


Nhập môn An toàn thông tin

PGS. Nguyễn Linh Giang
Bộ môn Truyền thông và
Mạng máy tính



Nội dung

- I. Nhập môn An toàn thông tin
- II. Đảm bảo tính mật
 - I. Các hệ mật khóa đối xứng (mã hóa đối xứng)
 - II. Các hệ mật khóa công khai (mã hóa bất đối xứng)
- III. Bài toán xác thực
 - I. Cơ sở bài toán xác thực
 - II. Xác thực thông điệp
 - III. Chữ ký số và các giao thức xác thực
 - IV. Các cơ chế xác thực trong các hệ phân tán
- IV. An toàn an ninh hệ thống
 - I. Phát hiện và ngăn chặn xâm nhập (IDS, IPS)
 - II. Lỗ hổng hệ thống

Nội dung

- Tài liệu môn học:
 - W. Stallings “Networks and Internetwork security”
 - W. Stallings “Cryptography and network security”
 - Introduction to Cryptography – PGP
 - D. Stinson – Cryptography: Theory and Practice

Chương IV. Tin cậy hai bên

- Phân cấp khóa
- Quản trị và phân phối khóa trong sơ đồ mã hóa đối xứng
- Quản trị khóa trong sơ đồ mã hóa công khai
- Chia sẻ khóa phiên bí mật bằng hệ mã hóa công khai
- Đảm bảo tính mật

Quản trị và phân phối khóa trong mã hóa đối xứng

- Đặt vấn đề:
 - Trong kỹ thuật mật mã truyền thống, hai phía tham gia vào truyền tin phải chia sẻ khoá mật \Rightarrow khoá phải được đảm bảo bí mật : phải duy trì được kênh mật phân phối khóa.
 - Khóa phải được sử dụng một lần: Khoá phải được thường xuyên thay đổi.
 - Mức độ an toàn của bất kỳ hệ mật sẽ phụ thuộc vào kỹ thuật phân phối khoá.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Một số kỹ thuật phân phối khoá.
 - Phân phối khóa không tập trung: Khóa được A lựa chọn và phân phối vật lý tới B.
 - Phân phối khóa tập trung: Người thứ ba C lựa chọn khóa và phân phối vật lý tới A và B.
 - Nhận xét:
 - Hai kỹ thuật này khá cồng kềnh khi các bên tham gia vào trao đổi thông tin với số lượng lớn.

Quản trị và phân phối khóa trong mã hóa đối xứng

Sử dụng
phân
cấp khóa

Khóa
phiên

Khóa
chính



Bảo vệ bằng
mật mã



Bảo vệ bằng
mật mã



Bảo vệ
không bằng
mật mã

– Ít nhất có hai cấp khoá :

- Việc giao tiếp giữa hai trạm đầu cuối sẽ được mã hoá bằng một khoá tạm thời gọi là khoá phiên.
 - Khoá phiên sẽ được sử dụng trong thời gian một kết nối logic như trong mạng ảo hoặc liên kết vận chuyển, sau đó sẽ được loại bỏ.
 - Khoá phiên được truyền dưới dạng mã hoá bằng mã chính (master key). Khoá chính này được chia sẻ giữa KDC và trạm đầu cuối hoặc người sử dụng.

