BÀI THỰC HÀNH SỐ 2
Môn: MẬT MÃ & AN NINH MẠNG
-o0o-

I. MỤC TIÊU
- Cung cấp kiến thức về hệ mã bất đối xứng RSA.
- Cung cấp kiến thức về các hàm băm (hash function), sử dụng công cụ CrypTool để thực hiện tính toán giá trị băm trên thông điệp sử dụng nhiều hàm băm khác nhau và khảo sát kết quả.

II. CHUẨN BỊ TRƯỚC KHI THỰC HIỆN BÀI THỰC HÀNH
- Sinh viên ôn tập lại phần lý thuyết chương 3 và chương 4
- Cài đặt công cụ CrypTool 1 (version: 1.4.31 Beta 06 - English): https://www.cryptool.org/en/ct1-downloads

III. CÁCH THỨC VÀ HẠN CHÓT NỘP BÀI
- Sinh viên trả lời tất cả các câu hỏi trong bài thực hành vào file **<MSSV>_Lab02.docx** (sử dụng mẫu file trả lời được đính kèm) và nộp bài theo deadline của bài Lab02 ở Bkel, không nhận bài nộp qua email hay các hình thức khác.
- Thời gian để thực hiện bài Lab là 14 ngày.

IV. NỘI DUNG THỰC HIỆN

Phần 1. Hệ mã bất đối xứng RSA

1.1. Cách thức hoạt động của hệ mã RSA

RSA là một hệ mã hóa bất đối xứng được phát triển bởi Ron Rivest, Adi Shamir và Leonard Adleman (tên của nó cũng chính là tên viết tắt của 3 tác giả này) và được sử dụng rộng rãi trong mã hoá thông điệp và chữ ký số. Trong hệ mã hóa này, khoá công khai (public key) được chia sẻ công khai cho tất cả mọi người.

