TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
KHOA CÔNG NGHỆ THÔNG TIN

BÀI TẬP – THẢO LUẬN

AN TOÀN VÀ BẢO MẬT THÔNG TIN

Số tín chỉ: 2
Hệ đào tạo: Chính quy
Ngành: Công nghệ thông tin
Họ và tên giảng viên : Nguyễn Lan Oanh
Đơn vị công tác: Bộ môn Công nghệ phần mềm

Năm học: 2016 – 2017

BÀI TẬP CHƯƠNG 2

Bài 1: Cho hoán vị:

1 2 3 4 5

3 5 1 2 4

là khóa bí mật của mật mã hoán vị.

a. Giải mã bản mã: “SACBANCLAA”

b. Mã bản rõ : “gonewiththewwind”

Bài 2: Cho hoán vị:

1 2 3 4 5

2 4 5 3 1

là khóa bí mật của mật mã hoán vị

a. Hãy trình bày quá trình giải mã bản mã: **“EPDIEIDNESYOOUF”.**

b. Hãy mã bản rõ: “**casablanca**”

Bài 3: Cho khoá của mã Affine (a,b)=(19,23)

a. Hãy trình bày quá trình mã bản tin sau: **“Hello”**

b. Hãy trình bày quá trình giải mã : “**IJMB**”

Bài 4: Cho khoá của mã Affine (a,b)=(21,23)

a. Hãy giải mã bản mã: **“GBEEJ”**

b. Hãy mã bản rõ : “Bill”

Bài 5: Biết khoá của mã Affine (a,b)=(23,15)

a, Hãy giải mã bản mã: **”KTGP”**

b, Hãy mã bản rõ: “**mediocre**”

Bài 6: Biết khoá của mã Affine là (a,b) =(21,24)

a. Hãy mã bản tin: **“runaway”**

b. Hãy giải mã bản mã **“PENE”**

Bài 7: Cho ma trận khóa của mật mã Hill: K= 3 5

2 7

Hãy mã bản rõ: **“song”**

Bài 8: Cho ma trận khóa của hệ mật mã Hill: K= 3 5

2 7

Hãy giải mã bản mã: **“UUZQ”**

Bài 9: Cho từ khoá **MATION** của hệ mật mã Viginene .

Hãy mã bản rõ: **“anotherbrickinthewall”**

Bài 10: Cho từ khoá **INFORM** của hệ mật mã Viginene.

a.Trình bày quá trình giải mã bản mã: **IATHYQRUZWPSVSHYQWTTZ”**

b. Mã bản rõ: **“electricity”**

Bài 11: Cho từ khoá **PRO** của hệ mật mã Viginene.

a.Hãy mã bản rõ: **“paintmylove”**

b. Hãy giải mã bản mã: **“HVOZEOX”**

Bài 12: Cho từ khoá **TECT** của hệ mật mã Viginene.

a. Giải mã bản mã: **“ERWGXORAFJX”**

b. Hãy mã bản rõ: **“seagame”**

Bài 13: Cho từ khoá **SECURITY** của hệ mật mã Viginene

a. Hãy mã bản rõ: **“international”**

b. Hãy giải mã bản mã: **“EEUNVV”**

BÀI TẬP CHƯƠNG 3

Bài 1: Hãy chứng minh rằng phép giải mã DES có thể thực hiện bằng cách áp dụng thuật toán mã hoá DES cho bản rõ với bảng khoá đảo ngược.

Bài 2: Cho DES(x,K) là phép mã hoá DES của bản rõ x với khoá K. Giả sử y = DES(x,K) và y' = DES(c(x),c(K)) trong đó c(.) kí hiệu là phần bù theo các bít của biến. Hãy chứng minh rằng y' = c(y) (tức là nếu lấy phần bù của bản rõ và khoá thì bản mã kết quả cũng là phần bù của bản mã ban đầu). Chú ý rằng kết quả trên có thể chứng minh được chỉ bằng cách sử dụng mô tả "mức cao" của DES - cấu trúc thực tế của các hộp S và các thành phần khác của hệ thống không ảnh hưởng tới kết quả này.

