BÀI THỰC HÀNH SỐ ????

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: Lương Hữu Phú Lợi**

**MSSV: 1911545**

**Nhóm: L02**

**Phần 1. Hệ mã bất đối xứng RSA**

**Câu 1.** Cho biết vai trò của the public và private key trong hệ mã khoá công khai với ứng dụng mã hoá?

- **Public key:** là khóa mà ai cũng biết bằng do người nhận public ra ngoài. Thường được dùng cho việc mã hóa những thông tin mà chỉ người có private key mới giải mã được.

- **Private key:** là khóa mà chỉ duy nhất mà người nhận mới biết. Thường dùng để mã hóa chữ kí số và chỉ những người có public key tương ứng mới giải mã được.

**Câu 2.** Thực hiện tính toán: mã hoá và giải mã thông điệp sử dụng giải thuật RSA cho các câu bên dưới:

1. p=3;q=11,e=7;M=5
2. p=5;q=11,e=3;M=9
3. p=7;q=11,e=17;M=8
4. p=11;q=13,e=11;M=7
5. p=17;q=31,e=7;M=2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | p=3;q=11 | p=5;q=11 | p=7;q=11 | p=11;q=13 | p=17;q=31 |
| n = p\*q | 33 | 55 | 77 | 143 | 527 |
| ø(n)=(p-1)\*(q-1) | 20 | 40 | 60 | 120 | 480 |
| e = | 7 | 3 | 17 | 11 | 7 |
| d = (d\*e mod ø = 1 ) | 3 | 27 | 53 | 11 | 343 |
| Public key {n,e} | 33 ,7 | 55, 3 | 77,17 | 143,11 | 527,7 |
| Private key {p,q,d) | 3, 11, 33 | 5, 11, 27 | 7,11,53 | 11,13,11 | 17,31,343 |
| Cipher = (plaintext)^e mod n | 57 mod 33 = 14 | 93 mod 55 = 14 | 817 mod 77 = 57 | 711 mod 143 = 106 | 27 mod 527 = 128 |
| Plaintext = (ciphertext)^d mod n | 143 mod 33 = 5 | 1427 mod 55 = 9 | 5753 mod 77 = 8 | 10611 mod 143 = 7 | 128343 mod 527 = 2 |

**Câu 3.** Giả sử trong hệ mã khoá công khai sử dụng RSA, bạn biết được một ciphertext C = 10 được gởi đến một người có public key là e = 5, n = 35.

Chúng ta có thể sử dụng được các thông tin như trên để giải mã được thông điệp gốc (M) được không, nêu từng bước thực hiện và giải thích?

Publickey: e = 5 và n = 35

=> p = 7 và q = 5

ø = 6\*4 = 24

d = 5 (bởi vì 5\*5 mod 24 =1)

Vậy: M = (ciphertextd) mod m = 10^5 mod 35 = 5

**Câu 4.** Trong ứng dụng với hệ mã khoá công khai sử dụng RSA, chúng ta biết được một thành viên đang dùng public key là e = 31, n = 3599. Chúng ta có thể tìm được private key của thành viên nói trên được hay không, nêu từng bước thực hiện và giải thích?

Gợi ý: Cố gắng thử sai để tìm lại 2 số nguyên tố p và q từ n, sử dụng thuật toán Euclid mở rộng để tìm giá trị d

Publickey: e = 31 và m = 3599

Ta chọn được: p = 59 và q = 61

Nên:

- n = 60\*58 = 3480

- d = 3031

Vậy private key là: p = 59, q = 61 và d = 3031

**Phần 2. Hàm băm (Hash function)**

**Câu 1.** Hàm một chiều (one-way function) là gì?

One-way function là : hàm ánh xạ từ một miền giá trị thành một tập giá trị và phải thỏa mãn:

* Mọi giá trị của hàm đều có một giá trị nghịch đảo duy nhất.
* Hàm được tính một cách rất dễ dàng nhưng tính nghịch đảo lại rất khó khăn.

- Ngoài ra hàm One-way function còn có Trapdoor one-way function.

