BÀI THỰC HÀNH SỐ 2

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: Lê Bảo Khánh**

**MSSV: 1911363**

**Nhóm: L01**

**Phần 1. Hệ mã bất đối xứng RSA**

**Câu 1:**

**Vai trò của public key:**

Khóa công khai (public-key): Bất kỳ ai cũng được biết . Được dùng để mã hóa thông điệp cần gửi hay xác minh chữ ký của một thông điệp đã nhận

**Vai trò của private key:**

Khóa riêng (private-key): Chỉ người dùng biết. Được dùng để giải mã một thông điệp đã nhận hay ký(tạo) chữ ký trên một thông điệp cần gửi

**Câu 2:**

**Chương trình Python:**

p = 17  
q = 31  
e = 7  
  
M = 2  
#######################################################################  
################### Generate private and public key ###################  
#######################################################################  
n = p \* q  
print(f"n = {n}")  
phi = (p - 1) \* (q - 1)  
print(f"phi = {phi}")  
  
# Finding d:  
d = 0  
for x in range(0, 1000):  
 if x \* e % phi == 1:  
 d = x  
 break  
  
print(f"d = {d}\n")  
  
print(f"Public key: n= {n}, e = {e}")  
print(f"Private key: p= {p}, q = {q} and d = {d}")  
  
#######################################################################  
####################### Encrypt and Decrypt ###########################  
#######################################################################  
print("\nEncrypt and Decrypt")  
C = M\*\*e % n  
print(f"Plain text: M= {M}")  
print(f"Ciphertext: C= {M}^{e} mod {n} = {C}")  
print(f"Encrypt: {C}^^{d} mod {n} = {C\*\*d % n}")

1. p=3;q=11,e=7;M=5

\* Tạo cặp khoá public key và private key:

n = p\*q = 3\*11 = 33

ø(n) = (p-1)\*(q-1)= 2\*10 = 20

e = 7 (7 và 20 là 2 số nguyên tố cùng nhau)

d = 3 (thoả điều kiện: 7\*3 mod 20 = 1)

Public key: n = 33 và e = 7

Private key: p = 3, q = 11 và d = 3

\* Mã hóa:

M = 5

C = 57 mod 33 = 14

\* Giải mã:

M = 143 mod 33 = 5

1. p=5;q=11,e=3;M=9

\* Tạo cặp khoá public key và private key:

n = p\*q = 5\*11 = 55

ø(n) = (p-1)\*(q-1)= 4\*10 = 40

e = 3 (3 và 40 là 2 số nguyên tố cùng nhau)

d = 27 (thoả điều kiện: 27\*3 mod 40 = 1)

Public key: n = 55 và e = 3

Private key: p = 5, q = 11 và d = 27

\* Mã hóa:

M = 9

C = 93 mod 55 = 14

\* Giải mã:

M = 1427 mod 55 = 9

1. p=7;q=11,e=17;M=8

\* Tạo cặp khoá public key và private key:

n = p\*q = 7\*11 = 77

ø(n) = (p-1)\*(q-1)= 6\*10 = 60

e = 17 (17 và 60 là 2 số nguyên tố cùng nhau)

d = 53 (thoả điều kiện: 53\*17 mod 60 = 1)

Public key: n = 77 và e = 17

Private key: p = 7, q = 11 và d = 53

\* Mã hóa:

M = 8

C = 817 mod 77 = 57

\* Giải mã:

M = 5753 mod 77 = 8

1. p=11;q=13,e=11;M=7

\* Tạo cặp khoá public key và private key:

n = p\*q = 11\*13 = 143

ø(n) = (p-1)\*(q-1)= 10\*12 = 120

e = 11 (17 và 120 là 2 số nguyên tố cùng nhau)

d = 11 (thoả điều kiện: 11\*11 mod 120 = 1)

Public key: n = 143 và e = 11

Private key: p = 11, q = 13 và d = 11

\* Mã hóa:

M = 7

C = 711 mod 143 = 106

\* Giải mã:

M = 10611 mod 143 = 7

1. p=17;q=31,e=7;M=2

\* Tạo cặp khoá public key và private key:

n = p\*q = 17\*31 = 527

ø(n) = (p-1)\*(q-1)= 16\*30 = 480

e = 7 (7 và 480 là 2 số nguyên tố cùng nhau)

d = 343 (thoả điều kiện: 343\*7 mod 480 = 1)

Public key: n = 527 và e = 7

Private key: p = 17, q = 31 và d = 343

\* Mã hóa:

M = 2

C = 27 mod 527 = 128

\* Giải mã:

M

= 128343 mod 527

= 128256 x 12864 x 12816 x 1282 x 1281 mod 527

= 35 x 256 x 35 x 101 x 47 x 128

= 2 mod 527

= 2

**Câu 3:**

**Ciphertext:**

C = 10

**Public key:**

e = 5

n = 35

**Tìm plaintext:**

\* Phân tích n:

n = 35 = 5 \* 7

=> Chọn p = 5, q = 7

\* Tìm d:

Ta có:

ø(n)=(p–1)(q-1)=4 x 6=24

Tiếp theo, tìm d sao cho

+ d.e 1 (mod 24) (hay 5d 1 mod 24)

+ d < 24

Sử dụng Extended Euclidean hoặc Brute Force,

ta tìm được d = 5 vì 5 . 5 = 25 = 1 . 24 + 1

\* Giải mã:

M = 105 mod 35 = 5

**Câu 4:**

**Public key:**

e = 31

n = 3599

**Tìm private key:**

\* Tìm p và q:

Phân tích n = 3599 ra thừa số nguyên tố:

Ta thử phân tích trong khoảng từ 1 đến

Chọn cách thử và sai, ta được 3599 / 59 = 61

Vậy p = 59, q = 61

Cách khác: n = 3599 = 3600 – 1 = 602 – 12 = (60 - 1) (60 + 1) = 59 . 61

Vậy p = 59, q = 61

\* Tìm d:

Ta có:

ø(n)=(p–1)(q-1)=58 x 60= 3480

Tiếp theo, tìm d sao cho

+ d.e 1 (mod 3480) (hay 31d 1 mod 3480)

+ d < 3480

Sử dụng Extended Euclidean

ta tìm được d = 3031 vì 3031 . 31 = 93961= 27 . 3480 + 1

\* Private key:

PR = {3031, 3599}

**Phần 2. Hàm băm (Hash function)**

**Câu 1:**

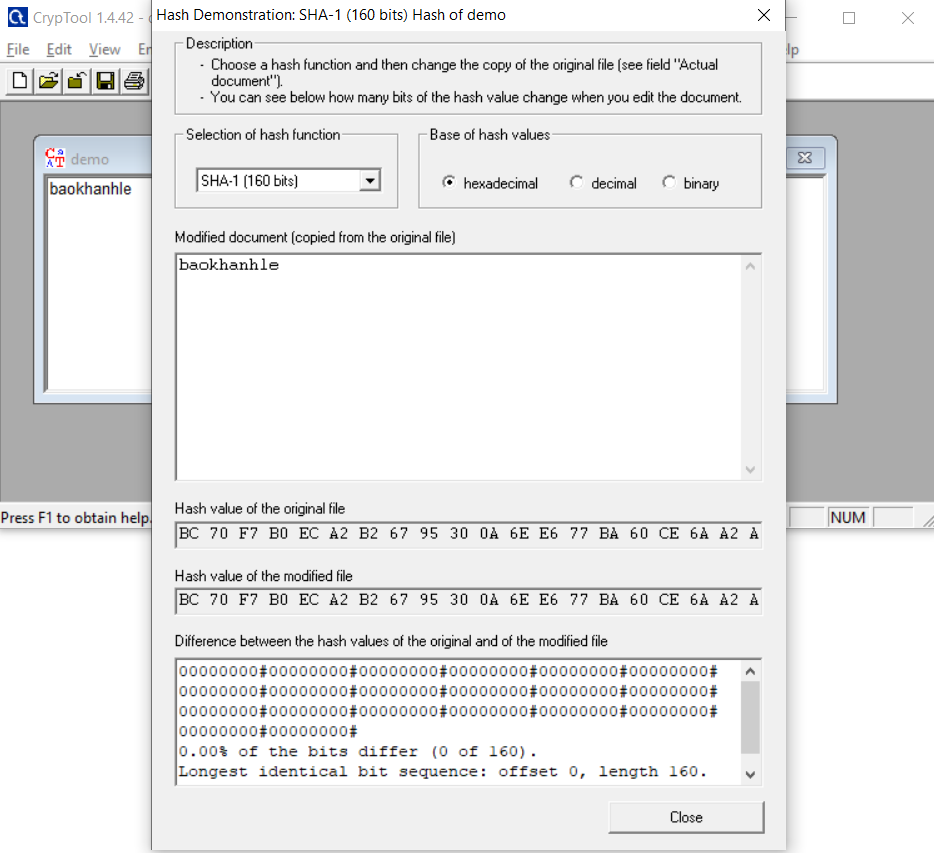
Hàm một chiều (one-way function) y = f(x) là hàm ánh xạ một miền xác định (domain) vào một miền giá trị (range) sao cho mỗi giá trị y = f(x) có một và chỉ một giá trị hàm ngược x = f-1(y) tương ứng.

Bên cạnh đó, việc tính toán hàm thuận y = f(x) là dễ dàng trong khi tính toán hàm ngược x = f-1(y) là không khả thi (infeasible)

**Câu 2:**

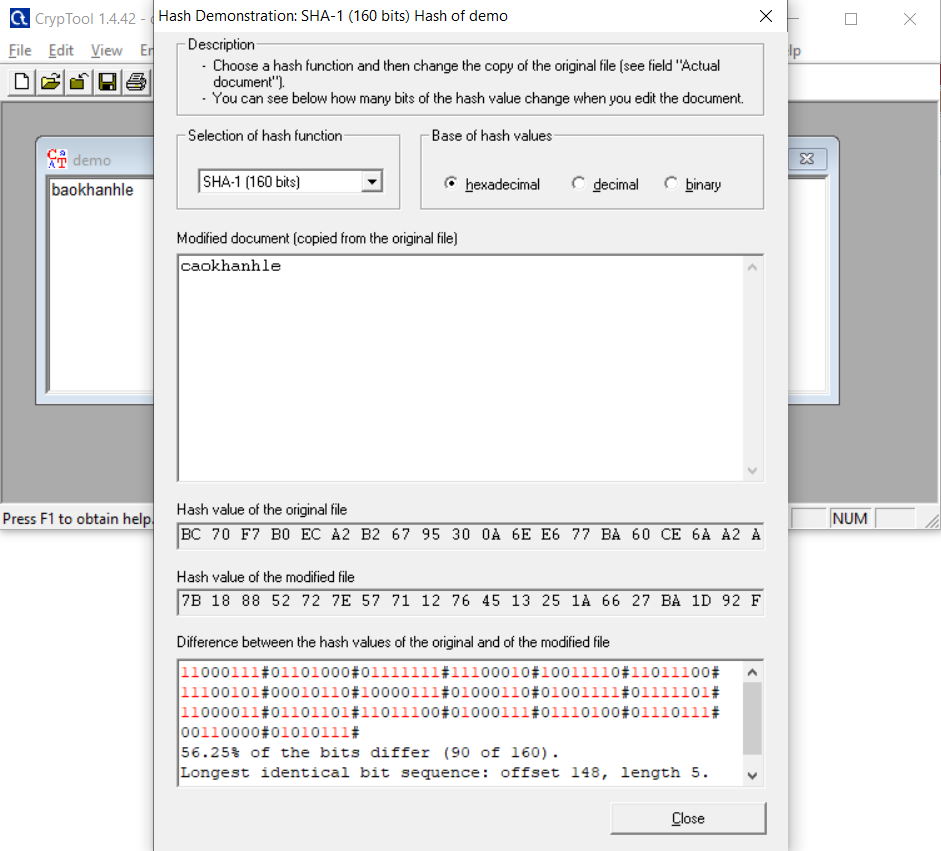
Plaintext: baokhanhle

SHA-1 (baokhanhle) = BC 70 F7 B0 EC A2 B2 67 95 30 0A 6E E6 77 BA 60 CE 6A A2 A7



Thay đổi một kí tự trong plaintext: caokhanhle

SHA-1(caokhanhle) = 7B 18 88 52 72 7E 57 71 12 76 45 13 25 1A 66 27 BA 1D 92 F0

****Ta thấy, chỉ cần một thay đổi nhỏ trong plain text có thể thay đổi hơn một nửa giá trị hash (57.03%), do đó hash function có thể đảm bảo sự toàn vẹn của dữ liệu

**Câu 3:**

a.

Chọn thử từng ký tự

Vào menu “Indiv. Procedures” -> “Hash” -> “Hash Demonstration”.