Quản trị và phân phối khóa trong mã hóa đối xứng

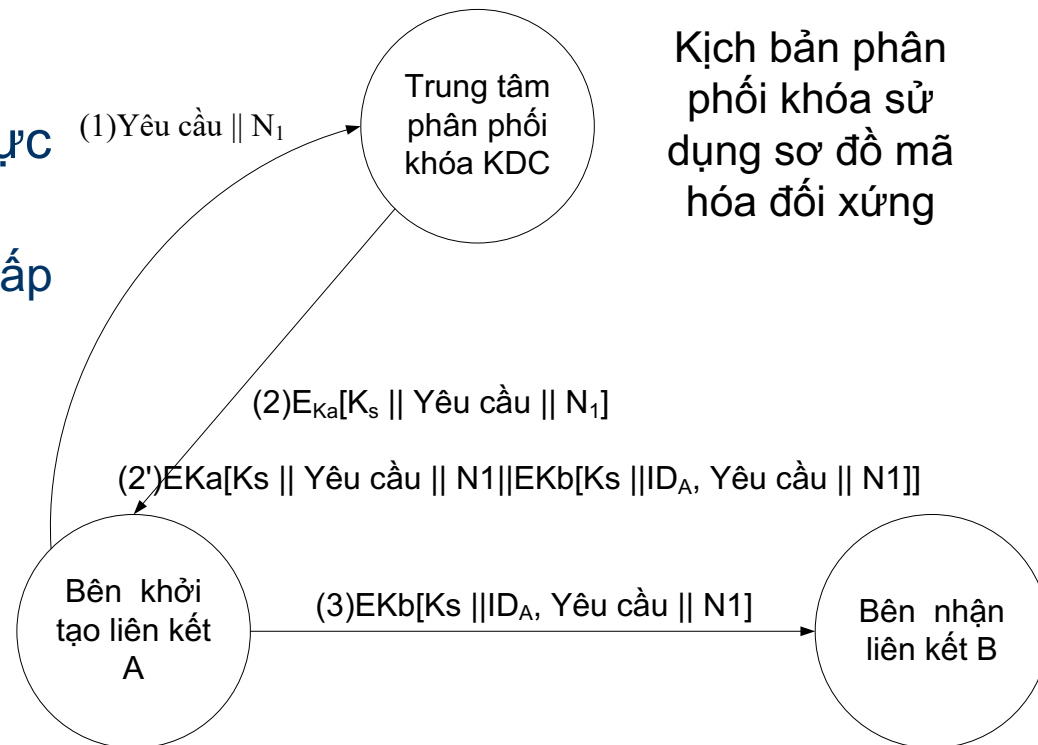
- Kịch bản quá trình phân phối khóa.
 - Giả thiết: mọi người sử dụng cùng chia sẻ một khóa mật chính với trung tâm phân phối khóa (KDC).
 - Tiền đề:
 - Người sử dụng A muốn thiết lập kết nối logic với người sử dụng B.
 - Hai phía trao đổi thông tin yêu cầu khóa phiên sử dụng một lần để bảo mật dữ liệu truyền qua kết nối.
 - Phía A có khóa mật K_{MA} , khóa này chỉ có A và KDC biết.
 - Phía B có khóa mật K_{MB} , khóa này chỉ có B và KDC biết.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Yêu cầu:

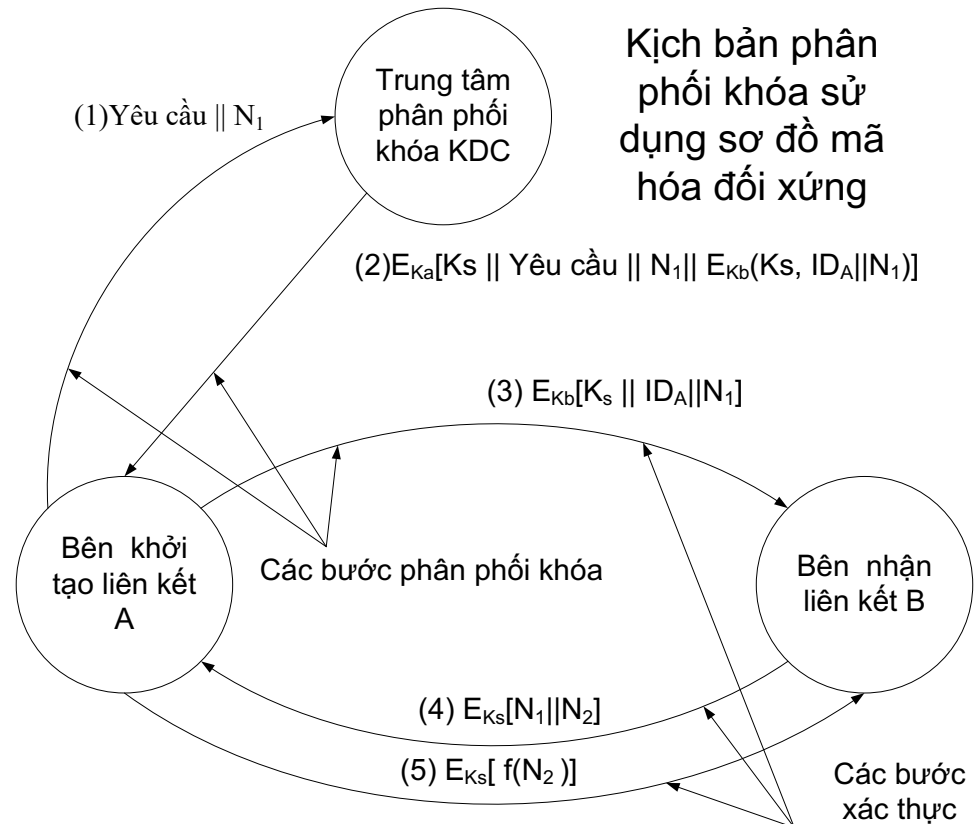
- A → KDC: KDC: xác thực A.