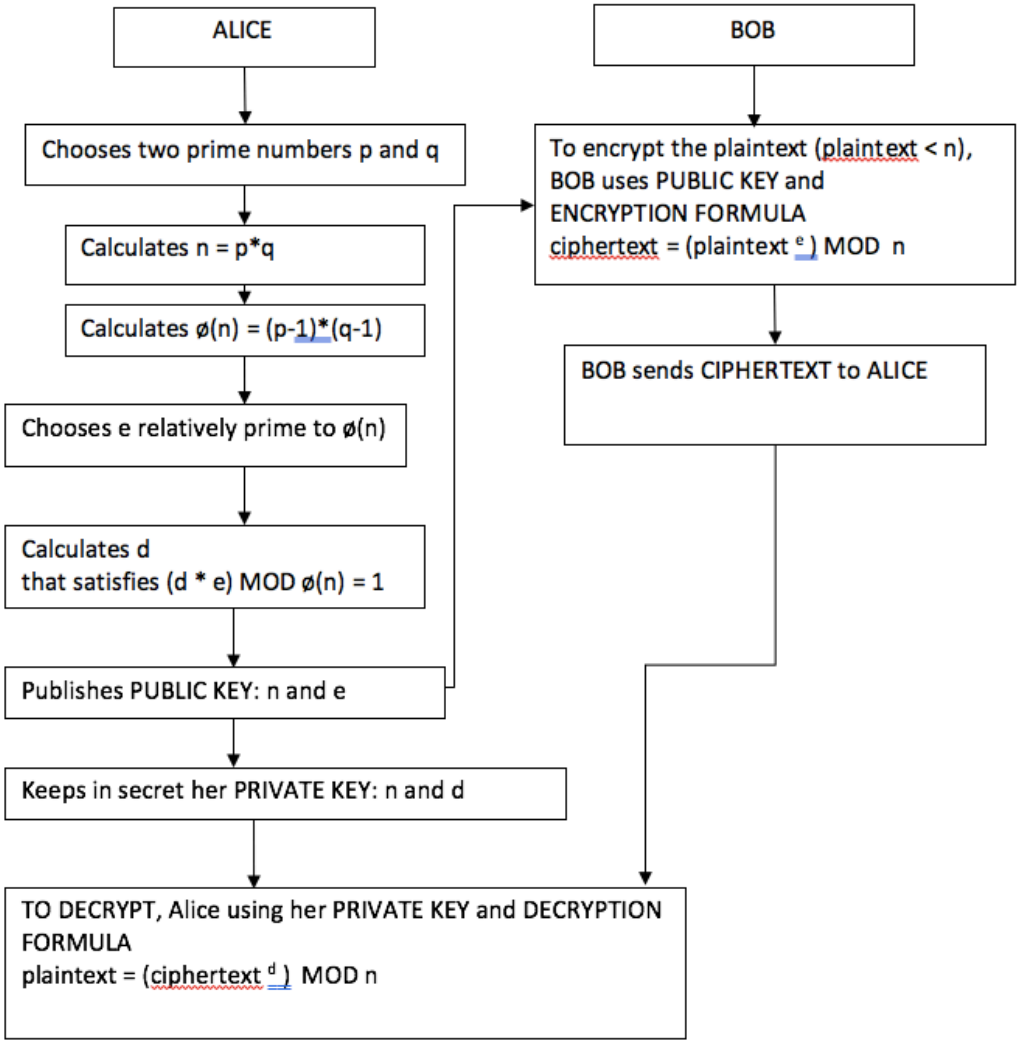
Tóm tắt giải thuật RSA

Ví dụ minh hoạ:

Alice:
Bước 1: Chọn 2 số nguyên tố p = 5 and q = 11
Bước 2: n = p*q = 5*11 = 55
Bước 3: ø(n) = (p-1)*(q-1) = 4*10 = 40
Bước 4: e = 3 (40 và 3 là 2 số nguyên tố cùng nhau)
Bước 5: tính d = 27 (thoả điều kiện (27 * 3) MOD 40 = 1)
Alice Public Key: n = 55 và e = 3
Alice Private Key: n = 55 và d = 27

Mã hoá thông điệp:
Bob muốn gởi thông điệp đến Alice: plaintext = 12
Bob tính ciphertext = 12^3 mod 55 = 23
Bob gởi ciphertext 23 đến Alice

Giải mã thông điệp:
Alice nhận được ciphertext: 23. Để giải mã thông điệp này, Alice sử dụng khoá riêng (Private Key):
plaintext = 23^{27} mod 55 = 12
Alice giải mã được thông điệp: 12



Ví dụ 2:

Trong thực tế cả hai thực thể giao tiếp (Bob và Alice) đều tạo cặp khoá (public và private key) và cả hai thực thể có thể gởi và nhận thông điệp của nhau. Trong ví dụ này chúng ta xem xét tất cả các bước mà Alice và Bob thực hiện để có thể gởi/nhận thông điệp an toàn cho nhau.

1. Alice và Bob tạo cặp khoá public key và private key

Đối với Alice (theo 5 bước như ở ví dụ trước):
1. Chọn p = 3 and q = 11
2. n = p*q = 3*11 = 33
3. ø(n) = (p-1)*(q-1)= 2*10 = 20
4. e = 7 (7 và 20 là 2 số nguyên tố cùng nhau)
5. d = 3 (thoả điều kiện: 7*3 mod 20 = 1)

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

Đối với Bob (tương tự theo 5 bước như ở ví dụ trước)
1. Chọn p = 5 and q = 13
2. n = p*q = 65
3. ø(n) = (p-1)*(q-1)= 4*12= 48
4. e = 11 (11 and 48 are relatively prime)
5. d = 35 (35*11 mod 48 = 1)

Bob Public Key: m = 65 and e = 11
Bob Private Key: p = 5, q= 13 and d = 35

2. Khi Alice muốn gởi thông điệp cho Bob, Alice sẽ làm theo các bước sau:
1. Truy cập vào website của Bob (hoặc các kênh chia sẻ khác của Bob) để lấy public key: n = 65 và e = 11
2. Alice muốn gởi thông điệp (plaintext) = 17 (thoả điều kiện 17 < 65)
3. Alice mã hoá plaintext sử dụng Public key của Bob: 17^{11} mod 65 = 23
4. Alice gởi ciphertext: 23 cho Bob

Bob nhận ciphertext: 23 từ Alice. Để giải mã, Bob sử dụng PRIVATE KEY và công thức như bên dưới:
23^{35} mod 65 = 17 (Bob sử dụng private key d = 35)
Bob giải mã và nhận được thông điệp của Alice (plaintext): 17

