An toàn và bảo mật thông tin

Chương 1. Các khái niệm cơ sở và hệ mã cổ điển

Câu 1: Phân biệt các thuật ngữ cryptography, cryptanalysis, cryptology. "Khoa học mật mã" tương ứng với từ tiếng anh nào?

Trả lời:

- cryptography(sinh, chế mật mã): nghiên cứu các kỹ thuật toán học nhằm cung cấp các công cụ hay dịch vụ đảm bảo an toàn thông tin.
- cryptanalysis(phá giải mã): nghiên cứu các ký thuật toán học nhằm phục vụ phân tích mật mã và tạo ra các đoạn mã giả nhằm đánh lừa bên nhận.
- cryptology(ngành mật mã): thường được quan niệm là sự kết hợp của hai ngành cryptography và cryptanalysis.

Khoa học mật mã tương ứng với từ :cryptography

Câu 2: Trong thời kỹ nào kỹ thuật mật mã chưa được coi là ngành khoa học? tại sao?

Trả lời: Thời kỳ tính từ thượng cổ cho đến năm 1949 kỹ thuật mật mã chưa được coi là ngành khoa học. Vì trong thời kỹ này ngành này còn mang nhiều tính thủ công, kỹ thuật hơn là tính khoa học.

Câu 3: Hãy phân biệt các hệ mã thông thường(Morse Code, ASCII code) với các hệ mật mã?

Trả lời:

- Hệ mã thông thường biến đổi thông tin đầu vào mã không dùng khóa còn đối với hệ mật mã sử dụng thêm khóa trong quá trình biến đổi đầu vào.
- Đối với các hệ mã thông thương(Morse Code, ASCII code) một đoạn văn bản sau A sau khi mã hóa thành văn bản B thì bất kỳ một người nào iết văn bản đó được mã hóa bằng thuật toán nào(ví dụ: Morse Code, ASCII code) đều có thể từ văn bản B mà tìm ra văn bản A. Còn đối với hệ mật mã một người mặc dù có văn bản B và biết thuật toán mã hóa nhưng nếu không biết khóa sẽ không thể suy ra được văn bản A.

Ví dụ:

- Đối với hệ mã ASCII Code: Nếu một người nhận được đoạn văn bản `97 110 32 116 111 97 110 32 98 97 111 32 109 97 116 32 116 104 111 110 103 32 116 105 110` người đó dễ dàng giải mã được chuỗi thông tin `an toan bao mat thong tin` .
- Đối vơi hệ mật mã afine cipher: Nếu một người nhận được đoạn văn bản `wj pkwj xwk iwp pdkjc pej` nếu người đó không biết khóa là cặp (1,4) thì người đó sẽ không thể giải mã ra chuỗi tin ban đầu là `an toan bao mat thong tin` mặc dù người đó biết đoạn mã được mã hóa bằng hệ mã afine cipher.

Câu 4: Hãy phân tích ý nghĩa của luật Kirchoff để thấy tại sao hệ mật mã hiện đại không chấp nhận quan điểm che giấu thuật toán mật mã:

Trả lời:

Luật Kirchoff khẳng định toàn bộ cơ chế sinh mã và giải mã ngoài trừ thông tin về khóa là không bí mật với kẻ thù. Các hệ mật mã hiện đại không chấp nhận quan điểm che giấu thuật toán mật mã vì thuật toán mã hóa giải mã được che giấu thì nếu muốn trả đổi thông tin với một người nào ta phải chi người đó biết thuật toán giải mã và khóa việc che giấu thuật toán làm cho việc trao đổi trở nên phức tạp hơn nếu số lượng người trao đổi rất nhiều. Hơn nữa nếu sử dụng hệ mã hóa công khai thì khi một người muốn gửi thông tin cho mình họ không biết thuật toán thì điều đó là vô nghĩa. Nếu ta chỉ công khai khóa và không công khai thuật toán thì không còn ý nghĩa của hệ mật mã này.

Câu 5: Phân tích nhược điểm chính của hệ mã đối xứng(SKC):

Trả lời: Nhược điểm chính của hệ mã đối xứng:

- Trong hệ mã đối xứng vai trò của hai phía là như nhau và có thể đổi vai trò. Chính vì vậy về sau nếu có mâu thuẫn sẽ không thể xác định được người mã hóa hoặc giải mã.
- Trong hệ mã đối xứng nếu hai người muốn trao đổi thì họ phải có một khóa bí mật chỉ hai người đó biết. Nếu một người muốn trao đổi với n người thì họ phải lưu n khóa để có thể giao tiếp với n người đó. Trong một hệ thống có n người thì số lượng khóa cần tạo và quản lý là n(n-1)/2.
- Trên cơ sở mã đối xứng ta không thể xây dựng khái niệm chữ ký điện tử và dịch vụ không thể phủ nhận được.
- Vấn đề khó khăn trong xác lập và phân phối khóa giữa hai bên thường ở xa nhau và chỉ có thể liên lạc qua một kênh truyền thông thường không thể trách nghe trộm.

Câu 6: Ưu điểm chính của mã công khai với mã mật:

Trả lời:

- Hệ mã công khai đơn giản hóa việc tạo,quản lý khóa: cụ thể mỗi người chỉ cần quản lý một cặp khóa là có thể trao đổi với tất cả mọi người khác.
- Hệ mã công khai giúp phân biệt được người mã hóa và giải mã.
- Cho phép xây dựng chữ ký điện tử cũng như dịch vụ không thể phủ nhận được.

Câu 7,8,9,10: Lý thuyết trong sách giáo khoa.

Câu 11 : Tìm số lượng khóa thực sử được dùng với khóa nhân tính. Hãy lập luận chi tiết:

Trả lời: Số lượng khóa thực sử được sử dụng với khóa nhân tính là 12 vì những khóa khác sẽ không tạo ra ánh xạ một một giữa bản chữ gốc sang bản thế.

Ví dụ: nếu khóa là 2 thì sẽ có hai kỹ tự b và c có thể cùng được mã hóa thành ký tự c. Như vậy việc giải mã sẽ gặp khó khăn.

Câu 12: Hãy tìm số khóa khả thi affine cipher. Lập luận chi tiết.