- $[ID_A; E_{KMA}[Yêu\ cầu\ cấp\ khóa; ID_B]; N_1]$



Quản trị và phân phối khóa trong mã hóa đối xứng

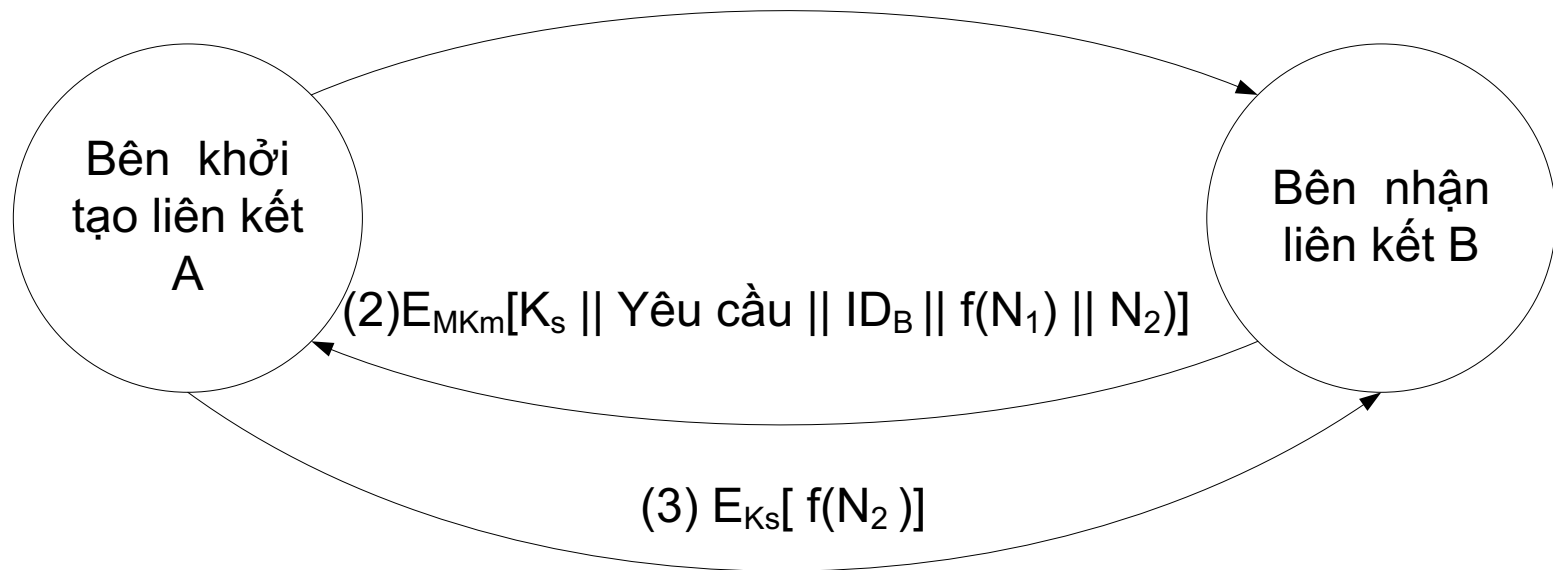
- Vấn đề xác thực:
 - B cần xác thực:
 - Nguồn gốc của $E_{kb}[K_s \parallel ID_A]$: bằng khóa K_b .
 - Tính toàn vẹn của $E_{kb}[K_s \parallel ID_A]$.
 - Xác thực A.
 - A cần xác thực:
 - Xác thực B.
 - Xác thực phiên làm việc với B.