3. Tiếp theo, Bob muốn gởi thông điệp phản hồi cho Alice, Bob cũng thực hiện theo quy trình tương tự như Alice:
1. Bob truy cập vào website của Alice (hoặc các kênh chia sẻ khác của Alice) để lấy Public Key của Alice: n = 33 and e =7
2. Bob muốn gởi thông điệp (plaintext) = 14 (thoả điều kiện 14 < 33)
3. Bob tiến hành mã hoá thông điệp sử dụng Public Key của Alice: 14^7 mod 33 = 20
4. Bob gởi ciphertext: 20 đến Alice

Alice nhận ciphertext = 20 và tiến hành giải mã sử dụng Private Key với công thức giải mã:
20^3 mod 33 = 14 (Alice sử dụng private key d = 3)
Alice giải mã và nhận được thông điệp của Bob (plaintext): 14
Trong ví dụ này:
- Alice sử dụng Public Key của Bob để gởi thông điệp cho Bob.
- Bob sử dụng Public Key của Alice để gởi thông điệp cho Alice.
- Để giải mã, Bob và Alice sử dụng Private Key tương ứng của họ.

1.2. Bài tập

Sinh viên trả lời các câu hỏi sau đây:

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

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

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

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

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

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

e. p=17;q=31,e=7;M=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?

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

Thuật toán Euclid mở rộng

```
Procedure Euclid_Extended (a,m)
int,  y0=0,y1:=1;
While a>0 do {
     r:= m mod a
     if r=0 then Break
     q:= m div a
     y:= y0-y1*q
     m:=a
     a:=r
     y0:=y1
     y1:=y
  }
 If a>1 Then Return null
 else Return y
```

Phần 2. Hàm băm (Hash function)

1.1. Giới thiệu về hàm băm

Hàm băm là hàm có chức năng chuyển thông điệp có kích thước bất kì bất kỳ về kích thước cố định. Giả thiết hàm hash là công khai và không dùng khóa. Hash chỉ phụ thuộc thông điệp và được sử dụng để phát hiện thay đổi của thông điệp . Hash có thể sử dụng nhiều cách khác nhau với thông điệp, hash thường được kết hợp dùng để tạo chữ ký trên thông điệp.

Hàm Hash tạo nên dấu vân tay (tức là thông tin đặc trưng) của một file hay thông điệp, Hàm Hash được giả thiết là công khai, mọi người đều biết cách sử dụng, công thức như bên dưới:

$$h = H(M)$$

Với h là giá trị hash, M là thông điệp, H là hàm hash (hàm băm).

Tham khảo một số hàm băm:

Name	Length	Type
GOST	256 bits	hash
HAS-160	160 bits	hash
HAVAL	128 to 256 bits	hash
MD2	128 bits	hash
MD4	128 bits	hash
MD5	128 bits	hash
RadioGatún	Up to 1216 bits	hash
RIPEMD-64	64 bits	hash
RIPEMD-160	160 bits	hash
RIPEMD-320	320 bits	hash
SHA-1	160 bits	hash
SHA-224	224 bits	hash
SHA-256	256 bits	hash
SHA-384	384 bits	hash
SHA-512	512 bits	hash
Skein	256, 512 or 1024 bits	hash
Snefru	128 or 256 bits	hash
Tiger	192 bits	hash
Whirlpool	512 bits	hash
FSB	160 to 512 bits	hash
ECOH	224 to 512 bits	hash
SWIFFT	512 bits	hash

1.2. Bài tập

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

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.