- Trapdoor one-way function là một kiểu của one-way function có chứa 1 loại *“back door”*. Như ta đã biết, hàm one-way function tính được dễ dàng nhưng tính giá trị nghịch đảo thì lại rất khó. Tuy nhiên nếu có thêm 1 số thông tin bí mật bổ sung thì cũng dễ dàng để tính hàm nghịch đảo đó.

**Câu 2.** Cho một ví dụ để minh hoạ việc sử dụng hàm băm có thể giúp kiểm tra tính toàn vẹn của thông điệp.

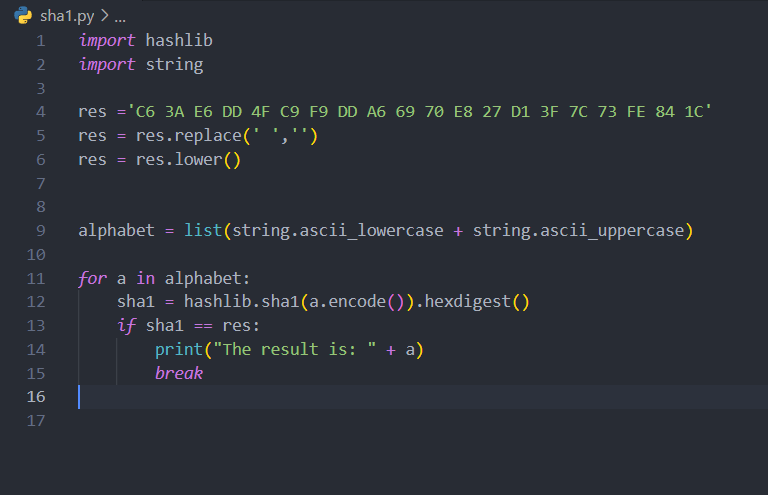
Gợi ý: mã hoá thông điệp, tạo ra thay đổi trên ciphertext và sử dụng hàm băm để kiểm tra thông điệp được giải mã có thay đổi so với thông điệp gốc ban đầu.

Khi ta tải file với IDM (Internet Download Manager) thì IDM sẽ tạo 1 file quản lý tính toàn vẹn của dữ liệu cần tải xuống, sau đó là các file hash là các phần dc IDM phân thành các cụm nhỏ để tải song song, đảm bảo tốc độ tải nhanh hơn và hạn chế bị mất dữ liệu hơn

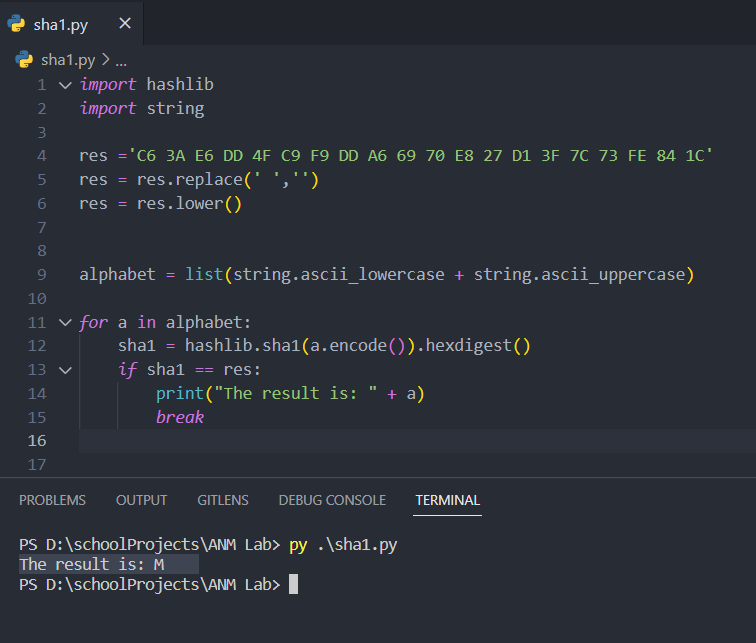
**Câu 3.** Hàm băm H(·) là hàm có chức năng chuyển thông điệp có kích thước bất kì bất kỳ về kích thước cố định:

1. Xem xét giá trị hash được tạo ra bằng cách áp dụng giải thuật hash SHA-1 trên một ký tự trong bảng chữ cái tiếng Anh: **C6 3A E6 DD 4F C9 F9 DD A6 69 70 E8 27 D1 3F 7C 73 FE 84 1C**. Hãy tìm ký tự chữ cái tiếng anh được sử dụng và mô tả cách làm? (dùng công cụ CrypTool)

Trong ứng dụng CrypTool, ta chọn **Indiv. Procedures” 🡪 “Hash” 🡪 “sha 1”** để has thông tin ta nhập ở bảng txt. Tuy nhien6CrypTool chỉ hash được 1 file txt cho 1 lần mà để thay thế hết bảng chữ cái thì ta sẽ mất 54 lần -> mất thời gian.

Vì vậy em chọn dùng python để tăng tốc độ xử lý, em dùng Python với đoạn code như sau 

Đầu tiên xử lý kết quả để lấy được chioi64 viết thường. Sau đó tạo danh sách các chữ cái từ a-z và A-Z là alphabet. Cho chạy hash từng thành phần trong alphabet để so sánh với kết quả đã cho. Khi tìm được kết quả thì dừng



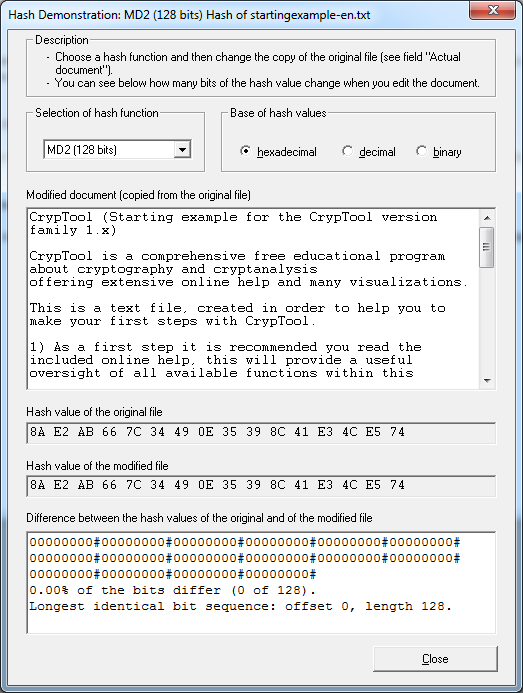
Vậy kết quả là chữ **M**

1. Giả sử bạn đã tìm ra được ký tự ở câu a, như vậy có thể kết luận hàm hash SHA-1 **không thoả mãn tính chất một chiều (one-way)** được hay không, giải thích câu trả lời?

Thông điệp chỉ chứa 1 bảng mã trong chữ cái tiếng anh. Nếu không có thông tin về input. Thì việc tìm ra input để vét cạn toàn bộ tổ hợp input có thể. Chúng ta có thể sử dụng bảng rainbow để giải mã nhưng nếu số lượng tổ hợp cực kì lớn thì điều này là không thể. Mà bảng rainbow lại phải cần số lượng lớn và nhiều thông tin của input. Do đó để dịch được ngược mã là thấp nên hàm băm SHA1 vẫn đảm bảo tính 1 chiều

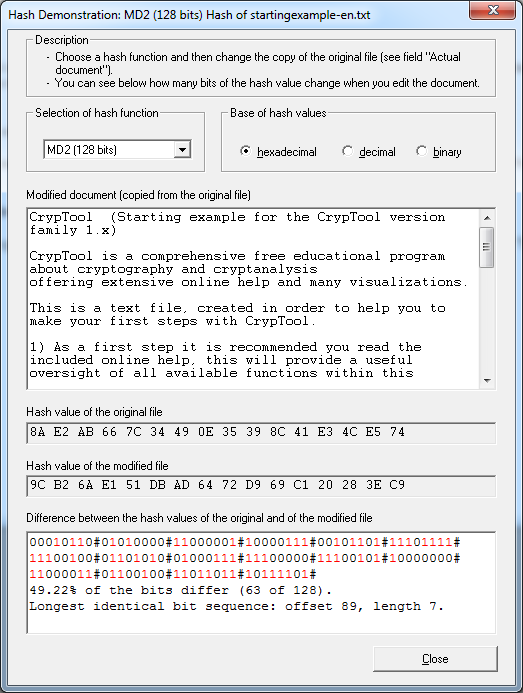
**Câu 4.** Sử dụng công cụ CrypTool để thực hành tính toán giá trị hash trên thông điệp bất kỳ