Quản trị và phân phối khóa trong mã hóa đối xứng

Kịch bản phân phối khóa không tập trung

(1) Yêu cầu || N_1



Quản lý khóa trong sơ đồ mật mã khóa công khai

- Các mô hình quản lý khóa
 - Bài toán phân phối khóa: tập trung xây dựng kênh mật phân phối khóa phiên bí mật.
 - Hai hướng sử dụng mật mã khóa công khai:
 - Phân phối khóa công khai;
 - Sử dụng mã hóa khóa công khai để phân phối khóa phiên

Phân phối khóa công khai

- Các mô hình
 - Công bố công khai
 - Công bố thư mục công khai
 - Trung tâm ủy quyền khóa công khai
 - Chứng thư khóa công khai

Phân phối khóa công khai

- Công bố công khai
 - Các bên tham gia trao đổi thông tin tự công bố khóa công khai;
 - Điểm mạnh: đơn giản.
 - Điểm yếu:
 - Một người thứ 3 có thể giả mạo khóa công khai;
 - Bên C giả mạo bên nhận tin B, gửi khóa công khai của mình K_{PC} cho A;
 - A mã hóa các bản tin gửi cho B bằng khóa K_{PC} của C;
 - B không đọc được bản tin A gửi
 - C có thể đọc được bản tin A gửi B

Phân phối khóa công khai

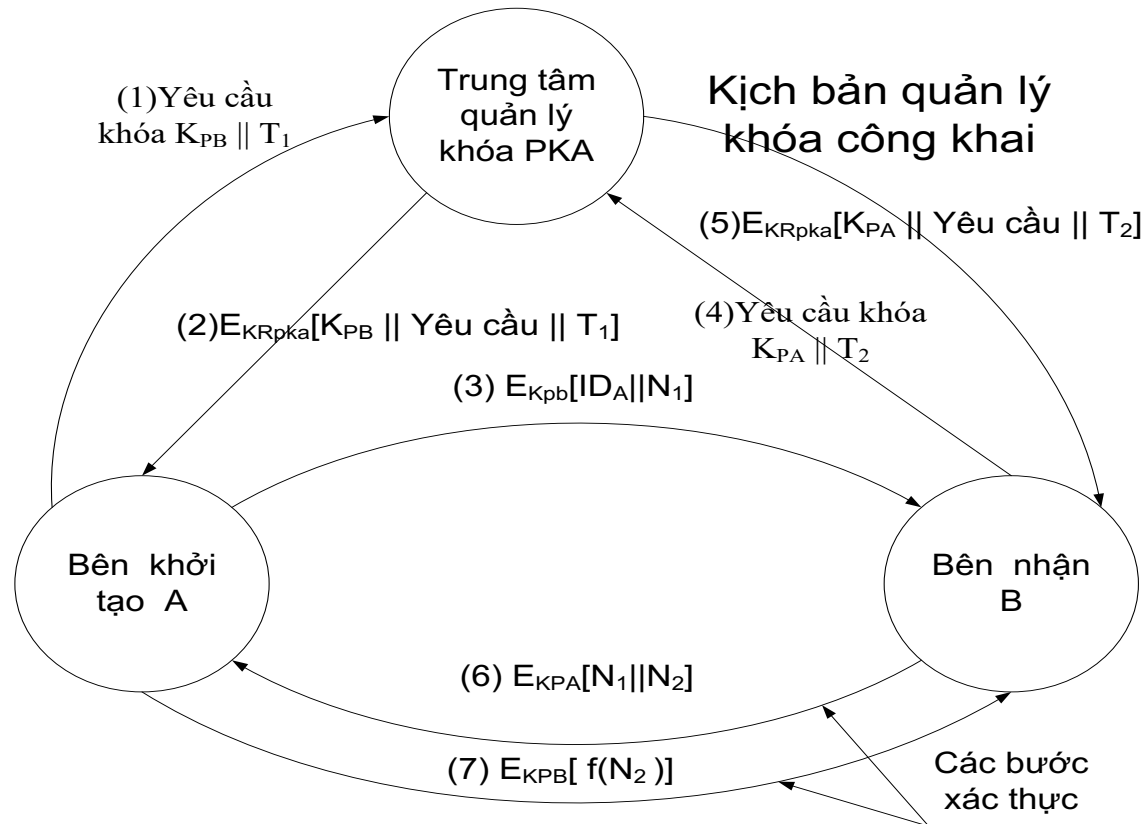
- Quản lý thư mục khóa công khai
 - Có bên thứ ba C được ủy quyền quản lý khóa công khai;
 - Bên thứ ba C tạo cho mỗi bên tham gia trao đổi thông tin một thư mục lưu trữ khóa;
 - Các bên đăng ký và gửi khóa công khai tới C. Quá trình đăng ký có thể thực hiện trên kênh bảo mật.
 - Các bên có thể thay thế khóa công khai theo nhu cầu
 - Khi đã sử dụng khóa nhiều lần để mã hóa lượng dữ liệu lớn;
 - Khi khóa riêng cần phải thay thế

