Faculty of Computer Science and Engineering

Ho Chi Minh City University of Technology



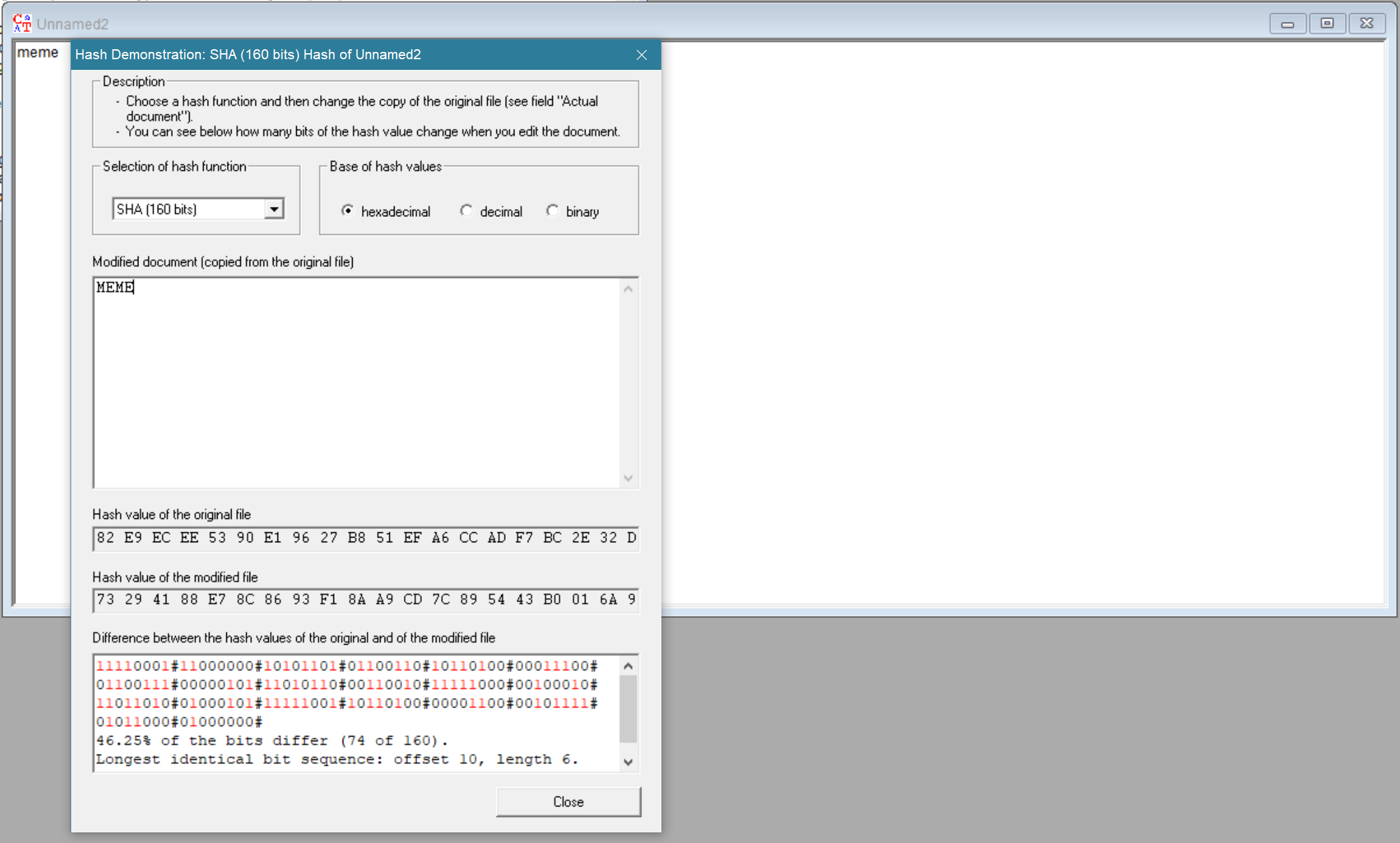
Nguyen Phuong Vuong - 1614186

Cryptography and Network Security

Lab 4

# Execise 1.

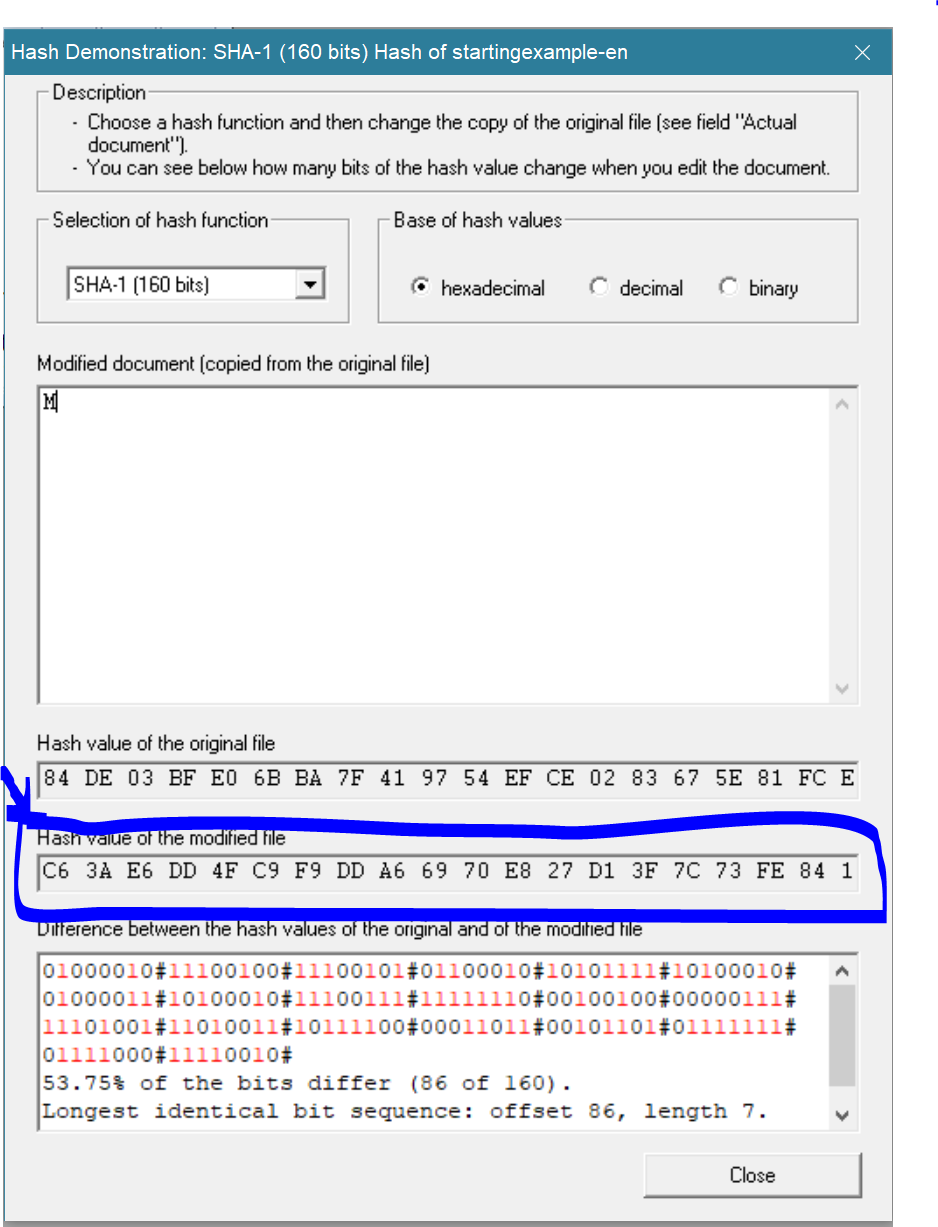
Sau khi A gửi cho B đoạn messeage là: MEME và đoạn Hash value là **73 29 41 88 E7 8C 86 93 F1 8A A9 CD 7C 89 54 43 B0 01 6A 94**(theo SHA 160bits).Sau khi dùng giải thuật DES, B nhận được messeage là MEME và B dùng SHA 160bits B tìm được hash value tương tự A. Nếu B nhận được messeage là meme thì sau khi hash nhận được hash value: **82 E9 EC EE 53 90 E1 96 27 B8 51 EF A6 CC AD F7 BC 2E 32 D4**. Điều này chứng tỏ tính toàn vẹn của message tức nếu messeage A gửi khác B nhận thì B có thể biết được đúng messeage hay không.



