Quản trị và phân phối khóa

Nguyễn Linh Giang
Khoa CNTT, ĐHBK HN

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: Khoá được A lựa chọn và phân phối vật lý tới B.
  - Phân phối khóa tập trung: Người thứ ba C lựa chọn khoá 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

- Nếu A và B trước đây và hiện nay đã dùng khoá, một phía có thể gửi khoá mới dùng khoá cũ để mã hoá.
- Nếu A và B có kết nối mã mật với phía thứ ba C, C có thể phân phối khoá theo đường mã mật tới A và B.

– Phân cấp khoá:
  - Việc sử dụng trung tâm phân phối khoá dựa trên cơ sở của việc phân cấp các khoá.

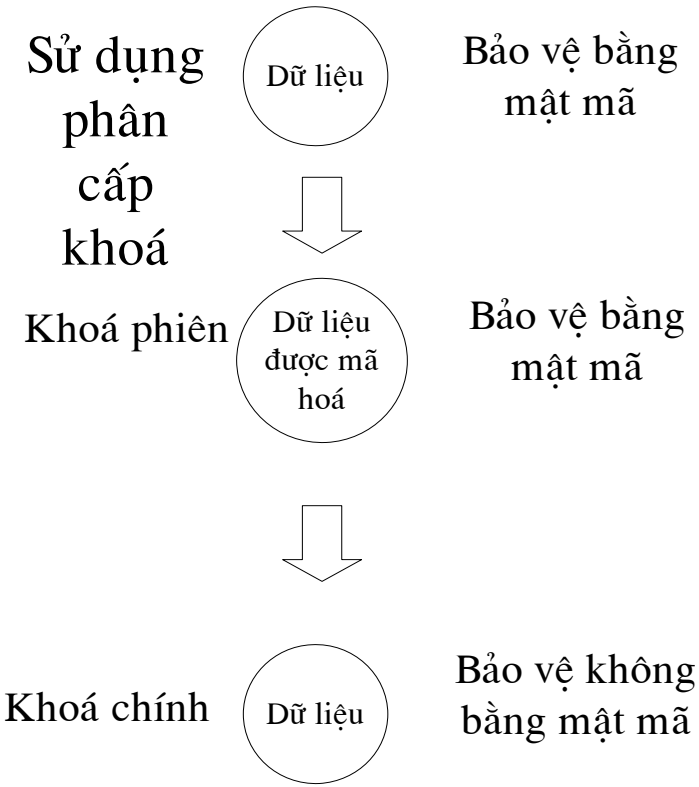
Quản trị và phân phối khóa trong mã hóa đối xứng

- Trên cấp độ tối thiểu, sẽ có hai cấp khoá được sử dụng:
  - Việc giao tiếp giữa hai tram 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 lôgic như trong mạng ảo hoặc liên kết vận chuyển, sau đó sẽ được loại bỏ.
  - Mỗi khoá phiên sẽ được nhận từ trung tâm phân phối khoá KDC trên cùng một hạ tầng mạng với kết nối đầu cuối.
  - 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

- Mỗi trạm đầu cuối sẽ có một khoá chính được chia sẻ với KDC.
- Các khoá chính này phải được chia sẻ theo một cách nào đó giữa KDC và máy trạm. Số lượng các khoá chính có thể kiểm soát được:
  - Nếu có N đối tượng cần tương tác với nhau theo cặp, như vậy cần có nhiều nhất N(N-1) /2 khoá phiên sẽ được sử dụng một lúc. Nhưng khi đó chỉ cần N khoá chính cho mỗi đối tượng. Như vậy các khoá chính có thể được phân phối theo đường không phải mật mã nhưphân phối vật lý.

Quản trị và phân phối khóa trong mã hóa đối xứng



Quản trị và phân phối khóa trong mã hóa đối xứng

- Kịch bản quá trình phân phối khóa.
  - Giả thiết: mội 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 lôgic 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 KA, khóa này chỉ có A và KDC biết.
    - Phía B có khóa mật KB, khóa này chỉ có B và KDC biết.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kịch bản phân phối khóa:
  - A yêu cầu KDC khóa phiên để bảo mật liên kết lôgic với B.
    - Trong thông điệp này chứa định danh của A và B cùng với dấu hiệu nhận diện N_1.
    - Dấu hiệu nhận diện N_1 này chỉ được sử dụng một lần trong trường hợp này.
    - Dấu hiệu nhận diện N_1 có thể là dấu thời gian, bộ đếm, hoặc là một số ngẫu nhiên.
    - Yêu cầu tối thiểu đối với dấu nhận diện: dấu hiệu này phải khác nhau đối với từng yêu cầu.
    - Để ngăn chặ sự giả mạo, dấu hiệu nhận diện phải khó bị iối phương dự đoán. Như vậy, số ngẫu nhiện là lựa chọn tốt.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Trung tâm phân phối khóa KDC trả lời A bằng thông điệp được mã hóa bằng khóa KA. Như vậy chỉ có A là người duy nhất có thể giải mã thành công thông điệp và A cũng xác định được nguồn gốc của thông điệp (A xác định được thông điệp là do KDC gửi tới do khóa KA chỉ có duy nhất A và KDC biết).