Bài 3: Mã kép là một cách để làm mạnh thêm cho DES: với hai khóa K_1 và K_2 cho trước, ta xác định $y = e_{K2}(e_{K1}(x))$ (dĩ nhiên đây chính là tích của DES với chính nó. Nếu hàm mã hoá e_{K2} giống như hàm giải mã d_{K1} thì K_1 và K_2 được gọi là các khoá đối ngẫu (đây là trường hợp không mong muốn đối với phép mã kép vì bản mã kết quả lại trùng với bản rõ). Một khoá được gọi là tự đối ngẫu nếu nó đối ngẫu với chính nó.

a/ Hãy chứng minh rằng nếu C_0 gồm toàn các số 0 hoặc gồm toàn các số 1 và D_0 cũng vậy thì K là tự đối ngẫu.

b/ Hãy tự chứng minh rằng các khoá sau (cho ở dạng hexa) là tự đối ngẫu:

0101010101010101

FEEFEFEFEFEFEFE

1F1F1F1F0E0E0E0E

E0E0E0E0F1F1F1F1

c/ Hãy chứng tỏ rằng nếu C_0 = 0101. . . 01 hoặc 1010. . .10 (ở dạng nhị phân) thì XOR các xâu bít C_i và C_{17-i} là 111. . .11, vơi $1 \leq i \leq 16$ (khẳng định tương tự cũng đúng đối với D_i).

d/ Hãy chứng tỏ các cặp khoá sau là đối ngẫu:

E001E001F101F101 01E001E001F101F1

FE1FFE1FF0EFE0E 1FFE1FFE0EFE0EFE

E01FE01FFF10FF10 1FE01FE00EF10EF1

Bài 4: Có thể tạo một mã xác thực thông báo bằng chế độ CFB cũng như chế độ CBC. Cho dãy các khối bản rõ $x_1 . . . x_n$, giả sư ta xác định véc tơ khởi đầu IV là x_1 . Sau đó mã hoá $x_2 . . . x_n$ bằng khoá K ở chế độ CFB để thu được $y_1 ... y_{n-1}$ (chú ý rằng chỉ có n-1 khối bản mã). Cuối cùng xác định $e_K(y_{n-1})$ làm MAC. Hãy chứng minh rằng MAC này đòng nhất với MAC được tạo trong phần 3.4.1. dùng chế độ CBC.

Bài 5: Giả sử một dãy các khối bản rõ $x_1 . . . x_n$ được mã hoá bằng DES, tạo ra các khối bản mã $y_1 . . . y_2$. Giả sử rằng một khối bản mã (chẳng hạn y_i) bị phát sai (tức là có một số số 1 bị chuyển thành số 0 và ngược lại). Hãy chỉ ra rằng số các khối bản rõ bị giải mã không đúng bằng một nếu ta dùng các chế độ ECB và OFB để mã hoá; và bằng hai nếu dùng các chế độ CBC và CFB để mã hoá.

Bài 6: Bài tập này nhằm nghiên cứu một phép tối ưu hoá thời gian - bộ nhớ đơn giản đối với phép tấn công bản rõ chọn lọc. Giả sử có một hệ mật trong đó P = C = K và đạt được độ mật hoàn thiện. Khi đó $e_K(x) = e_{K1}(x)$ có nghĩa là $K = K_1$. Kí hiệu $P = Y = \{y_1, . . ., y_N\}$. Cho x là bản rõ cố định. Định nghĩa hàm g: $Y \rightarrow Y$ theo quy tắc $g(y) = e_y(x)$. Ta xác định một đồ thì có hướng G chứa tập đỉnh Y, trong đó tập cạnh chứa tất cả các cạnh có hướng có dạng $(y_i, g(y_i))$, $1 \le i \le N$.

a/ Hãy chứng minh rằng G gồm tất cả các chu trình có hướng không liên thông.

b/ Cho T là một tham số thời gian mong muốn. Giả sử ta có một tập các phần tử $Z = \{z_1, . . ., z_m\} \subseteq Y$ sao cho với mỗi phần tử $y_i \in Y$ nằm trong một chu trình có độ dài tối đa là T hoặc tồn tại một phần tử $z_j \neq y_i$ sao cho khoảng cách tử y_i tới z_j

trong G tối đa là T. Hãy chứng tỏ rằng tồn tại một tập Z như vậy sao cho: $| Z | \leq 2N/T$ và như vậy $| Z | = 0(N/T)$.

c/ Với mỗi $z_j \in Z$ ta xác định $g^{-T}(z_j)$ là phần tử y_i sao cho $g^T(y_i) = z_j$, trong đó g^T là một hàm gồm T phép lặp của g. Hãy xây dựng một bảng X gồm các cặp $(z_i, g^{-T}(z_j))$ được sắp xếp theo các toạ độ đầu của chúng.

