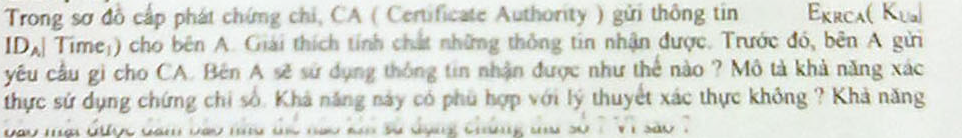
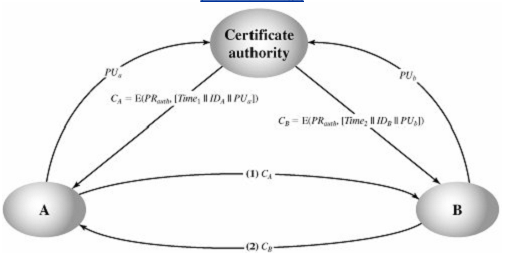
**Câu 1:**





- Giải thích thông tin nhận được:

Thông tin nhận được là một bản tin được mã hóa bởi khóa riêng của CA hay chính là 1 chứng chỉ số. Trong chứng chỉ số này bao gồm:

+ Khóa Public key của A: Kua

+ Ida: định danh của đối tượng A

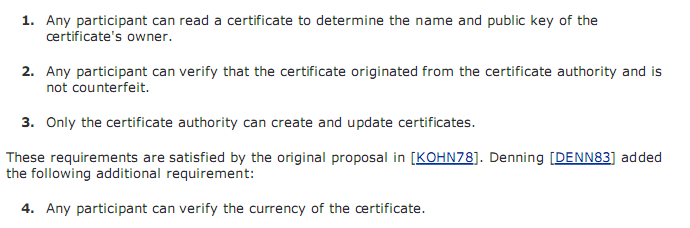
+ Time: nhãn thời gian (dùng để chống tấn công gửi lại - đoạn này ko nhớ rõ lắm, trong vở có ghi 1 ít)

Chứng chỉ này được mã hóa bởi khóa riêng của CA, và chỉ có Public key của CA mới có thể giải mã được chứng chỉ, vì thế nó chứng minh được rằng chứng chỉ này đã được CA “ký”

- Trước đó bên A gửi cho CA bản tin yêu cầu chứng thư trong đó có bao gồm khóa public key của A để CA thực hiện chứng nhận và gửi chứng chỉ số trả lại.

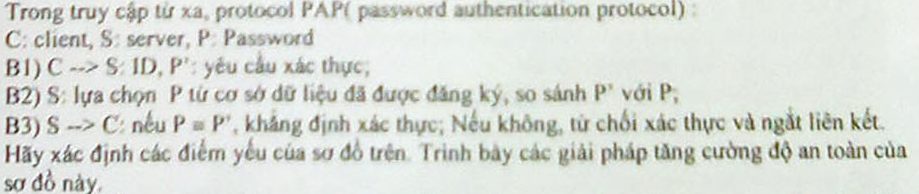
- Bên A sử dụng thông tin nhận được khi phải thực hiện trao đổi với một bên B nào đó. Trước khi các thông tin được truyền giữa hai bên thì A và B trao đổi cho nhau chứng chỉ số của mình. Khi B nhận đc chứng chỉ số của A, nó thực hiện dùng Public key của CA để giải mã chứng chỉ số và lấy được Public key của A. Sau khi đã chắc chắn A đc chứng nhận bởi CA, quá trình trao đổi bắt đầu. B sử dụng public key của A để thực hiện việc mã hóa bản tin...

- khả năng này hoàn toàn phù hợp với lý thuyết xác thực:



( dịch cái này là xong)

**Câu 2:**



Điểm yếu của sơ đồ trên :

- password P’ được gửi đi dưới dạng Plain text

- Không có sự chứng nhận về phía S liệu có đúng là server hay không, và cũng không có sự chứng nhận liệu C có đúng là client hay không

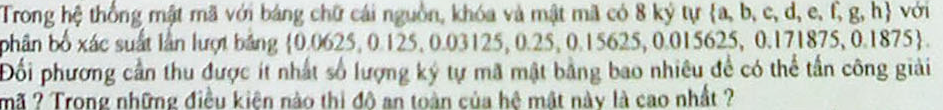
Những điểm yếu trên làm sơ đồ có thể là nạn nhân của các cuộc tấn công nghe trộm, giả mạo, man in the middle....

Các giải pháp tăng cường độ an toàn của sơ đồ này:

+ mã hóa password theo các sơ đồ như hash, v...v...

+ Có một hệ thống cấp phát chứng chỉ số để chứng thực các bên liên quan

**Câu 3:**



Bài này tớ không nhớ lắm, hiện giờ không có vở nên ko giải được, cậu xem lại vở.

Bài này tớ giải ra công thức tổng quát, không có kết quả cụ thể, ko biết là có đúng ko

Tớ chỉ nhớ là tớ gọi:

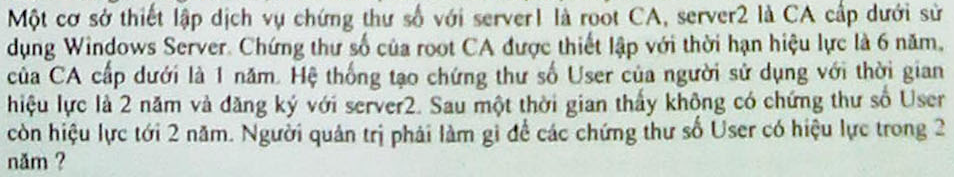
- đọ dài nguồn là Ln

- độ dài khóa là Lk

- độ dài mã mật là Lm

Sau đó tớ tính theo công thức trong vở ra công thức tổng quát

**Câu 4:**



Giải thích:

Do thời gian của CA cấp dưới chỉ là 1 năm, nên sau khi hết 1 năm CA cấp dưới phải xin chứng thư số mới. Lúc này, do user có hiệu lực 2 năm nên chưa cập nhật chứng thư.

Chứng thư của user không sử dụng được nữa do nó chưa được CA cấp dưới cấp phát lại, dẫn đến các đối tượng khác không công nhận user đó.

Để giải quyết tình trạng này có những cách sau đây:

- Xin cấp phát lại chứng chỉ cho user

- Tăng thời gian hiệu lực của CA cấp dưới lên 2 năm

- Giảm thời gian hiệu lực của chứng chỉ người dùng xuống 1 năm

- Đăng ký trực tiếp user với CA cấp trên