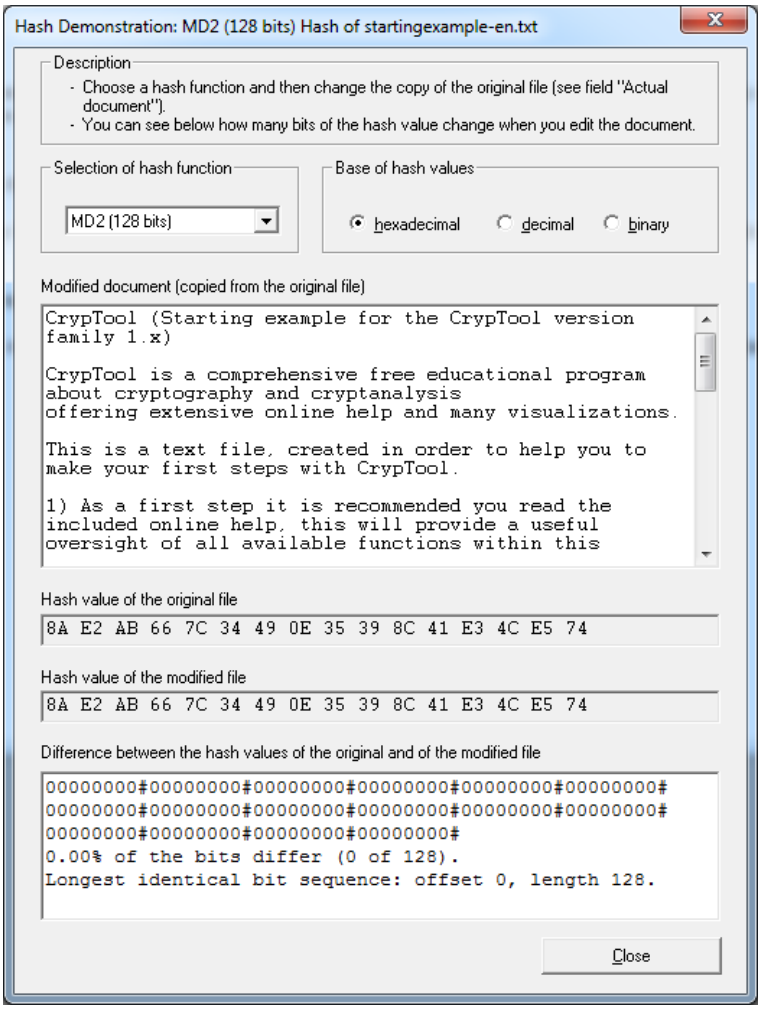
Câu 3. Hàm băm H(·) là hàm có chức năng chuyển thông điệp có kích thước bất kì bất kỳ về kích thước cố định:

a. 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)

b. 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?

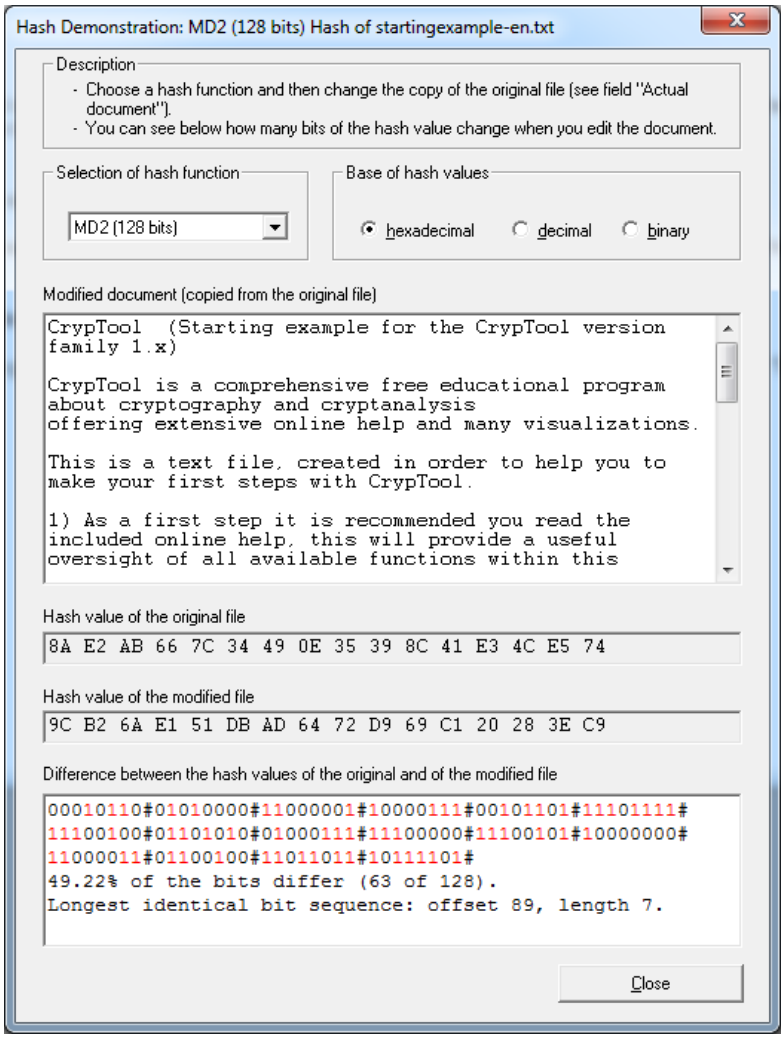
Câu 4. Sử dụng công cụ CrypTool để thực hành tính toán giá trị hash trên thông điệp bất kỳ

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.