Một mô tả giả mã của một thuật toán tìm K với $y = e_K(x)$ cho trước được trình bày ở hình 3.15. Hãy chứng tỏ thuật toán này tìm K trong tối đa là T bước (bởi vậy cỡ của phép tối ưu hoá thời gian - bộ nhớ là 0(N)).

Hình 3.15. Phép tối ưu hoá thời gian - bộ nhớ.

```
1.  Y_start = y
2.  Backup = false
3.  While  g(y) ≠ y_start   do
4.          if   y = z_j với mỗi j nào đó  and not  backup then
5.                  y = g^-T(z_j)
6.                  backup = true
          else
7.  y = g(y)
8.  K = y
```

d/ Hãy mô tả thuật toán giải mã để xây dựng một tập Z mong muốn trong thời gian 0(NT) không dùng một mảng có kích thước N.

bài 7: Hãy tính các xác suất của đặc trưng 3 vòng sau:

$L_0' = 00200008_{16}$ $R_0' = 00000400_{16}$

$L_1' = 00000400_{16}$ $R_1' = 00000000_{16}$ p = ?

$L_2' = 00000000_{16}$ $R_2' = 00000400_{16}$ p = ?

$L_3' = 00000400_{16}$ $R_3' = 00200008_{16}$ p = ?

Bài 8: Sau đây là một phép tấn công vi sai đối với DES 4 vòng sử dụng đặc trưng sau (đây là một trường hợp đặc biệt của đặc trưng được trình bày ở hình 3.10).

$L_0' = 20000000_{16}$ $R_0' = 00000000_{16}$

$L_1' = 00000000_{16}$ $R_1' = 20000000_{16}$ p = 1

a/ Giả sử rằng thuật toán sau (được nêu ở hình 3.16) được dùng để tính các tập $test_2,. . .,test_8$. Hãy chứng tỏ rằng $J_j \in test_j$ với $2 \le j \le 8$.

Hình 3.16. Tấn công DC lên DES 4 vòng.

Vào : L_0R_0, $L_0^*R_0^*$, L_3R_3 và $L_3^*R_3^*$, trong đó

$L_0' = 10000000_{16}$ và $R_0' = 00000000_{16}$

1. Tính $C' = P^{-1}(R_4')$
2. Tính $E = E(L_4)$ và $E^* = E^*(L_4^*)$
3. **For** j =2 **to** 8 **do**

   Tính $testj(E_j,E_j^*,C_j')$

b/ Với các cặp bản rõ - mã sau, hãy xác định các bít khoá trong $J_2,...,J_8$.

Bản rõ	Bản mã
18493AC485B8D9A0 E332151312A18B4F 38493AC485B8D9A0 87391C27E5282161	
482765DDD7009123 B5DDD833D82D1D1 682765DDD7009123 81F4B92BD94B6FD8	
ABCD098733731FF1 93A4B42F62EA59E4 8BCD098733731FF1 ABA494072BF411E5	
13578642AAEDCB FDEB526275FB9D94 33578642AAFFEDCB CC8F72AAE685FDB1	

c/ Hãy tính toàn bộ khoá (14 bít khoá còn lại cần phải xác định có thể tìm theo phương pháp tìm kiếm vét cạn).

BÀI TẬP CHƯƠNG 4 + 5

Bài 1: Cho (p, q, e) = (19, 11, 23) là các thông số trong hệ mật mã RSA.

a. Hãy trình bày quá trình giải mã bản mã: y= 50.

b. Hãy mã bản rõ: x=29

Bài 2: Cho hệ mật mã RSA biết **(p, q, e) = (23, 19, 29)**

a. Hãy trình bày quá trình giải mã bản mã: **y= 35.**

b. Hãy mã bản rõ: x=43

Bài 3: Cho hệ mật RSA, biết **(p,q,e) = (29,13,23)**

a. Hãy trình bày quá trình giải mã bản mã: **y=43;**

b. Hãy mã bản rõ: x=23

Bài 4: Cho **(p,q,e) = (23, 31, 17)**

a. Tìm khoá công khai và khoá bí mật của hệ mật mã RSA.

b. Trình bày quá trình mã bản tin: x=27.

c. Giải mã y=31

Bài 5: Cho khoá công khai của hệ mật RSA là **(p,q,e)=(31,13,19)**

a. Hãy trình bày quá trình giải mã bản mã **y=36**

b. Hãy trình bày quá trình mã : x= 29

Bài 6: Cho hệ mật mã RSA biết **(p,q,e) = (17,31,19)**

a. Tìm khoá công khai và khoá bí mật của hệ mật RSA.

b. Trình bày quá trình mã bản rõ: **x=43.**

c. Trình bày qúa trình giải mã: y=37

Bài 7: Cho hệ mật mã RSA biết **(p,q,e) = (17,41,19)**

a. Hãy trình bày quá trình giải mã bản mã: **y=51**

b. Trình bày qúa trình mã bản rõ: x=37

Bài 8: Cho hệ mật mã balo-MHK biết S=(1, 3, 8, 17, 35),p=79, a=19.

a. Tìm khoá công khai và khoá bí mật của Mã MHK.

b. Hãy mã bản rõ: **x=25**

Bài 9: Cho hệ mật mã balo- MHK biết S=(1, 3, 8, 17, 35), p=83,a =23.

a. Hãy giải mã bản mã: **y=106.**

b. Hãy mã bản rõ: x=1 0101

Bài 10: Cho S=(1, 3, 8, 17, 35), p= 79, a =25 của hệ mật mã balo- MHK

a. Tìm khoá công khai và khoá bí mật.

b. Trình bày quá trình mã bản rõ: **x=’Z’**

Bài 11: Cho S=(1, 3, 7, 15, 32), p=83, a=31 của hệ mật mã balo - MHK

Hãy trình bày quá trình giải mã: **y=115**.

Bài 12: Cho S=(1, 3, 7, 15, 32), p=97, a=411 của hệ mật mã balo- MHK

a.Tìm khoá công khai và khoá bí mật.

b.Hãy mã bản rõ: **x=’you’**

Bài 13: Cho S=(1, 3, 7, 15, 32), p=97, a=31 của hệ mật mã balo- MHK

a.Giải mã bản mã: **y=146.**

b. Mã bản rõ x= $1010101100101000_{(2)}$

Bài 14: Cho S=(1, 3, 8, 17, 35), p=83, a=29 của hệ mật mã balo- MHK

a. Quá trình giải mã bản mã: **y=192**.

b. Trình bày qúa trình mã x=$111100111010101_{(2)}$

Bài 15: Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA.

Người A có khóa (p, q, e) = (17,31,23)

Người B có khóa (p,q,e) = (31,29,19)

Trình bày cách A mã và kí lên bức điện m =29.

Bài 16: Cho (p, q, e) = (13, 41, 19) là các thông số trong sơ đồ kí số RSA.

a. Trình bày quá trình kí bức điện: x=29.

b. Hãy kiểm tra chữ kí sau (x,y)=(18,72).

Bài 17: Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA.

Người A có khóa (p, q, e) = (17,31,23)

Người B có khóa (p,q,e) = (19,53,31)

A kí và mã lên bức điện gửi cho B. B nhận được nội dung sau (39,19). B phải làm gì để đọc được nội dung trên?

Bài 18: Người A và người B dùng sơ đồ kí và mã là hệ mã RSA.

Người A có khóa (p,q,e) = (17, 31, 29)

Người B có khóa (p,q,e) = (41, 23, 19)

Giả sử A kí sau đó mã gửi cho B. B nhận được thông điệp từ A gửi đến là (10,18)

Hãy trình bày quá trình B giải mã và kiểm tra chữ kí.

Bài 19: Người A có (p,q,e)= (29,17, 31), B có (p,q,e)=(41,31,43) là các thông số của hệ mật RSA. y=sig(x), (x,y)= (23,71). Hỏi chữ kí trên là do ai kí?

Bài 20: Người A và người B dùng sơ đồ kí và mã là hệ mã RSA.

Người A có khóa (p,q,e) = (17, 23, 29)

Người B có khóa (p,q,e) = (31, 19, 23)

Trình bày cách A kí và mã lên bức điên x= 31.

Bài 21: Người A có (p,q,e)= (17,19, 31), B có (p,q,e)=(23,31,49) là các thông số của giải thuật RSA.

B kí và mã lên bức điện và gửi cho A. Giả sử A nhận được nội dung mã như sau: (27,78). A phải làm gì để đọc nội dung nhận được

Bài 22: Người A và người B dùng sơ đồ kí và mã là hệ mã RSA.

Người A có khóa (p,q,e) = (17, 31, 23)

Người B có khóa (p,q,e) = (41, 29, 13)

Trình bày cách A kí và mã lên bức điên x= 19.

Bài 23: Người A có (p,q,e)= (23,17, 31), B có (p,q,e)=(29,31,49) là các thông số của giải thuật RSA.

Hãy trình bày cách B kí và mã lên bức điện x= 27

Bài 24: Cho (p, q, e) = (29, 19, 23) là các thông số trong s ơ đ ồ k í RSA.

a.Trình bày quá trình kí lên bức điện x = 50.

b.Kiểm tra xem chữ kí (x,y)=(19, 14) có hợp lệ không trong đó y=sig(x)

Bài 25: Cho hệ mật mã Elgamal biết **(p, α, a, k) = (37, 2, 17, 13)**

Hãy kí lên bức điện: x=10

Bài 26: Cho hệ mật mã Elgamal biết **(p, α, a, k) = (31, 2, 15, 17)**

Hãy trình bày quá trình kí lên bức điện: x**= 13.**

Bài 27: Cho sơ đồ ký số Elgamal biết **(p, α, a) = (37, 2, 17)**

Hãy trình bày quá trình xác minh chữ ký: (x, γ, δ) = (10, 29, 15)

Bài 28: Cho hệ mật mã Elgamal biết **(p, α, a, k) = (37, 2, 17, 13)**

Hãy trình bày quá trình ký lên bản tin : x=10

Bài 29: Cho sơ đồ ký số Elgamal biết **(p, α, a) = (29, 2, 17)**

Hãy trình bày quá trình xác minh chữ ký: (x, γ, δ) = (10, 19, 15)

Bài 30: Cho sơ đồ ký số Elgamal biết **(p, α, a, k) = (29, 2, 15, 11)**

Trình bày quá trình ký lên bản tin: x=13

Bài 31: Hãy dùng thuật toán Euclide mỡ rộng để tính các phần tử nghịch đảo rau:

a) 17^{-1} mod 101

b) 357^{-1} mod 1234

c) 3125^{-1} mod 9987

Bài 32: Giải hệ phương trình đồng dư sau:

$x \equiv 12 \pmod{25}$

$x \equiv 9 \pmod{26}$

$x \equiv 23 \pmod{27}$

4.1. Giải hệ phương trình đồng dư sau

$13x \equiv 4 \pmod{99}$

$15x \equiv 56 \pmod{101}$

Gợi ý: trước tiên hãy dùng thuật toán Euclide mỡ rông rồi áp dụng định lý phần dư của China.

Bài 33: Giả sử I thực hiên sơ đồ Elgamal với p=31847, α =5,và β =26379. Hãy viết phương trìng thực hiện công việc sau:

a) Xác minh chữ kí (20679,11082) trên bức điện x=20543

b) Xác định số mũ mật a bằng cách dùng thuật toán tối ưu hoá thời gian - bộ nhớ của Shark, sau dó xác định giá trị k ngẫu nhiên dùng trong việc kí lên bức điện x.

Bài 34: Chứng minh rằng phương pháp giả mạo thứ hai trên sơ đồ Elgamal (mô tả trong mục 6.2) cũng tạo ra chữ kí thoả mãn điều kiện xác minh.

Bài 35: Giả thiết Bob đang dùng sơ dồ Elgamal, anh ta kí hai bức điện x_1 và x_2 bằng chữ kí (γ, δ_1) và (γ, δ_2) tương ứng (giá trị này của γ giống nhau trong cả hai chữ kí). Cũng giả sử UCLN $(\gamma_1-\gamma_2, p-1)=1$.

a) Hãy cho biết cách tính k hiệu quả khi biết thông tin này

b) Hãy mô tả cách sơ đồ chữ kí có thể bị phá.

c) Giả sử p=31847, α =5, và β =25703. Tính k và a khi cho trước chữ kí (2397 2,31396) vói bức điện x=8990 và chữ kí (23972, 20481 trên bứ c điện x=31415)