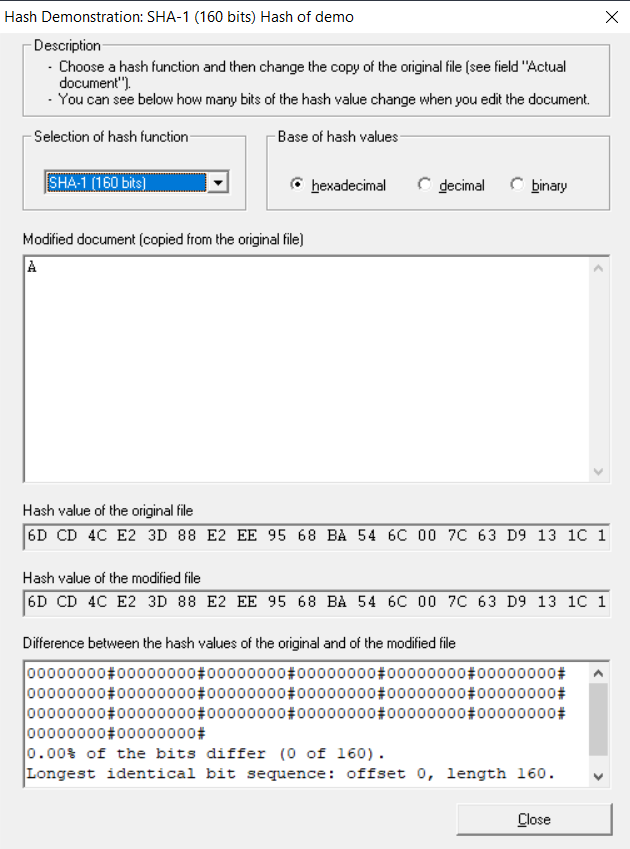
Ta chọn SHA-1 làm hash function.

Nhập từng ký tự A - Z vào box “Modified document” để kiểm tra

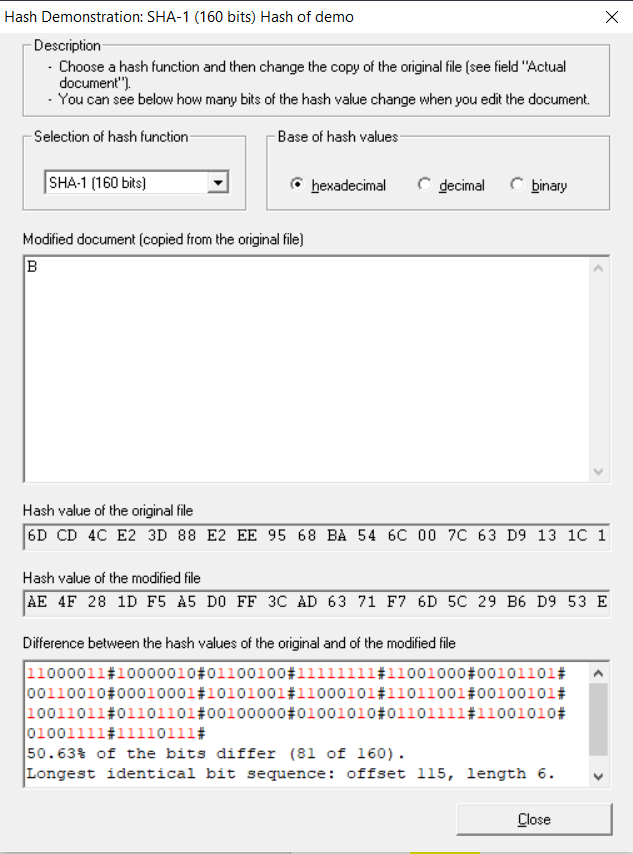
Nếu có kí tự nào sinh ra hash value = C6 3A E6 DD 4F C9 F9 DD A6 69 70 E8 27 D1 3F 7C 73 FE 84 1C thì đó là ký tự cần tìm

+ A:

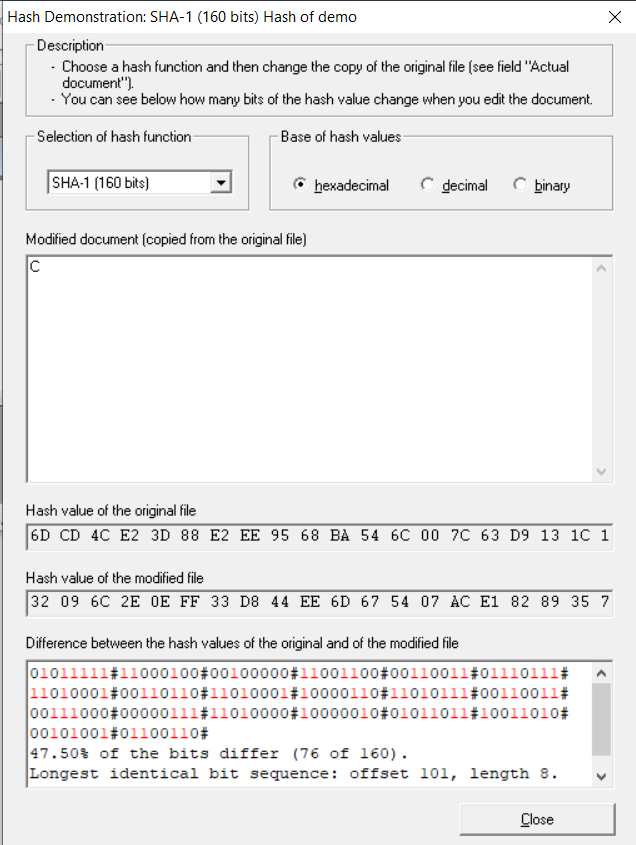
SHA-1 (A) = 6D CD 4C E2 3D 88 E2 EE 95 68 BA 54 6C 00 7C 63 D9 13 1C 1B