Phân phối khóa công khai

- Bên C định kỳ công bố toàn bộ thư mục khóa hoặc cập nhật;
- Các bên có thể truy cập thư mục khóa qua các kênh bảo mật.
 - Vấn đề xác thực đối với bên thứ ba C.
- Điểm yếu:
 - Nếu thám mã biết được khóa riêng của C
 - Toàn bộ các khóa công khai được lưu trữ có thể bị giả mạo.
 - Có thể nghe trộm các thông điệp do các bên trao đổi .

Phân phối khóa công khai

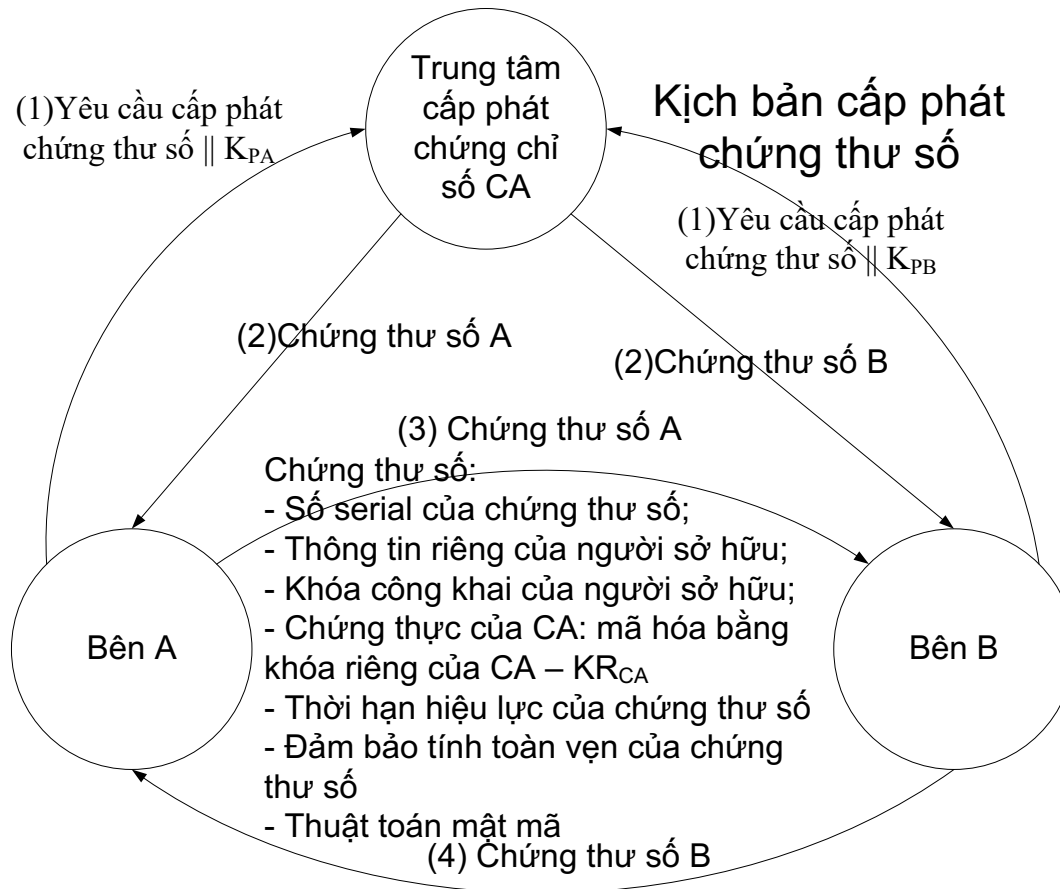
- Ủy quyền khóa công khai
 - Bên thứ ba được ủy quyền PKA tham gia lưu giữ khóa;
 - Các bên A, B biết khóa công khai của PKA;



