BÀI THỰC HÀNH SỐ 2

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: Nguyễn Hữu Bảo**

**MSSV: 1811523**

**Nhóm: L01**

**Phần 1. Hệ mã bất đối xứng RSA**

**Câu 1:**

Public key là để bên gửi mã hoá plain text, private key là để bên nhận giải mã cipher text

**Câu 2:**

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

**A:**

n = pq=33

ø(n) = (p-1)\*(q-1) =20

e = 7

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

Public Key: m = 33 và e = 7Private Key: p = 3, q = 11 và d = 3

**Mã hoá thông điệp:**B muốn gởi thông điệp đến A: plaintext = 5

B tính ciphertext = 57 mod 33 = 14B gởi ciphertext 14 đến A

**Giải mã thông điệp:**

A nhận được ciphertext: 14. Để giải mã thông điệp này, A sử dụng khoá riêng

Plaintext = 143 mod 33 = 5 A giải mã được thông điệp: 5

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

**A:**

n = pq=55

ø(n) = (p-1)\*(q-1) =40

e = 3

d = 27

Public Key: m = 55 và e = 3Private Key: p = 5, q = 11 và d = 27

**Mã hoá thông điệp:**B muốn gởi thông điệp đến A: plaintext = 9

B tính ciphertext = 93 mod 55 = 14B gởi ciphertext 14 đến A

**Giải mã thông điệp:**

A nhận được ciphertext: 14

Plaintext = 1427 mod 55 = 9 A giải mã được thông điệp: 9

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

**A:**

n = pq=77

ø(n) = (p-1)\*(q-1) =60

e = 17

d = 53

Public Key: m = 77 và e = 17Private Key: p = 7, q = 11 và d = 53

**Mã hoá thông điệp:**B muốn gởi thông điệp đến A: plaintext = 8

B tính ciphertext = 817 mod 77 = 57B gởi ciphertext 57 đến A

**Giải mã thông điệp:**

A nhận được ciphertext: 57.

Plaintext = 5753 mod 77 = 8 A giải mã được thông điệp: 8

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

**A:**

n = pq=143

ø(n) = (p-1)\*(q-1) =120

e = 11

d = 11

Public Key: m = 143 và e = 11Private Key: p = 11, q = 13 và d = 11

**Mã hoá thông điệp:**B muốn gởi thông điệp đến A: plaintext = 7

B tính ciphertext = 711 mod 143 = 106B gởi ciphertext 106 đến A

**Giải mã thông điệp:**

A nhận được ciphertext: 106.

Plaintext = 10611 mod 143 = 7 A giải mã được thông điệp: 7

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

**A:**

n = pq=527

ø(n) = (p-1)\*(q-1) =480

e = 7

d = 343

Public Key: m = 527 và e = 7Private Key: p = 17, q = 31 và d = 343

**Mã hoá thông điệp:**B muốn gởi thông điệp đến A: plaintext = 2

B tính ciphertext = 27 mod 527 = 128B gởi ciphertext 128 đến A

**Giải mã thông điệp:**

A nhận được ciphertext: 128.

Plaintext = 128343 mod 527 = 2 A giải mã được thông điệp: 2

**Câu 3:**

n = 35 nhỏ nên có thể dễ dàng đoán ra p = 5, q = 7

ø(n) = (p-1)\*(q-1) = 24

e = 5

d = 5

Private Key: p = 5, q = 7 và d = 5

M = 105 mod 35 = 5

**Câu 4:**

n = 3599 cũng còn kha khá nhỏ nên nếu thử chia lần lượt cho các số nguyên tố từ 2 trở lên thì sẽ tìm được p = 59, q = 61

ø(n) = (p-1)\*(q-1) = 3480

e = 31

d = 3031

Private Key: p = 59, q = 61 và d = 3031

**Phần 2. Hàm băm (Hash function)**

**Câu 1:**

Hàm 1 chiều là hàm không khả thi để tìm được giá trị đầu vào khi biết giá trị đầu ra

**Câu 2:**

Plain text: HUUBAO

Mã hoá bằng mã Caesar với k=1

Cipher text: IVVCBP

Cipher text bị thay đổi: IVVCBB

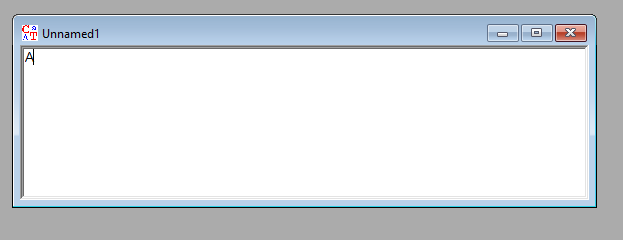
Dùng thuật toán hash MD2 với cipher text: 7F 31 63 8C C1 2D 1F AD E9 28 C9 22 A3 F8 A9 89

Dùng thuật toán hash MD2 với cipher text bị thay đổi: E6 56 43 B1 82 C4 C8 32 1C 0C 35 B3 8D 45 8F 93