Trả lời. Số lượng khóa khả thi của affine cipher là 12x26=312. Giải thích: Hệ mã afine cipher là sự kết hợp của hai hệ mã nhân tính và cộng tính. Với hệ mã nhân tính ta có 12 khóa khả thi, hệ mã công tính ta có 26 khóa khả thi nên số khóa khả thi của hệ mã affine cipher là tích của 12x26.

Câu 13: Tại sao không thể nói mọi khóa của hệ khóa một bảng thế là an toàn như nhau?

Trả lời: Không thể nói mọi khóa của mật mã một bảng thế là an toàn như nhau vì có khóa giúp che giấu thông tin có khóa không giúp che giấu thông tin. Ví dụ như khóa a b c d A B C D không có tác dụng che giấu thông tin nên sẽ không an toàn bằng các khóa khác.

Câu 14: Tại sao không thể sử dụng quan hệ thứ tự trong cùng một nhóm tần suất để phân tích giải mã. Giải thích qua ví dụ.

Trả lời: Không thể dùng quan hệ thứ tự trong cùng một nhóm tần suất để giải mã vì độ chênh lệch tần suất giữa các ký tự trong cùng một nhóm tần suất là không lớn nên sẽ không đúng trong mọi văn bản.

Ví dụ: ta có văn bản : `this is a shit` ta mã hóa sử dụng khóa: t->A h->B i->C s->D a->E

sau khi mã hóa ta sẽ được đoạn mã: ABCD CD E DBCA ta thấy xác suất các từ trong sâu này đều thuộc nhóm 2 gồm các từ với tần xuất trong văn bản tiếng anh được sắp xếp giảm dần là :

`t,a,o,i,s,h,r`. Nếu ta tính xác suất của sâu ta sẽ thấy p(A)=2/11,p(B)=2/11,p(C)=3/11,p(D)=3/11,p(E)=1/11. Nếu ta sử dụng quan hệ thứ tự trong nhóm 2 để giải mã ta thấy hai ký tự trong bản mã là C và D có xác xuất lớn nhất sẽ là mã hóa của `t` trong nhóm 2 như vậy là sai vì thực tế `t` là mã hóa của A. do vậy không thể sử dụng quan hệ tần xuất trong cùng một nhóm.

Câu 15 : Tại sao nói quy luật tần suất không đông đều chi phối mạnh mẽ hơn ở các từ có độ dài lớn hơn.

Trả lời: Ta thấy với các từ dài thì giữa các ký tự trong từ sẽ có quan hệ ràng buộc lớn hơn nên việc phân bố tần suất sẽ không đồng đều hơn. Ví dụ: ví dụ như nếu ta xét từ có hai âm tiết như oX thì X có thể nhận một trong 4 giá trị `n,f,r,x` còn nếu với một từ có nhiều âm tiết như mXasure thì X chỉ có thể nhận một giá trị `e` do vậy các từ có chưa nhiều âm tiết sẽ khiến cho một số từ có thể ghép với nhiều từ khác có xác xuất cao hơn.

Câu 16: Giải tới cùng ví dụ 1.8:

Câu 17: Hãy giải thích tại sao đồ tần suất trong mật mã đồng âm lại bằng phẳng và tại sao lại có dư thừa?

Trả lời: Trong mật mã đồng âm một ký tự ở bản góc có thể được mã hóa thành các ký tự khác nhau trong bản mã(các ký tự này gọi là đồng âm). Mà số lượng các ký đồng âm với một ký tự được xếp sao cho từ nào có tần suất xuất hiện nhiều sẽ có số lượng từ đồng âm nhiều hơn. Chính vì điều đó làm cho đồ thị tần suất phân bố đều hơn. Chình vì một ký tự trong văn bản gốc có thể được mã hóa thành các ký tự khác nhau trong bản mã nên số số lượng ký tự trong bản mã phải nhiều hơn trong bản gốc dẫn đến dư thừa.

Câu 18: Hãy so sánh IC của một bản rõ M và IC của một bản mã ngẫu nhiên R có cùng độ dài?

Trả lời : Ta biết rằng IC của một văn bản phụ thuộc vào hai yếu tố:

- Độ dài
- Tần suất xuất hiện các ký tự

Giữa bản rõ M và bản mã R theo đầu bài có cùng độ dài nên IC của hai văn bản sẽ chỉ khác nhau nếu tần xuất xuất hiện các ký tự khác nhau.

Nếu ta sử dụng các hệ mã có bảo toàn tần xuất các ký tự thì giá trị IC sẽ bằng nhau ngược lại sẽ khác nhau.

Chương 2: Mật mã khối và mã khóa đối xứng

Câu 1: Confusion và diffusion là gì? Nguyên lý tạo ra chúng có khác nhau?

Trả lời:

- Confusion(hỗn loạn, rắc rối): Sự phụ thuộc của bản rõ và bản mã phải thực sự phức tạp để gây rắc rối hỗn loạn cho kẻ thù có ý định phân tích tìm quy luật để phá mã. Quan hệ hàm số giữa mã-tin là hàm phi tuyến.
- Diffusion(khuếch tán): Làm khuếch tán những mẫu văn bản mang đặc tính thống kê(gây ra do sự dư thừa ngôn ngữ) lẫn vào toàn bộ văn bản. Từ đó gây khó khăn cho kẻ thù trong việc dò phá mã trên cơ sở thống kê cá mẫu lặp lại cao. Sự thay đổi một bit trong một khối bản rõ phải dẫn đến sự thay đổi hoàn toàn trong khối mã tạo ra.

Nguyên lý tạo ra sự confusion là sử dụng phép thay thế trong khi đó diffusion được tạo ra băng phép hoán vị. Toàn bộ sơ đồ biến đổi mật mã sẽ là một lưới các biến đổi thây thế-hoán vị.

Câu 2: Cấu trúc sử dụng vòng lặp Feistel là gì ?Tại sao lại cần nhiều vòng lặp? Sự thực hiện các vòng lặp có hoàn toàn giống nhau?

Trả lời: Chúng ta cần sử dụng nhiều vòng lặp để tạo ra tính confusion và diffusion. Các vòng lặp được thực hiện với cùng một hàm f nhưng với các tham số khác nhau. Theo đó đầu vào của một vòng lặp là đầu ra của vòng lặp trước và một khóa con.

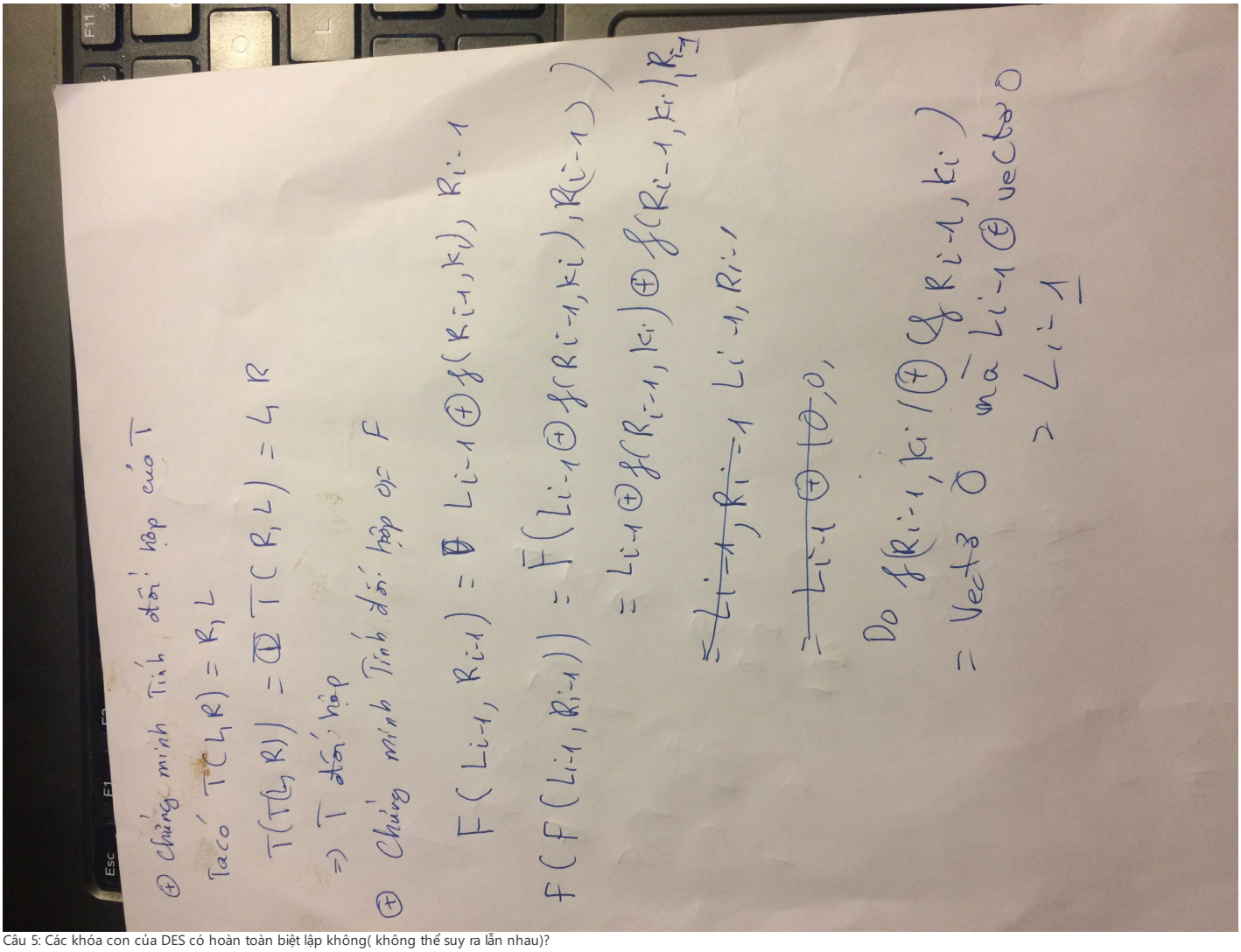
Câu 3: Tính đối hợp là gì? Tại sao cần tính đối hợp trong thiết kế DES?

Trả lời:

- Tính đổi hợp của hàm f tức là hàm f bằng hàm ngược của nó: f=f^-1 hay f(f(x))=x;
- Cần tính đối hợp trong thiết kế DES để có thể giải mã DES. DES(DES^-1(x))=x

Câu 4: Trong thuật toán DES chứng minh tính đối hợp của T và F đồng thơi chỉ rõ tại sao DES(DES^-1(x))=x với mọi x là chuỗi nhị phân 64 bit.

Trả lời:



Câu 5: Các khóa con của DES có hoàn toàn biệt lập không(không thể suy ra lẫn nhau)?

Trả lời:Các khóa con của DES không hoàn toàn biệt lập(có thể suy ra nhau). Ví dụ nếu ta biết khóa con 1 ta sẽ có thể tách để tìm ra đầu vào của khóa con 1 từ đó có thể tìm được khóa con 2 theo sơ đồ sinh khóa con của DES.

Câu 6: Các S-Box có tính chất gì đặc biệt? Có thể ra bao nhiêu S-box nếu không quan tâm tới các tính chất đó?

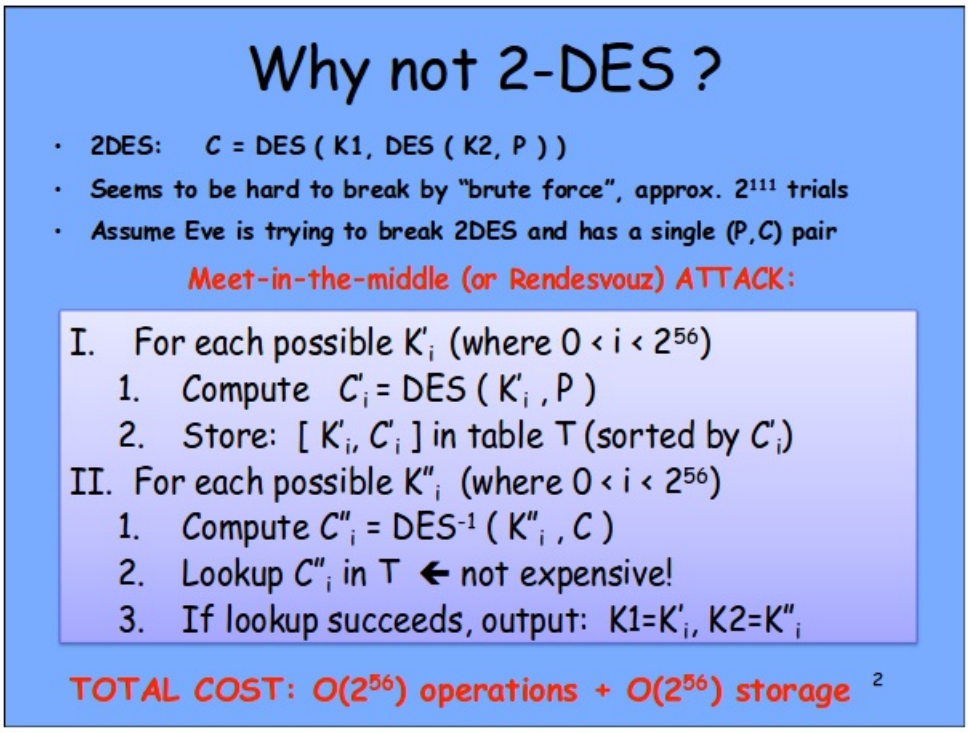
Trả lời:

Các tính chất đặc biệt của S-Box:

- Các bit vào luôn phụ thuộc không tuyến tính và các bit ra.
- Sửa đổi một bit vào làm thay đổi ít nhất hai bit ra.
- Khi một bit vào thay đổi và 5 bit còn lại cho thay đổi thì S-Box thể hiện ra một tính gọi là phân bố đồng nhất: So sánh bit 0 và bit 1 pử đầu ta luôn ở mức cân bằng. Tính chất này khiến cho việc phân tích theo lý thuyết thống kê để tìm cách phá giải S-Box trở nên vô nghĩa.

Nếu không kể đến các tính chất trên có thể xây dựng được số S-Box là :16^(16*4)

Câu 7: Hãy giải thích chiều dài thực sự của 2-DES là 57:



Trả lời: Ta xét khóa DES(k2,P) ta thất k2 có 2 mũ 56 khả năng. Với mỗi khả năng của k2 ta tính giá C1 là bản mã sau khi đã mã hóa P với k2 lưu cặp giá trị k2,x1 này vào một bảng T.

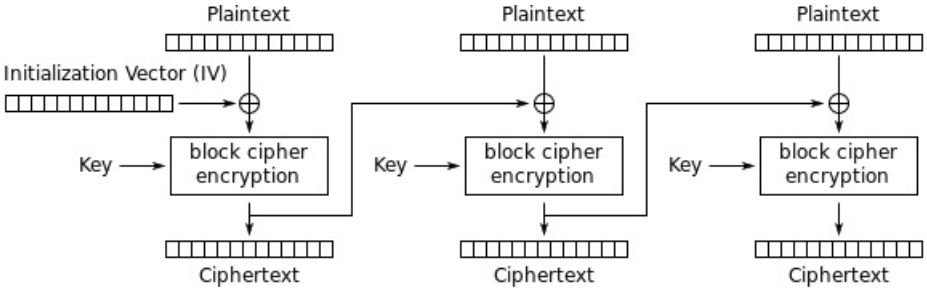
Bây giờ xét khóa C=DES(k1,c1') với C1 là các giá trị tính được ở khóa trên.

Ta sẽ tiến hành rõ để tìm k1 bằng cách giải mã dựa vào công thức c1'=DES-1(k1,C) . Với mỗi giá trị c1' ta sẽ so sánh với giá trị c1 trong bảng T nếu tìm thấy thì cặp khóa đó là k1 và khóa k2 là khóa tương ứng với c1 trong bảng T.

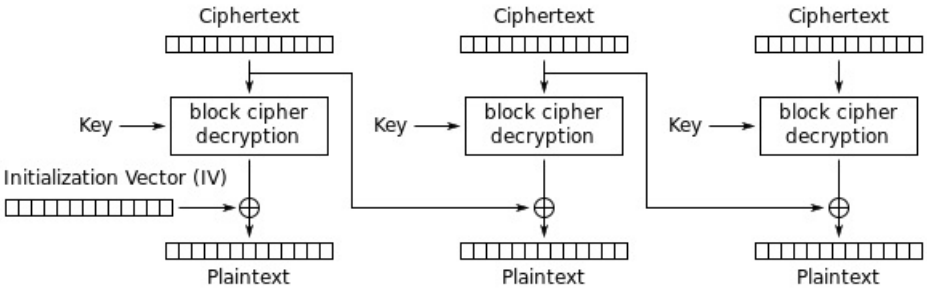
Câu 8: Hãy vẽ sơ đồ giải mã cho CBC,CFB

Trả lời:

Sơ đồ mã hóa và giải mã CBC:

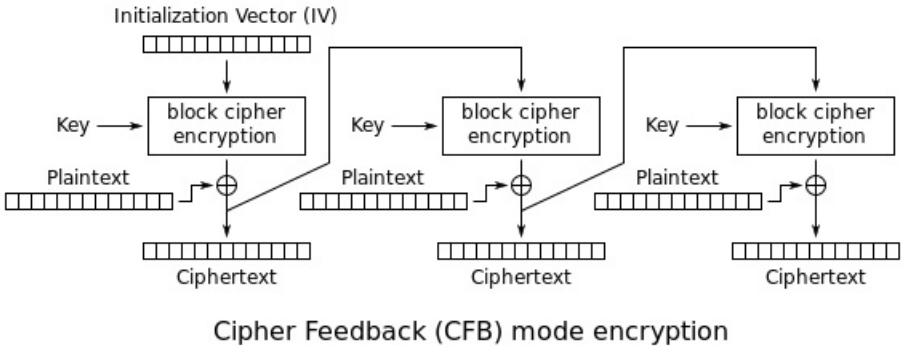


Cipher Block Chaining (CBC) mode encryption

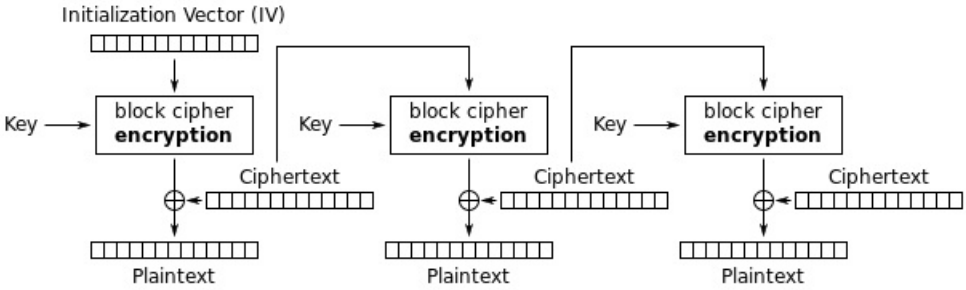


Cipher Block Chaining (CBC) mode decryption

Sơ đồ mã hóa và giải mã CFC:



Cipher Feedback (CFB) mode encryption



Cipher Feedback (CFB) mode decryption

Chương 3:Hệ mật mã khóa công khai

Câu 1:Lập luận cụ thể chứng minh bài toán đóng thùng với một vector mang là vector siêu tăng sẽ luôn là dễ nếu có nghiệm?

Trả lời: Với bài toàn đóng thúng ta sẽ dễ dàng tìm được lời giải nếu tồn tại nếu tồn tại lời giải ta chỉ cần duyệt từ phần từ cuối vector đến đầu vector nếu giá trị đó nhỏ hơn giá trị thùng có thể chứa ta sẽ thêm giá trị đó vào thùng và trừ đi giá trị đó khỏi giá trị thùng có thể chứa. Nếu giá trị đang xét lớn hơn giá trị còn chứa được của thùng ta sẽ kết thúc thuật toán. Vậy ta dễ dàng giải được nếu tồn tại lời giải với độ phức tạp O(n).

Câu 2: Chọn một số ngẫu nhiên M trong khoảng từ 5-20 thực hiện các công việc sau:

```
a) Hãy xây dựng một vector siêu tăng có 5 thành phần trong đó có một thành phần đúng bằng M và số cuối
cùng là 60.Cho biết các phép tính thể hiện tính tăng của dãy số.
b) Dựa vào dãy trên xây dựng hệ mã công khai theo phương pháp mekle-hellman.
c) Viết M dưới dạng nhị phân gọi X là 5 bit cuối cùng. Sử dụng hệ mã vừa tạo để tĩnh mã Y từ X.
d) Với Y vừa tìm được cho biết cách giải mã để tìm X.
```

Trả lời: a) Chọn M=10. Vector siêu tăng v=(3,4,10,20,60) Chứng minh tính siêu tăng: 4>3; 10>4+3;20>10+4+3;60>3+4+10+20

b) Xây dựng hệ mã công khai dựa vào vector (3,4,10,20,60) chọn m=120, chon w(omega)=23 => a=w.v(mod m)=(69,92,110,100,60)

Hệ mã sẽ là: Khóa công khai a=(69,92,110,100,60,120) Khóa bí mật là : (v,m,w)=((3,4,10,20,60),120,23);

c) M=01010 Y= sigma(a[i].m[i])=192

d)Giải mã

- Tính w' module nghịch đảo của w(tức là w.w'=1 mod m) w'=47
- Tính Y'=Y.w' (mod m)=24
- Ta có Y'=v.M. Tìm M: 24-20=4;4-4=0 => M=(01010)

Câu 3: Trong pha thiết lập tham số của RSA tại sao lại phải chọn hai số nguyên tố p và q có độ lớn xấp xỉ nhau?

Trả lời: Hai số nguyên tố p,q được chọn có độ lớn xấp xỉ nhau để tăng số lần lặp khi kẻ thù muốn tìm ra p,q bằng phương pháp vét cạn. Cụ thể để tìm p,q kẻ thù sẽ cần dùng hai vòng lặp lồng nhau. Nếu hai giá trị đó lệch nhau quá nhiều thì sẽ tìm được p,q tại những vòng lặp đầu tiên.

Ví dụ: để tìm p,q theo duyệt toàn bộ

```
for(i=0;i<n;++i){
    for(j=0;j<n;++j){
        if(i*j==n){
            p=i;
            q=j;
        }
    }
}
```

Nếu 300=pxq=15x16 thì cần 14x300+16=4216 lần lặp nếu 300=2x150 thì cần 1x300+150=450 lần lặp.

Câu 5: Cho p=11,q=17 trong hệ RSA. Chọn ngẫu nhiên 5<=M<=20. Thực hiện các công việc sau:

```
a)Xây dựng khóa công khai và bí mật

b)Tính Mã của Tin M.

c)Nếu sử dụng mã này làm chữ ký xác định chứ ký cho M nói trên.

d) Nếu muốn gửi một thông điệp M vừa có tính bảo mật vừa có tính xác thực cần thực hiện công việc cụ thể
như thế nào?
```

Trả lời: Chọn M=10

a) Xây dựng khóa công khai và bí mật

```
n=pxq=187
m=(p-1)(q-1)=160
chọn e=7
tìm được d=23
Khoá công khai là(7,187)
Khóa mật mà(23,11,17)
```

b) Mã hóa tin M:

gọi Y là bản mã của M: Y=Eza(M)=175

c) Chữ ký chó M

S=DzA(M)=65

d)Nếu muốn thông báo M vừa có tính bảo mắt vừa có tính xác thực cần cần thực hiện các việc như sau:

Giả sử A muốn gửi B thông báo M vừa có tính bảo mật, vừa có tính xác thực. Công việc cần thực hiện là:

B1: A gửi cho B một đoạn tin Y đã được mã hóa bởi khóa bí mật của A sau đó là khóa công khai của B như sơ đồ hình 75.

B2: B nhận được đoạn tin Y đầu tiên sẽ dùng khóa bí mật của mình để giải mã lần 1 thu được đoạn tin đã được mã hóa bởi khóa riêng của A sẽ tiến hành giải mã tiếp theo khóa công khai của A thu được tin ban đầu: Trang 75.

Cụ thể tính xác thực là ở bước A mã hóa bằng khóa bí mật của mình điều này chỉ có thể được thực hiện bởi A nên xác thực đoạn tin đó được mã hóa bởi A vì chỉ A mới biết khóa bí mật của mình. Còn tính mật thì được thực hiên bằng cách mã hóa bằng khóa công khai của B đảm bảo chỉ có B mới có thể giải mã.

Chương 4: Chữ ký điện tử và hàm băm

Câu 1:Phân biệt giữa chữ ký truyền thống và chữ ký điện tử?

Trả lời:

- Chữ ký truyền thống là dấu vết của con người tác động lên bản giấy đã chứa văn bản(in, viết tay). Phần chữ ký và văn bản có sẵn là độc lập không có quan hệ ràng buộc nào.
- Chữ ký điện tử được tao ra một các khách hẳn và phức tạp hơn. Khi có một văn bản nhị phân X người ta phải tạo ra một chữ kỹ là một văn bản nhị phân nhị phân S phụ thuộc hàm vào X, tức là S=f(X). Hơn nữa quan hệ này là bí mật. Nói cách khác trong chữ ký truyền thống thì chữ ký giống nhau với mọi nội dung văn bản còn trong chữ kỹ điện tử là tùy theo nội dung văn bản.

Câu 2: Tại sao nói chữ ký điện tử có hai công dụng: vừa xác thực nội dung văn bản, vừa xác thực danh tính người ký?

Trả lời: Ta nói chữ ký điện tử vừa có công dụng xác thực nội dung vừa xác thực danh tính người ký vì. Chữ ký điện tử tạo ra sự phụ thuộc hàm giữa chữ ký và nội dung văn bản. Khi một người biết được chữ ký theo văn bản người đó chỉ cần dùng khóa công khải để xác minh chữ ký đó xem có phù hợp với nội dung văn bản không như vậy chữ ký có tác dụng xác thực nội dung văn bản. Bên cạnh đó do việc sinh chữ ký đòi hỏi cần khóa bị mật mà chỉ người ký mới biết được nên chữ ký có tác dụng xác thực danh tính người ký.

Câu 4: Với sơ đồ chữ ký đơn giản ban đầu, phân tích khả năng tấn công của kẻ địch theo kiểu lắp ghép nối?

Trả lời: Với sơ đồ chữ ký đơn giản ban đầu nếu ta có một văn bản dài ta cần chia ra các khối và thực hiện ký trên các khối đó. Và chữ ký trên các đoạn văn bản đó là độc lập với nhau. Khi đó các khối có nội dung giống nhau sẽ cùng được ký bởi một chữ ký tạo điều kiện thuận lợi cho kẻ tấn công có thể thống kê và cắt ghép các đoạn văn bản để có thể lợi dung được. Cụ thể khi một người có một văn bản đã được ký khi họ đọc văn bản họ sẽ tìm ra các khối giống nhau sau đó họ sẽ tìm trong chữ ký khối đó và sau đó họ có thể dùng các khối của các văn bản khác nhau để tạo ra văn bản theo ý họ.

Câu 5: Phác thảo một sơ đồ chữ ký chi tiết sử dụng thuật toán RSA và xây dựng một ví dụ minh họa bằng sô?

Trả lời :

ảnh

Câu 6: Trong trường hợp không gian hàm băm là 64 bit khi đem thử một lượng văn bản là 2^32 thì xác suất để tìm thấy đụng độ là bao nhiêu?

Trả lời: ảnh

Câu 7:Hãy nêu cách để tạo ra 2^32 văn bản có nội dung cơ bản là như nhau nhưng giá trị băm chúng hầu hết khác nhau:

Trả lời:

Câu 8: Hai văn bản có nội dung đối nghịch nhau nhưng có giá trị băm trùng nhau.

Trả lời:Băm một giá trị

Chương 5: Quán lý khóa

Câu 1: Trong các giao thức thống nhất khóa SKC giữa hai bên A,B và có sử dụng trung gian C tại sao nên tránh việc để C liên lạc trực tiếp với B.

Trả lời: Không nên để C liên lạc trực tiếp với B vì nếu để C liên lạc trực tiếp với B có vậy B có thể thao túng cả hai phía có thể gặp phải kẻ gian.

Câu 2: Hãy liên hệ việc sử dụng khóa phiên với mô hình tấn công đã học ở chương 1?

Trả lời: Việc sử dụng khóa phiên có thể giúp cho khóa được an toàn trong các mô hình tấn công đã học như: tấn công chỉ biết bản mã, tấn công chỉ biết bản rõ(vì dù có biết bản rõ nhưng sau một thời gian khóa đã thay đổi), tấn công bản rõ chọn sẵn(khóa thay đổi sau mỗi phiên khóa thay đổi nên cũng không có ý nghĩa) tương tự tấn công bản mã chọn sẵn cũng không thể phá giải được.

Câu 3: Trong giao thức needham=schroeder hãy giải thích:

```
a) ý nghĩa của việc sử dụng giá trị ngẫu nhiên r1
b) Bên B có thể xác thực sự tồn tại đúng của bên A bằng giá trị r2 vậy A có thể xác thực được B không?
c)Có cần thiết phải tất cả các bên xác thực lẫn nhau không?
```

Trả lời: a) Giá trị r1 giúp cho A có thể xác thực sự tồn tại đúng của C.

b) B có thể xác thực sự tồn tại đúng của A nhưng A không thể xác thực được sự tồn tại đúng của B.

c) Không cần thiết tất cả các bên cần xác thực lẫn nhau.Nếu A muốn gửi khóa cho B thì A cần xác thực B nhưng B không cần xác thực A vì nếu B là nhận được một gói tin thì với anh ta không có thiệt hại gì cho mình nên anh ta có thể nhận mà không cần xác nhận.

Câu 4: Phân tích vấn đề mà Denning-sacco đưa ra trong xây dựng giao thức chuyển khóa có bên thứ ba tin cậy. Giải pháp cho vấn đề này là như thế nào? Có điểm yếu nào tồn tại không?

Trả lời: Vấn đề denning-sacco đưa ra: Nếu bạn để bị mất một khóa phiên cũ thì một kẻ gian có thể sử dụng nó để mạo danh bạn thành công. Cụ thể do kẻ nham hiểm E đã nghe trộm nói chuyện giữa A và B. Do vậy E có thể phát lại thông điệp thứ ba trong giao thức needham-schroeder mà A đã gửi cho B trong phiên liên lạc tạo khóa phiên ks. Dó đó E có thể dễ dàng sử dung Ks để thách thức B

Giải pháp cho vấn đề này: denning-sacco đã đề cải thiện giao thức needham-schrorder với việc sử dụng nhãn thời gian để hạn chế nghe trộm và phát lại của kẻ địch.

Điểm yếu tồn tại: Vẫn đề chênh lệch đồng hồ giữa B và C.