Bước 1. Vào menu “**Indiv. Procedures” 🡪 “Hash” 🡪 “Hash Demonstration**”.



Bước 2. Chọn giải thuật hash MD2 ở mục **Selection of hash function**

Bước 3. Thêm một ký tự khoảng cách trắng ở sau từ khoá **CrypTool**, chúng ta thấy giá trị hash đã thay đổi đáng kể chỉ với một thay đổi nhỏ trong thông điệp (khác biệt 63/128 bit – 49.22%) so với giá trị hash ban đầu. Một hàm băm tốt sẽ phản ứng rất nhạy đối với 1 thay đổi nhỏ trong plaintext.

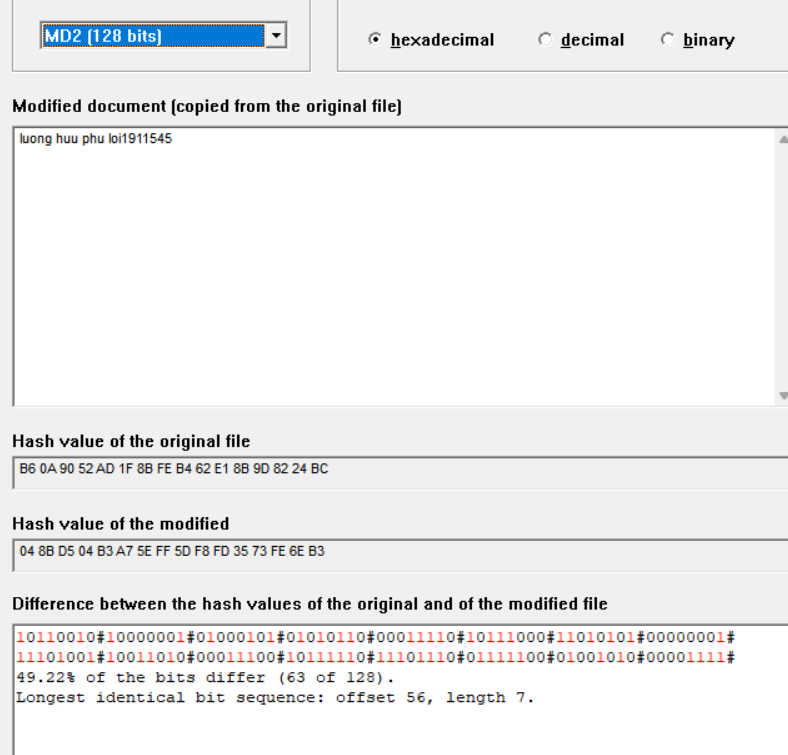


Bước 4. Thực hiện lại bước 3 cho các giải thuật hash khác và đánh giá giá trị hash nhận được với giá trị hash ban đầu.