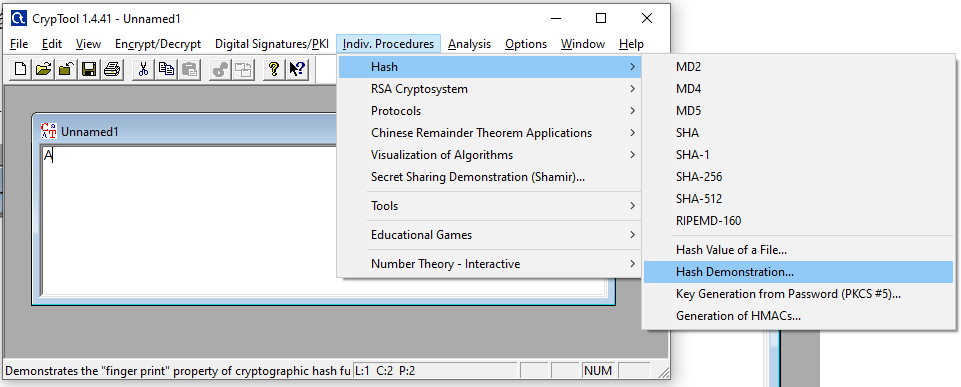
Chúng ta thấy 2 dãy hex khác nhau rõ rệt

**Câu 3:**

Gõ 1 chữ A vào ô văn bản:



Chọn các mục như hình:



Thay từng chữ từ B đến Z rồi từ a đến z cho đến khi giá trị hash hiển trị trong ô duới trùng với giá trị đề bài:

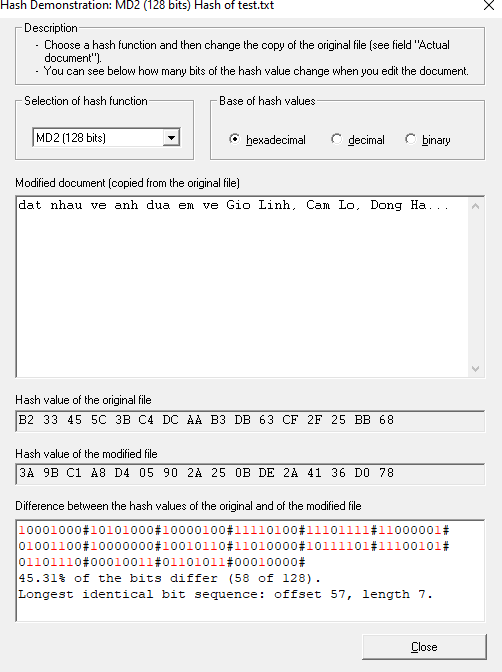


Cuối cùng tìm được chữ M thoã mãn

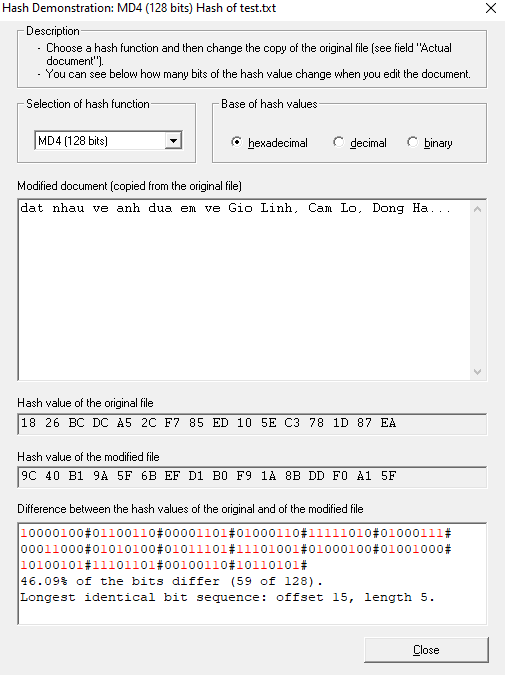
1. Không thể kết luận hàm hash SHA-1 không thoả mãn tính chất một chiều, bởi vì đề đã gợi ý bản rõ là 1 ký tự tiếng anh nên chỉ cần thế lần lượt 52 ký tự hoa thường vào sẽ ra được ký tự cần tìm. Không có gợi ý đó thì chúng ta k biết phải dò theo quy tắc nào để tìm ra bản rõ

**Câu 4:**

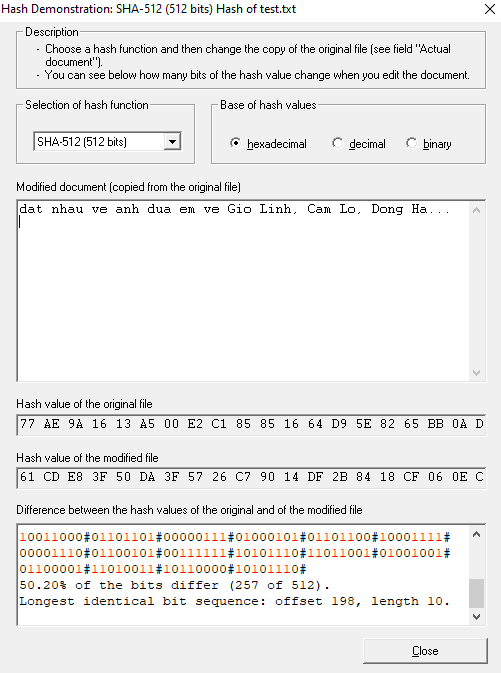
45.31%:



46.09%:



50.2%:



49.38%:

