-this-file.txt rồi enter, sẽ có kết quả sau



Đổi: 76 69 thành 7**9** 6**6**

Ấn Ctrl X



Chọn Yes để lưu ra ngoài

1. Tạo giá trị hàm băm cho tệp tin mới