Câu 5: Vấn đề cụ thể của denning-sacco là vấn đề chênh lệch đồng hồ giữa B và C. Cụ thể nếu trên máy C thời gian là 1491116917 nhưng trên máy B thời gian là 1491216917 và giao thức chỉ cho chêch lệch thời gian 100 thì khi gói tin đến B sẽ không bao giờ được chấp nhận. Giải pháp là sử dụng một đồng hộ chung cho tất cả các máy.

Câu 8:

Theo sơ đò E có thể nhận được khóa eB từ giả mạo B gửi cho A khóa eE sau đó có thể dùng nó để lấy khóa phiên từ đó làm khóa đứng giữa mạo danh hai bên và có thể nghe lén toàn bộ cuộc nói chuyện.

Bonus:

1,cơ chế ngụy trang khóa trong các hệ mã mật

=>

2,chọn(w,m)=1 để làm gì

=>

3,tại sao phải bẻ x thành các đoạn u bit mã RSA

=> vì nếu để xâu có độ dài lớn hơn u bit khi mã hóa qua phép module cho n ta cũng sẽ chỉ được một chuỗi có độ dài lơn nhất là u bit sẽ dẫn đến mất mát thông tin.

4,tại sao khi giao dich trên mạng cần kết hợp DES và RSA

=> Cần sử dụng kết hợp DES và RSA vì RSA có tốc độ chậm hơn rất nhiều so với DES nên thường dùng RSA để khởi tạo khóa cho việc sử dụng DES.

Chương 6 xác thực

Câu 1: Xác thực danh tính khác gì với xác thực thông điệp?

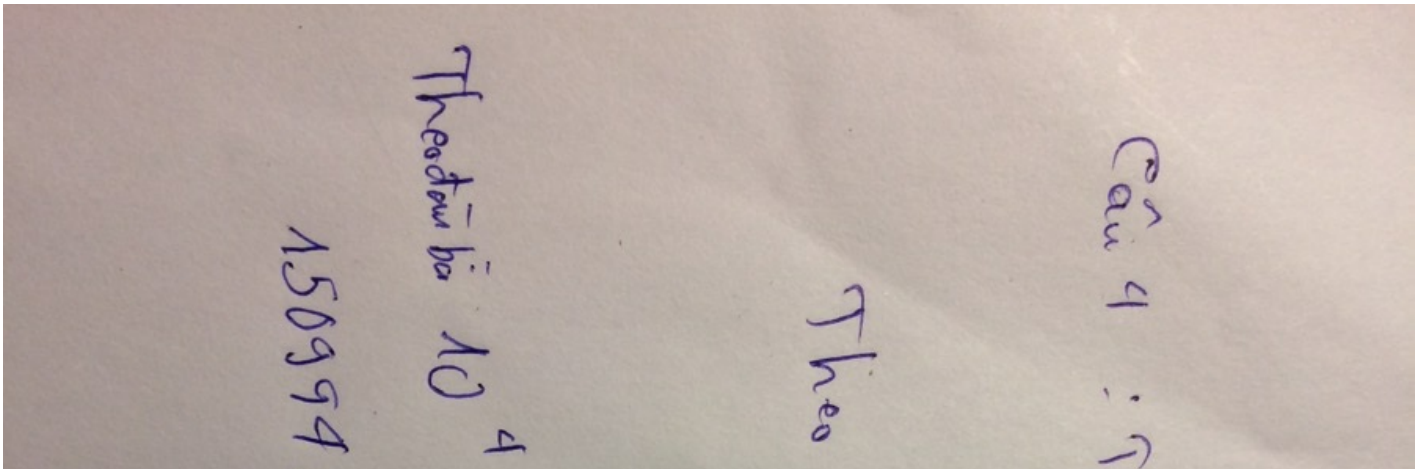
=> Xác thực danh tính là xác thực xem người đó có đúng với danh tính người đó cung cấp không còn xác thực thông điệp là xác thực xem thông điệp đó có phải được gửi có bị thay đổi không.

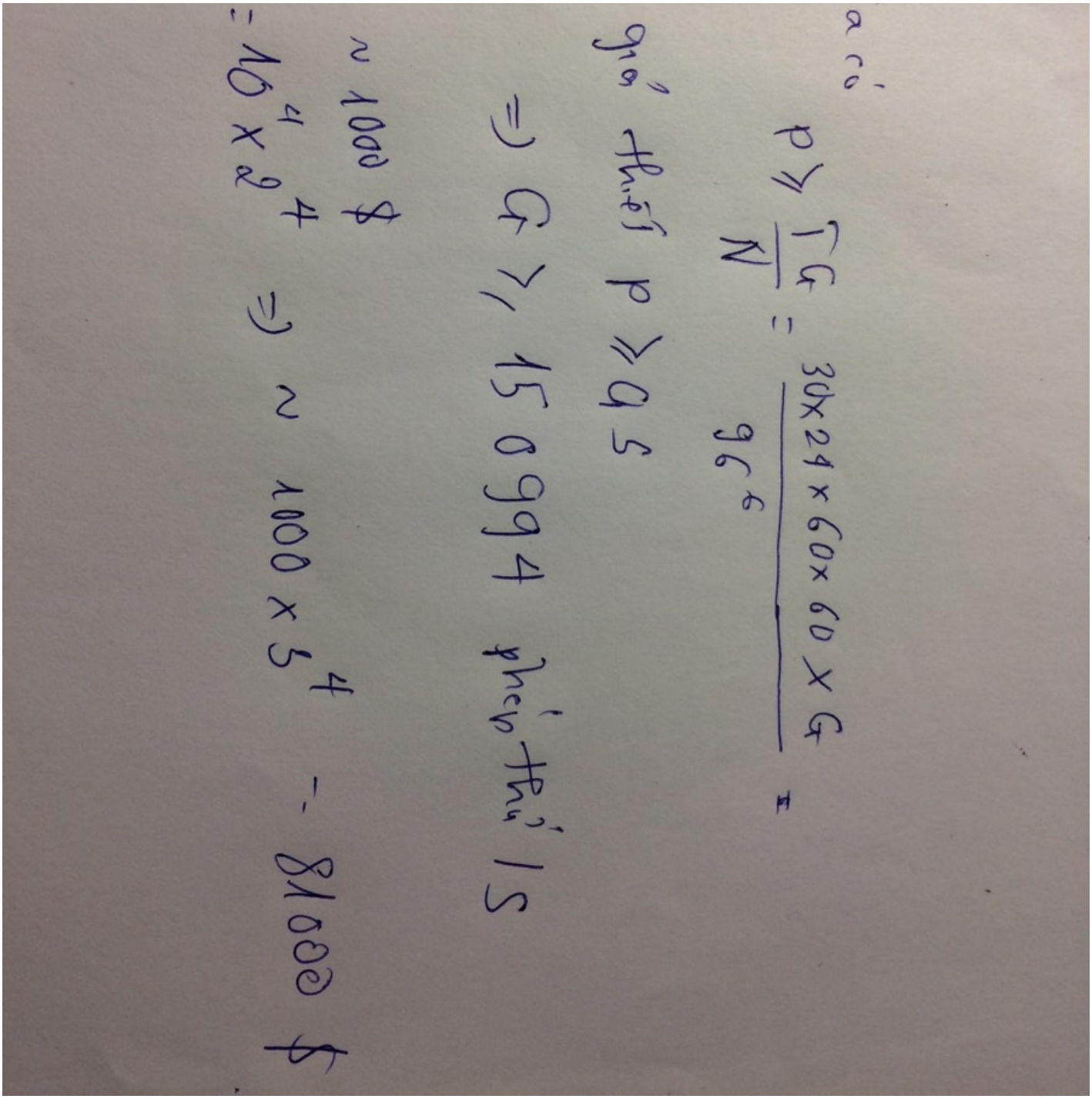
Câu 3:

=> Vì trong một số hệ thống kích thước A và C có thể khác nhau một phần thông tin của giá trị c thuộc C được sử dụng để xác định hàm f thuộc F được dùng cho cặp (a,c) này nên F phải bao gồm một tập các hàm f.

Câu 4:

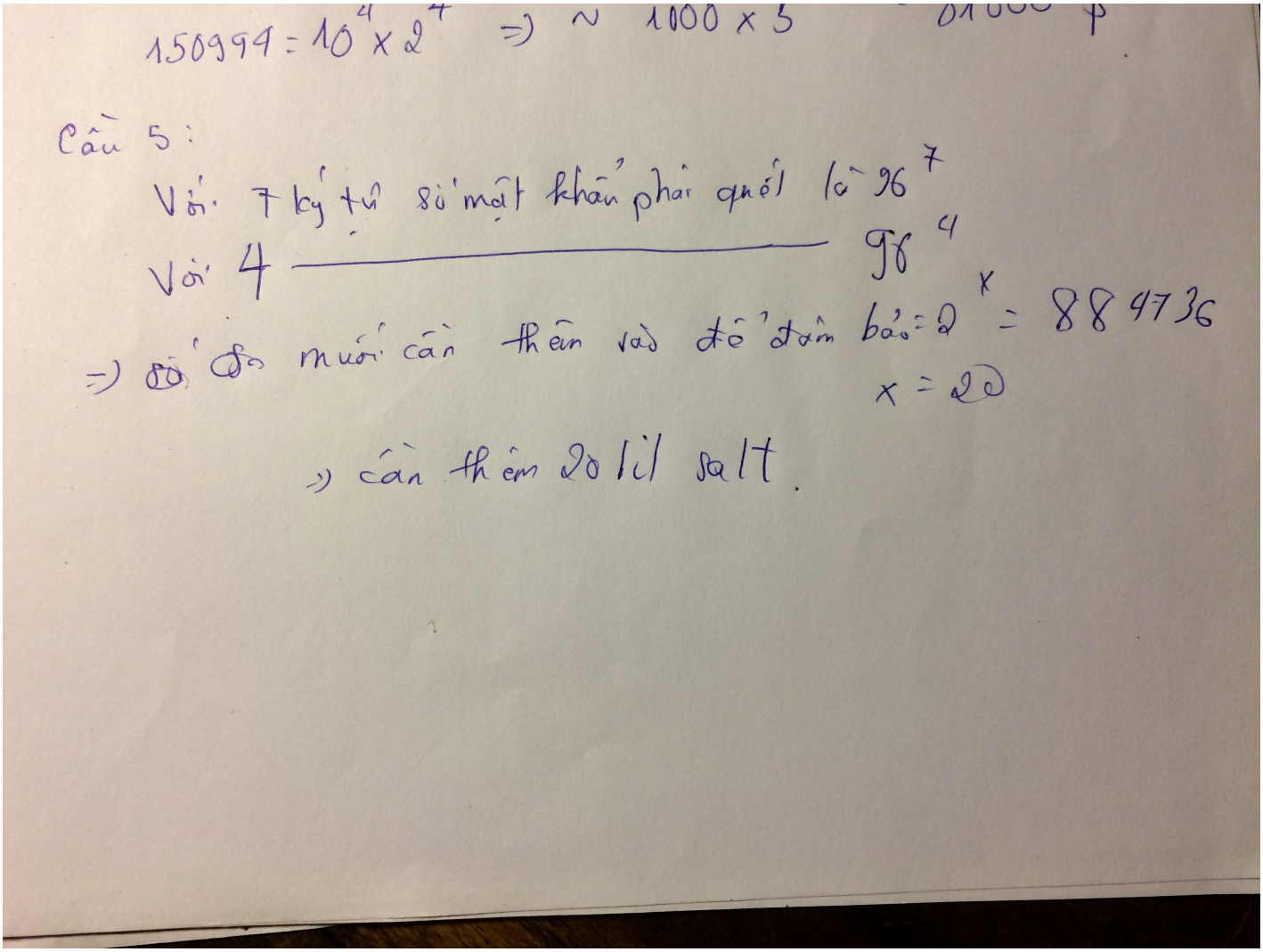
=>





Câu 5:

=>



Câu 7:

=> Không thể tấn công từ điển với hệ thống loại thách thức- đáp ứng vì các thống tin gửi qua lại trên đường truyền thay đổi liên tục(giá trị r) nên không thể tấn công từ điển được.

Câu 8: Capcha cũng là một hình thức xác thực. Capcha được sử dụng để trách các chương trình tấn công theo kiểu từ điển. Do Capcha sinh ra là ngẫu nhiên nên mỗi lần kẻ tấn công muốn thử một mật khẩu trong từ điển họ phải điền lại Capcha. Việc sử dụng Capcha tương tự như kết hợp xác thực bằng mật khẩu và thách thức - đáp lại.