**LAB 7**

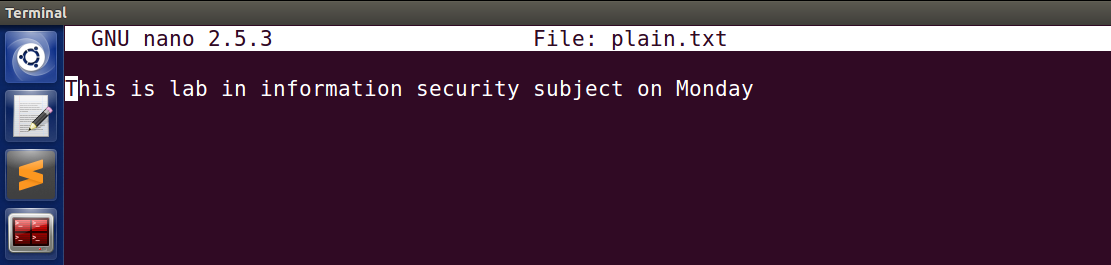
**Sinh viên thực hiện: Nguyễn Văn Thắng 17110230**

**Nguyễn Văn Hà 17110130**

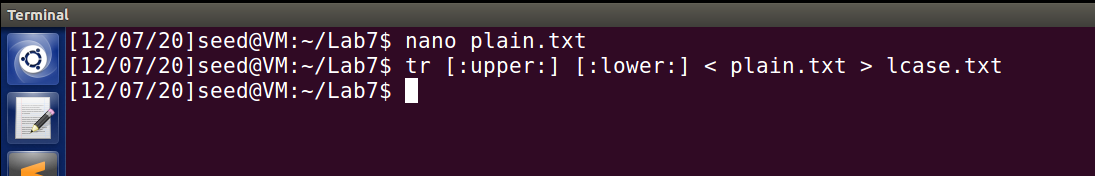
**Lab A–Breaking traditional substitution cipher & Exploring the MD5 collisions**

1. **Generating monoalphabetic substitution ciphertext with linux tr**

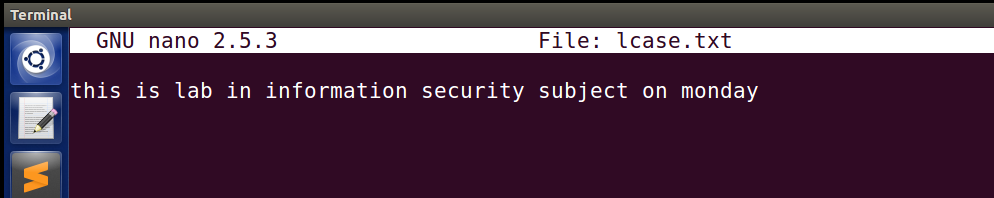
* Plain.txt



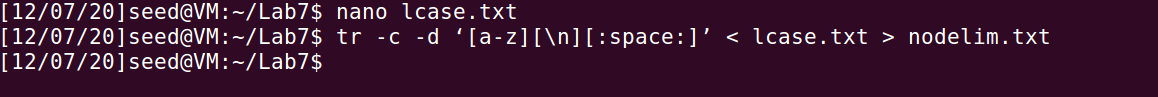
* Create lcase.txt (convert all letters to lowercase letters)