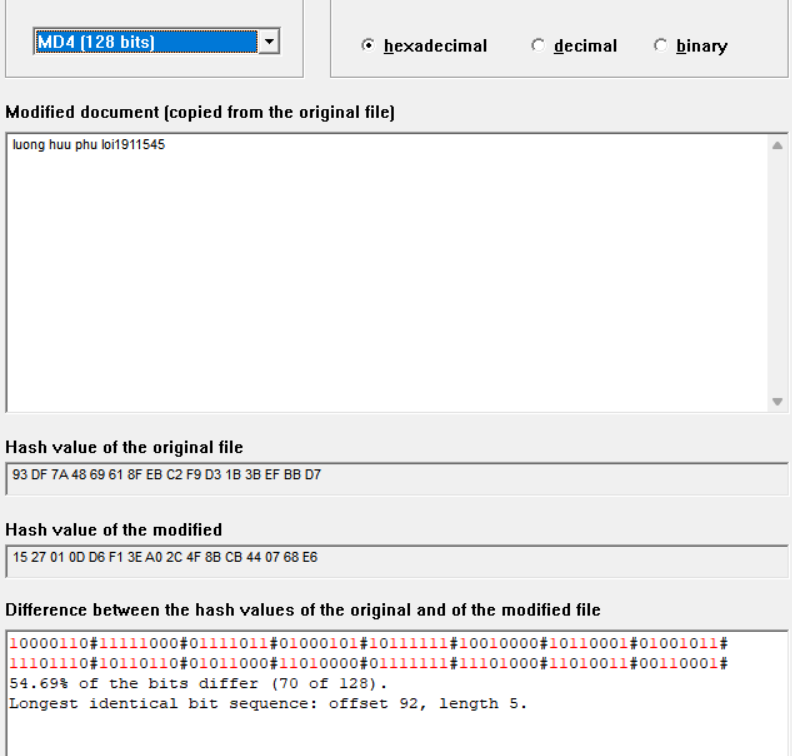
- Sử dụng đoạn plain text: “luong huu phu loi 1911545”

- Sau đó thay đổi khoảng trắng giữa loi và 1911545 ta có plain text “luong huu phu loi1911545”