****+ B:

SHA-1 (B) = AE 4F 28 1D F5 A5 D0 FF 3C AD 63 71 F7 6D 5C 29 B6 D9 53 EC

****+ C:

SHA-1 (C) = 32 09 6C 2E 0E FF 33 D8 44 EE 6D 67 54 07 AC E1 82 89 35 7D

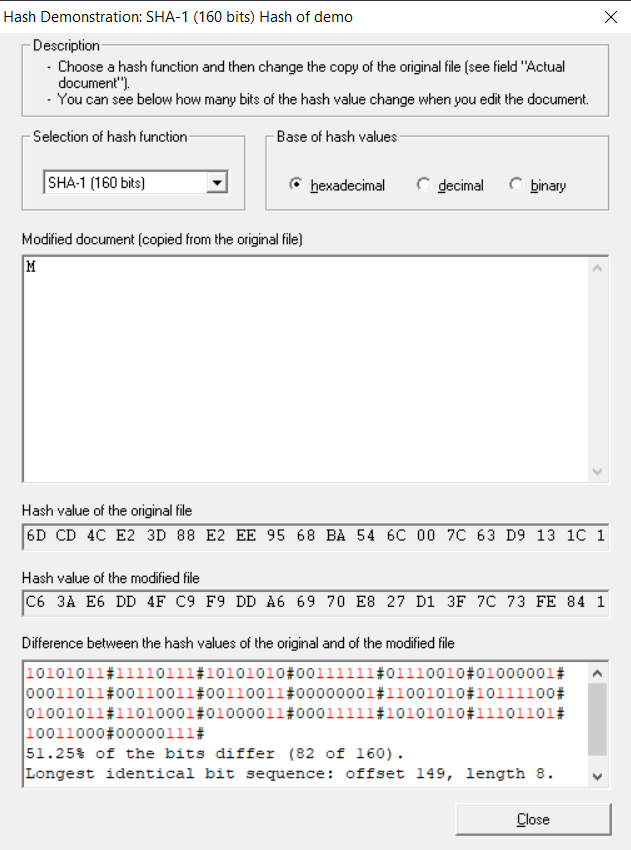
****...

...

...

+ M:

SHA-1 (M) = C6 3A E6 DD 4F C9 F9 DD A6 69 70 E8 27 D1 3F 7C 73 FE 84 1C

****

Vậy M chính là ký tự cần tìm

b.

Không thể kết luận hàm hash SHA-1 không thoả mãn tính chất một chiều (one-way), do việc tính toán hàm ngược (hay tìm lại plaintext ban đầu) vẫn tốn kém rất nhiều về mặt thời gian (không khả thi trong giới hạn thời gian tương đối ngắn), đặc biệt trong trường hợp plaintext có độ dài lớn

**Câu 4:**

Plaintext: This is a message

Tiến hành thêm một ký tự khoảng trắng vào sau từ “is”, ghi lại sự thay đổi

Tiến hành lại với các giải thuật hash khác, ta được bảng sau:

|  |  |  |  |
| --- | --- | --- | --- |
| Hash function | Số bit thay đổi | Tổng số bit | Phần trăm (%) thay đổi |
| MD2 | 70 | 128 | 54.69 |
| MD4 | 67 | 128 | 52.34 |
| MD5 | 61 | 128 | 47.66 |
| SHA | 76 | 160 | 47.50 |
| SHA-1 | 96 | 160 | 60.00 |
| SHA-256 | 129 | 256 | 50.39 |
| SHA-512 | 268 | 512 | 52.34 |
| RIPEMD-160 | 69 | 160 | 43.13 |