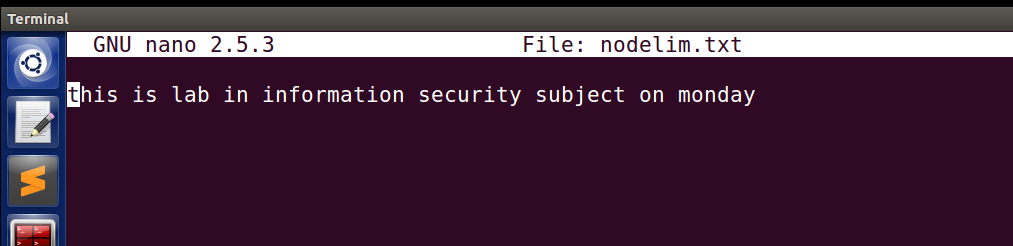
* Content file lcase.txt



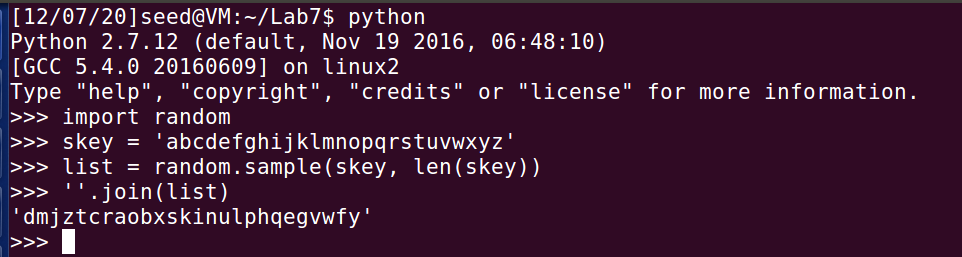
* Create file nodelim.txt (Remove delimiters and numbers from source files while preserving spaces.)