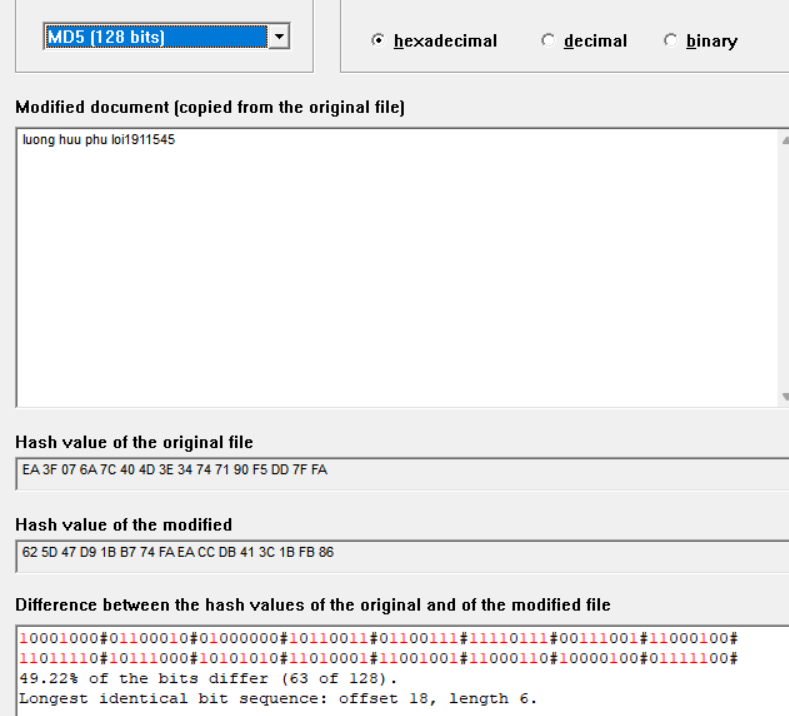
**MD2**



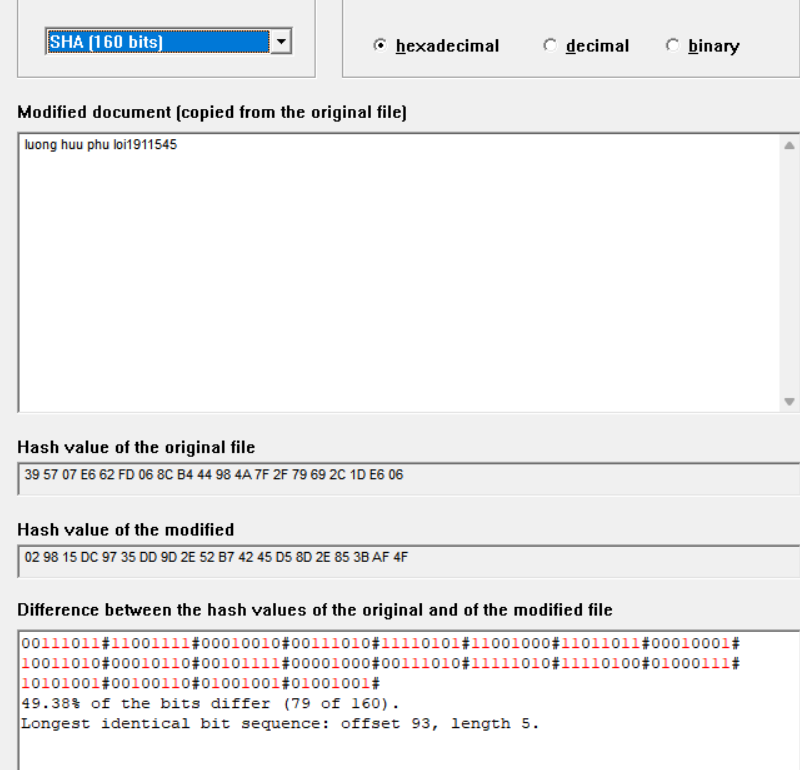
**MD4**



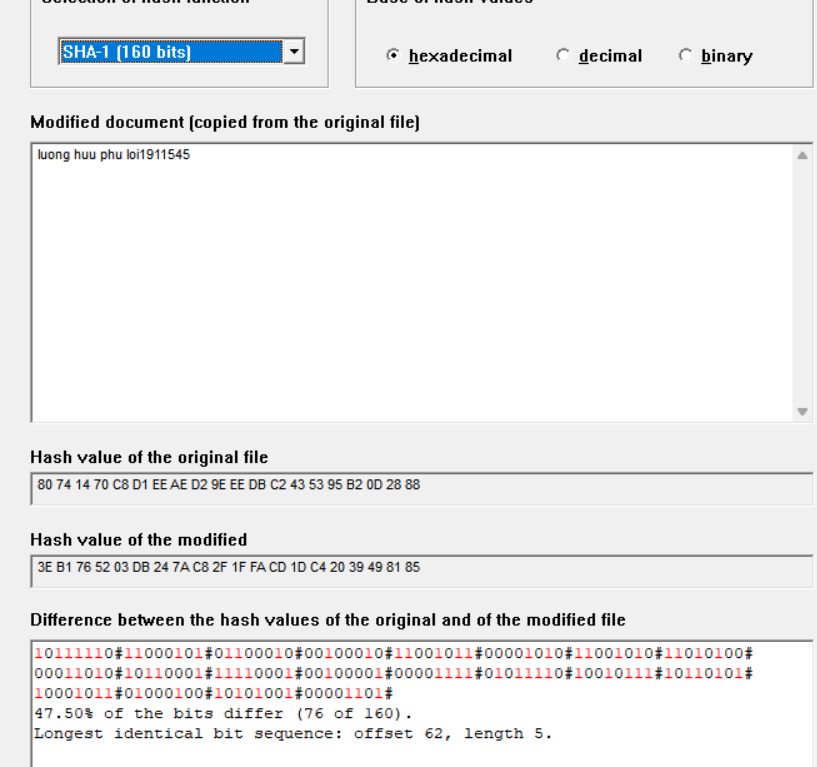
**MD5**



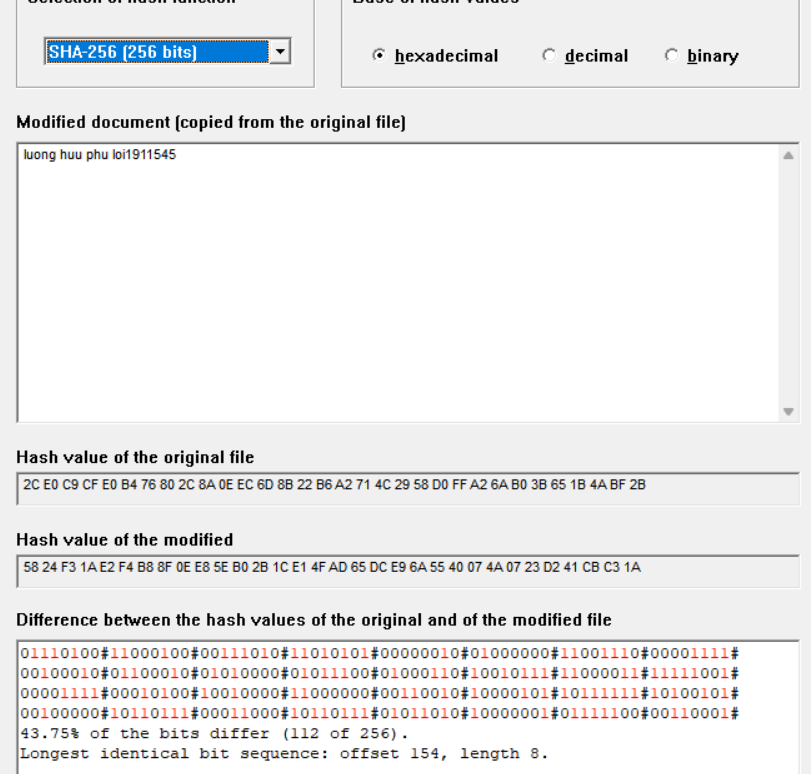
**SHA**



**SHA-1**



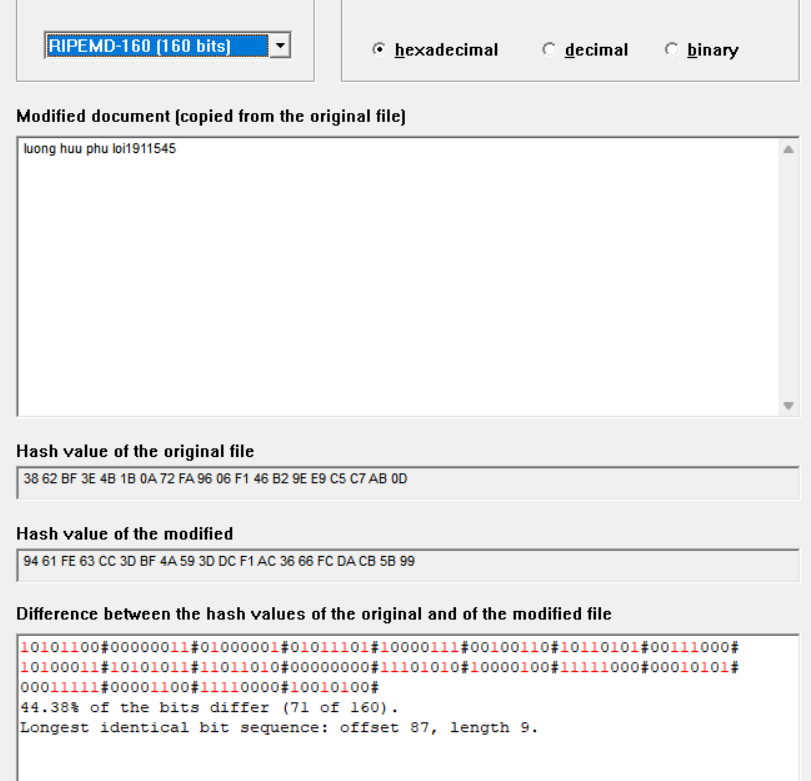
**SHA-256**



**SHA-512**



**RIPEMD**



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **MD2** | **MD4** | **MD5** | **SHA** | **SHA-1** | **SHA-256** | **SHA-512** | **RIPEMD** |
| **49.22** | **54.69** | **49.22** | **49.38** | **47.50** | **43.75** | **48.24** | **44.38** |