Phân phối khóa công khai

- Chứng chỉ khóa công khai
 - Trung tâm cấp phát chứng thư số CA;
 - Chỉ cần xác nhận khóa công khai một lần;
 - Không cần truy cập CA mỗi khi cần khóa công khai;
 - Khóa công khai sẽ do các bên tự quản lý;
 - Sơ đồ hoạt động:
 - Các bên gửi khóa công khai tới CA để chứng thực;
 - Nhận chứng thư số từ CA kèm thời gian hiệu lực;
 - Các bên xuất trình chứng thư số trong các giao dịch;

Phân phối khóa công khai



Phân phối khóa mật đối xứng sử dụng mã hóa công khai

- Sơ đồ đơn giản:
 - A gửi B: $K_{PA} || ID_A$
 - B tạo khóa phiên K_S và gửi lại A: $E_{KPA}(K_S)$
- Sơ đồ kèm xác thực
 - A gửi B: $E_{KPB}(N_1 || ID_A)$
 - B gửi A: $E_{KPA}(N_1 || N_2)$
 - A gửi B: $E_{KPB}(N_2)$
 - A gửi B: $E_{KPB}(E_{KRA}(K_S))$

Đảm bảo tính riêng tư

1. Các cơ chế đảm bảo an toàn hệ thống:

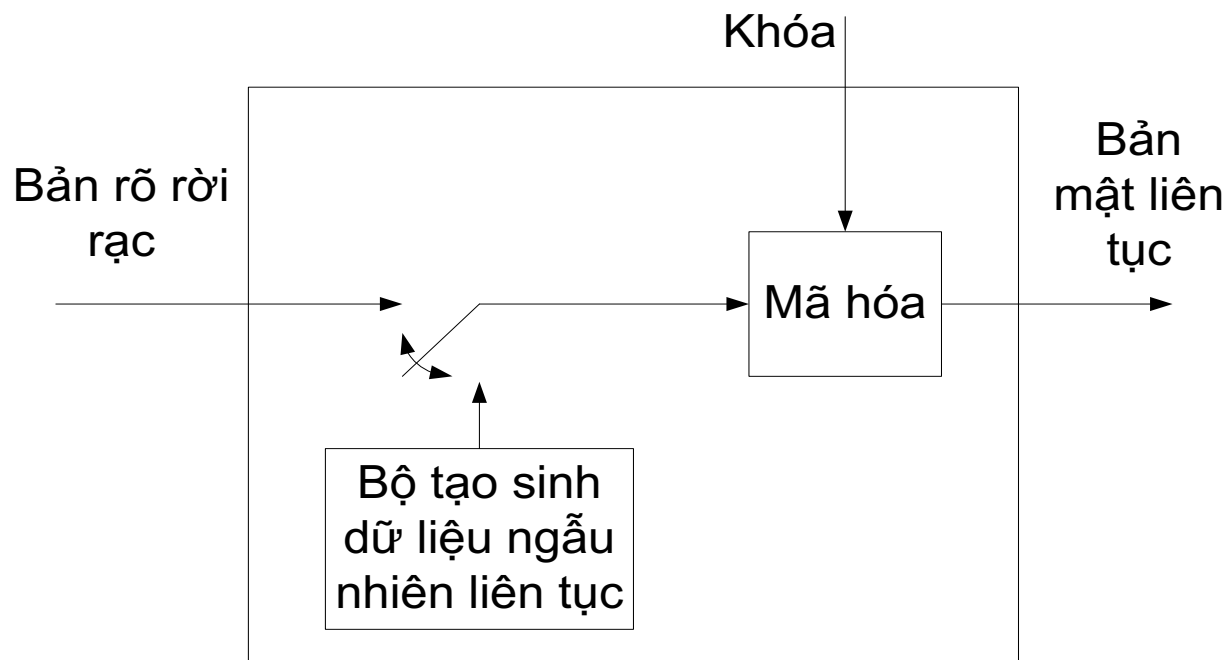
- Cơ chế bảo mật đường liên kết (link encryption approaches).
 - Mỗi đường truyền thông có thể bị tấn công đều được kết nối với các thiết bị mã hóa tại hai đầu \Rightarrow mọi quá trình truyền tải trên đường đều được bảo mật.
 - Nhược điểm:
 - Yêu cầu nhiều thiết bị mã hóa – giải mã đối với mạng lớn.
 - Thông điệp phải được giải mã mỗi khi đi vào bộ chuyển mạch gói bởi vì bộ chuyển mạch cần phải đọc địa chỉ (virtual circuit number) trong phần đầu gói tin để định tuyến cho gói.