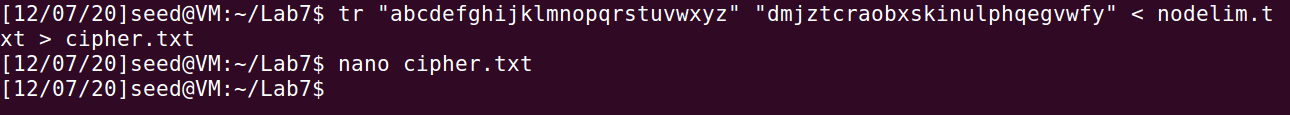
* Content file nodelim.txt



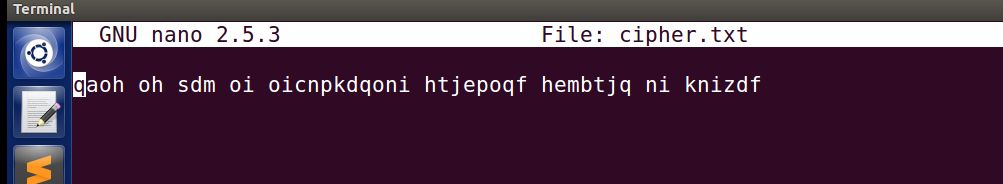
* Generate key



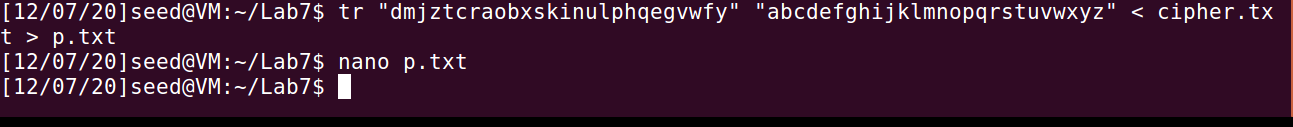
* Encrypt nodelim.txt



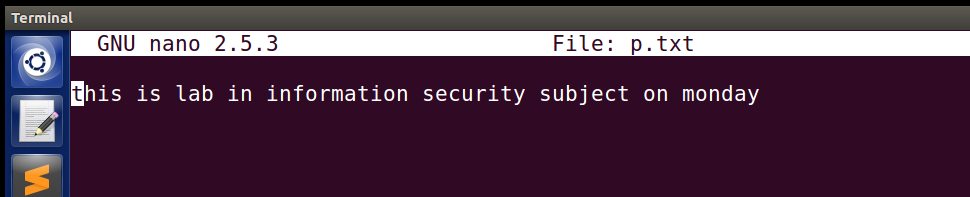
* Cipher.txt



* Encrypt

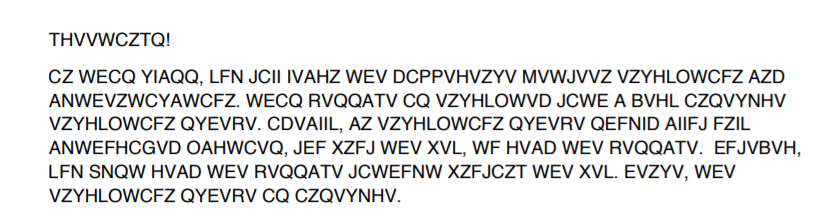


* Result

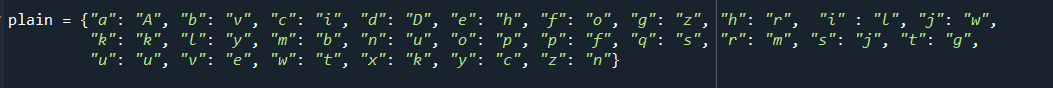


1. **Breaking the Substitution Cipher.**

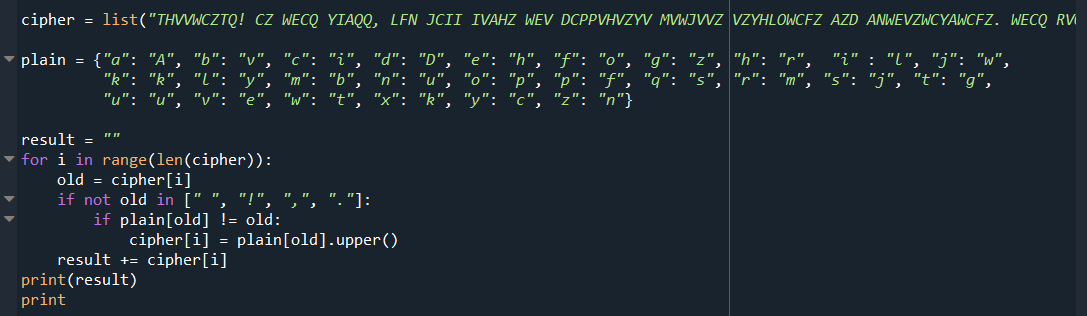
* Cipher:



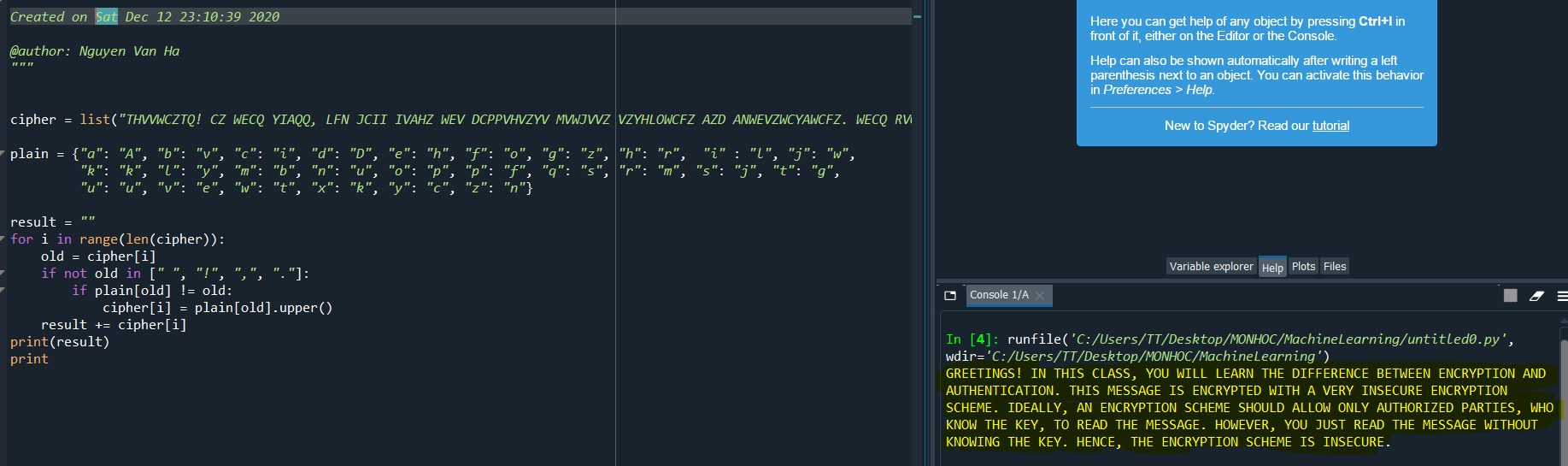
* Plain



* Code

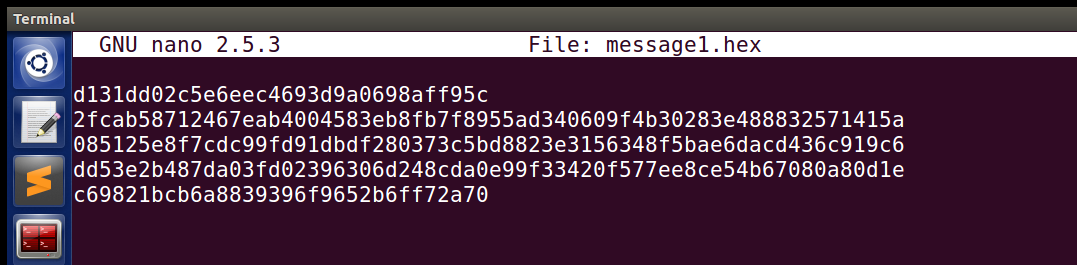


* Result

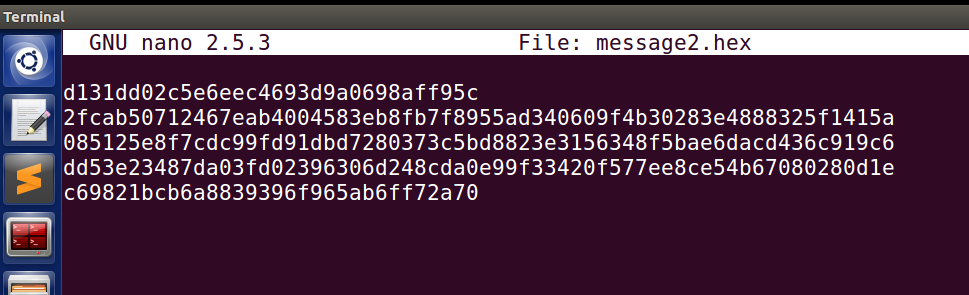


1. **Breaking the Vigenere Cipher**
2. **MD5 Collisions**

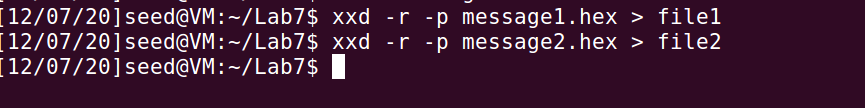
* File message1.hex



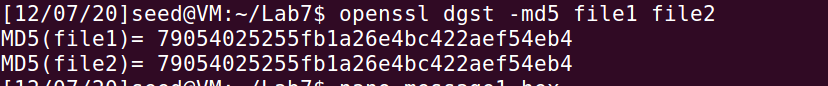
* File message2.hex



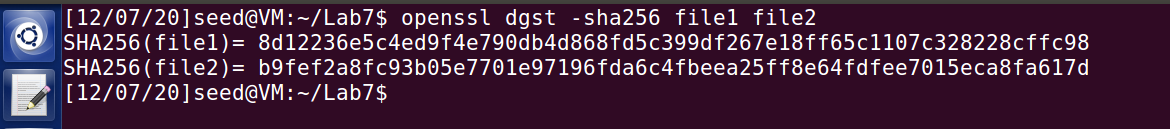
* Convert 2 file hex to binary file



* Verify that they’re the same with MD5



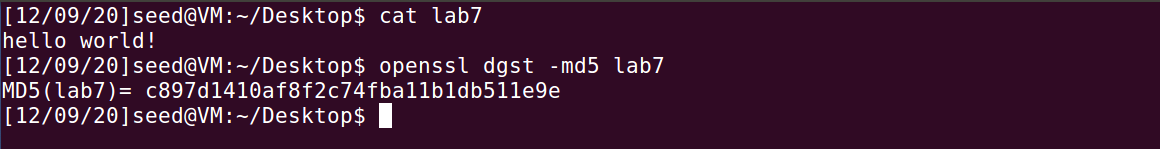
* Verify that they’re different with SHA-256



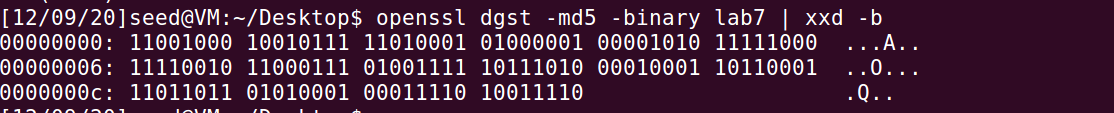
**Lab B: Crypto-Lab: – Exploring Collision-Resistance, Pre-Image Resistance and MACs**