# Execise 2.

a, Nếu ta có 200 bits input(tức là có 2200 trường hợp của input) thì dựa vào hàm hash ta có thể sinh ra 200 bits output(2200 trường hợp của output). Theo đề hash value tức output chỉ có 160 bits nên ta có 40 bits (200 – 160 = 40 bits) là tùy chọn. Vậy ta sẽ có được 240 input tạo ra output(hash value) trùng nhau. Hay trung bình với khả năng sinh hash value giống nhau của 1 input là 240/2120 khả năng.

b, Ta dùng phương pháp vét cạn để quét tất cả các trường hợp tạo ra hash value. Theo đề, messeage là 1 chữ theo alphabet nên có 52 trường hợp (26 chữ hoa và 26 chữ thường). Sau khi thực hiện vét cạn ta được messeage là M.



c, Hàm SHA-1 là hàm 1 chiều tức là không thể thì hash value sinh ra mà giải ngược lại messeage ban đầu. Ta chỉ dùng phương pháp vét cạn tất cả các khả năng có thể có của messeage để xác định được hash value thỏa mãn.

d, Sau khi ta chỉnh lại file ban đầu(meme) thành MEME. Ta nhận được 1 hash value(SHA 160bits) khác hash value ban đầu (khác đến 46,25 %).