 - Như vậy thông điệp là một điểm yếu tại mỗi bộ chuyển mạch. Do đó nếu phải làm việc với mạng công cộng, người sử dụng không thể kiểm soát được an toàn thông tin tại nút mạng.

Đảm bảo tính riêng tư

- Cơ chế bảo mật đầu – cuối (end – to – end encryption approaches).
 - Quá trình mã hóa mật được thực hiện tại hai hệ thống đầu cuối. Máy trạm nguồn mã hóa thông tin và được truyền qua mạng tới trạm đích.
 - Trạm nguồn và trạm đích cùng chia sẻ khóa mật và do đó có thể giải mã thông điệp.
 - Dạng bảo mật này cho phép bảo đảm an toàn đối với các tấn công vào các điểm kết nối hoặc các điểm chuyển mạch.
 - Dạng bảo mật này cho phép người sử dụng yên tâm về mức độ an toàn của mạng và đường liên kết truyền thông.

Đảm bảo tính riêng tư

- Thủ tục đệm luồng truyền tải:



Kết chương

- Quản lý khóa công khai
 - Giải quyết vấn đề giả mạo khóa công khai.
 - Bên thứ 3 chứng thực khóa công khai.
 - Yêu cầu giao dịch chứng thực mỗi khi có phiên trao đổi thông tin: phức tạp, làm tăng giao dịch trong mạng
 - Cấp chứng chỉ số xác nhận chủ thể cho các bên tham gia trao đổi thông tin.
 - Các thông tin xác nhận chủ thể
 - ID của chứng chỉ.
 - Dấu hiệu đặc trưng xác định duy nhất chủ thể: khóa công khai (quan hệ 1-1 với khóa riêng bí mật).
 - Dấu xác thực của bên cấp chứng chỉ số: mã hóa bằng khóa riêng của bên thứ 3 cấp chứng chỉ số

Kết chương

- Thời hạn hiệu lực của chứng chỉ số.
- Dấu hiệu để xác thực tính toàn vẹn về mặt nội dung của chứng chỉ số.