**Task 1: Generating Message Digest and MAC**

* Sử dụng câu lệnh openssl dgst để mã hóa tệp theo thuật toán md5
* Mã hex



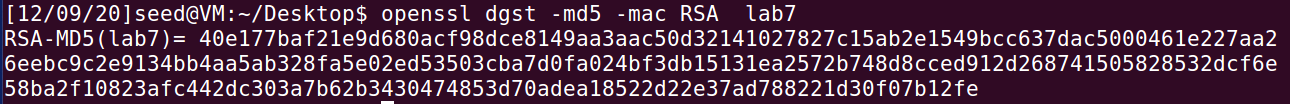
* Mã nhị phân



* Mã hóa với mac có key là password123 bằng thuật toán md5



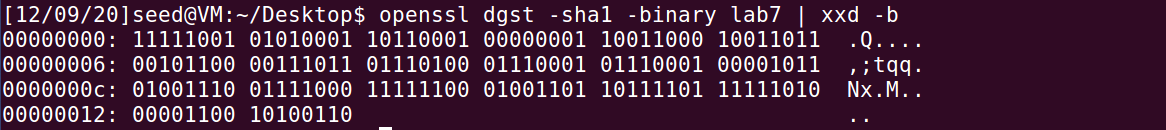
* Mã hóa với mac không cần key với thuật toán md5



* Sha1
* Mã hex



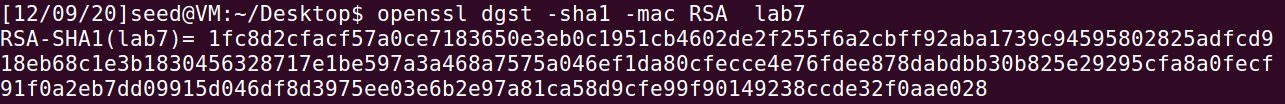
* Mã nhị phân



* Mã hóa với mac có key là password123 bằng thuật toán sha1 dưới dạng mã hex



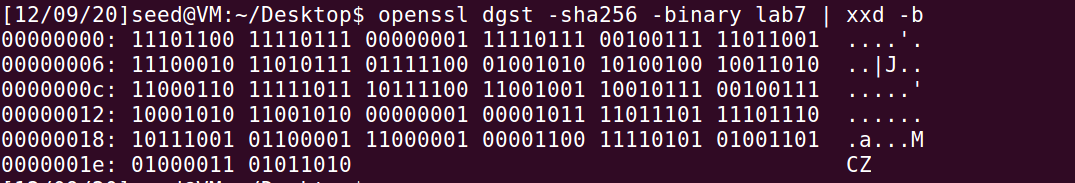
* Mã hóa với mac không cần key với thuật toán sha1 dưới dạng mã hex



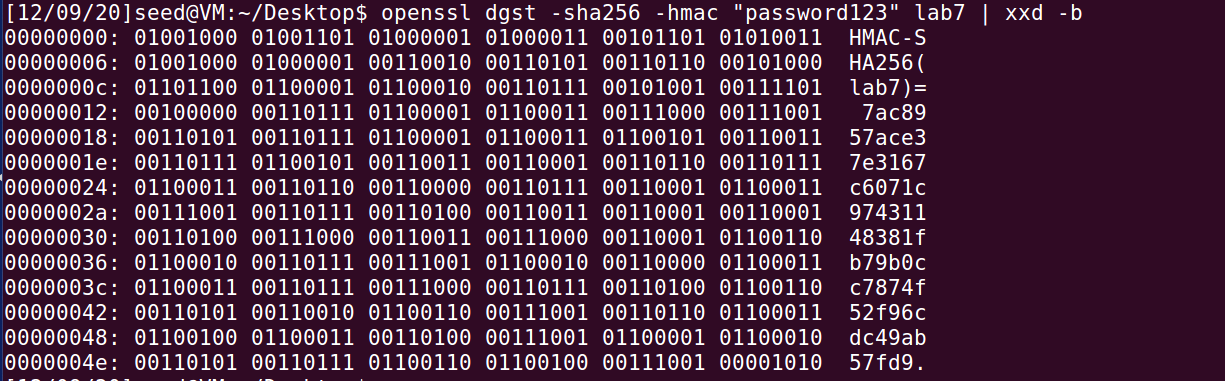
* Sha256
* Mã hex



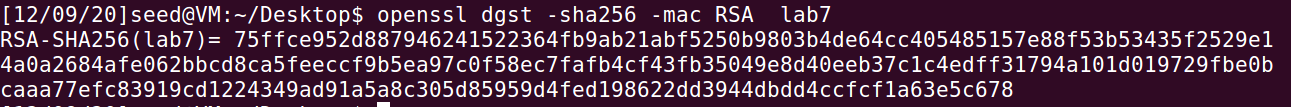
* Mã nhị phân



* Mã hóa với mac có key là password123 bằng thuật toán sha256 dưới dạng mã nhị phân



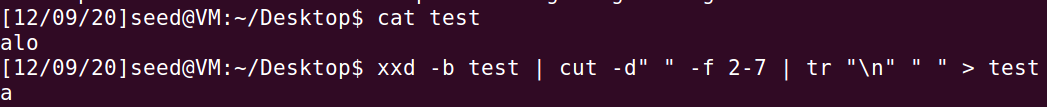
* Mã hóa với mac không cần key với thuật toán sha1 dưới dạng mã hex

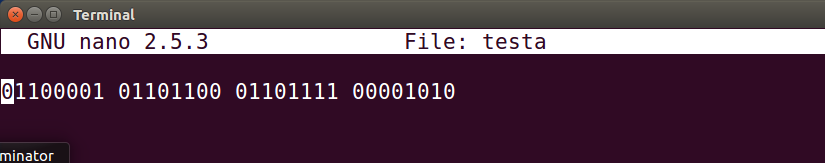


**Tast3: The Randomness of a Hash**

1. **Create a text file of any length**.

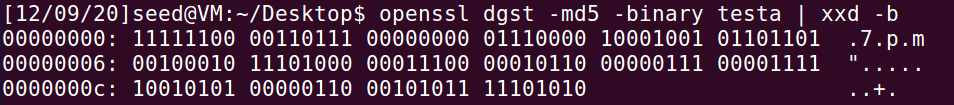
* Sau khi tạo 1 file có độ dài bất kỳ thì dịch file đó ra mã nhị phân với câu lệnh như sau:



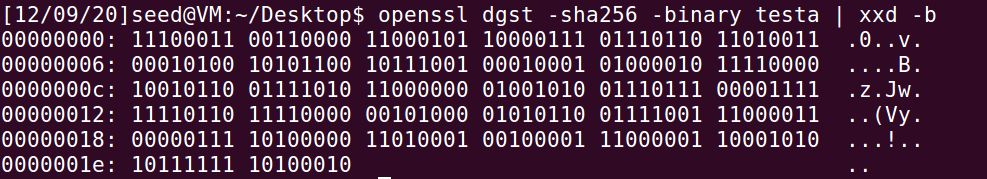


1. **Generate the hash value H1 for this file using a specific hash algorithm**.

* Sử dụng câu lệnh openssl dgst để tiến hành mã hóa file đã tạo ở câu a và thu được kết quả như sau:
* Md5

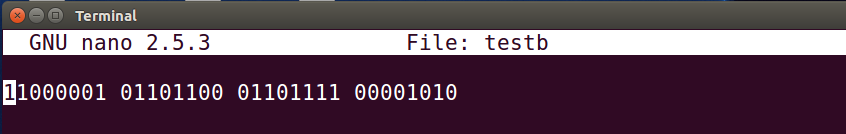


* Sha256



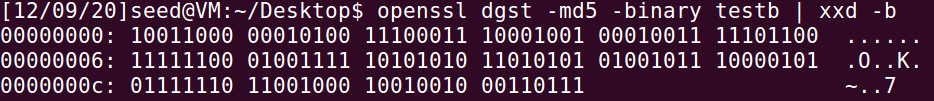
1. **Flip one bit of the input file. You can achieve this modification using Bless**.

* Sau khi đảo bit thì ta được file kết quả như sau:

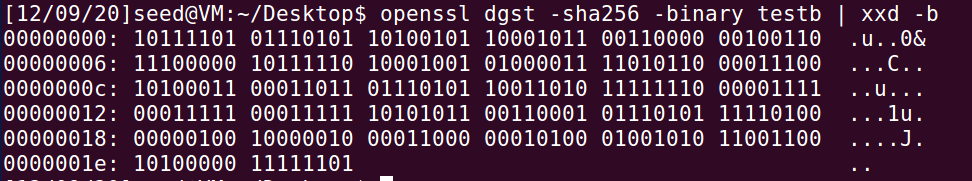


1. **Generate the hash value H2 for the modified file**.

* Sử dụng câu lệnh openssl dgst để mã hóa file sau khi đảo bit ta được kết quả như sau:
* Md5



* Sha256



1. **Observe whether H1 and H2 are similar or not. Write a short program to count how many bits are different between H1 and H2**.

* Theo như quan sát kết quả ở câu b và d thì ta có thể thấy được khi đảo bit ở file đầu vào thì dẫn đến sự thay đổi của H2 và khác với H1.