  Trong thông điệp chứa những thông tin dành cho A:

  - Khóa phiên sử dụng một lần KS;
  - Thông điệp gốc cùng với dấu hiệu nhận dạng N_1. Các thông tin này cho phép A so sánh câu trả lời từ KDC với yêu cầu ban đầu.

Quản trị và phân phối khóa trong mã hóa đối xứng

Như vậy, A có thể kiểm tra rằng yêu cầu ban đầu không bị thay đổi trước khi KDC nhận được và do có dấu hiệu nhận dạng N_1 nên thông điệp này không phải là phiên bản phát lại của một yêu cầu nào đó trước đó.

Trong thông điệp cũng có những thông tin dành cho B:

- Khóa phiên sử dụng một lần KS;
- Định danh của A – IDA.

Hai thông tin này được mã hóa với khóa mật KB chia sẻ giữa B và KDC. Những thông tin này được gửi cho B để thiết lập liên kết và chứng minh định danh của A.

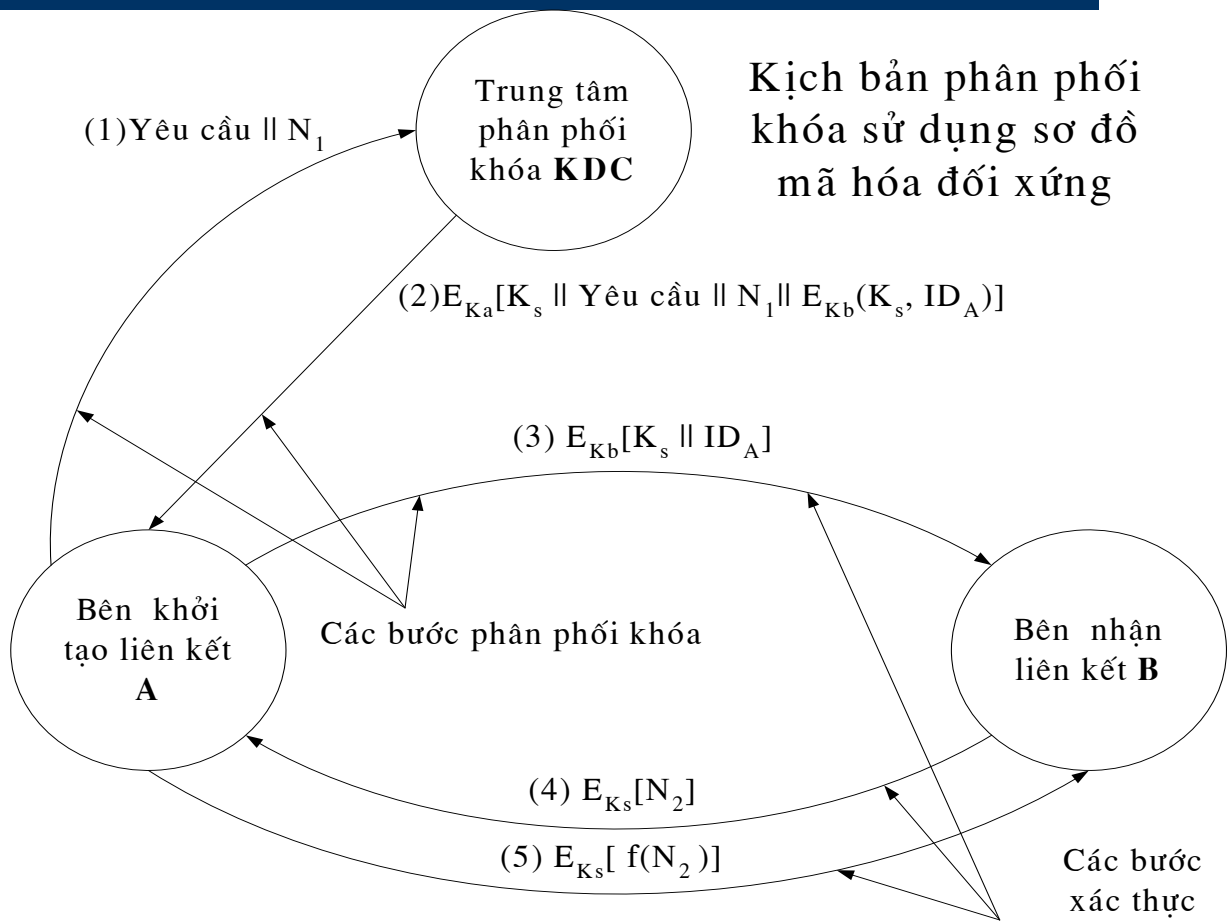
Quản trị và phân phối khóa trong mã hóa đối xứng

- A lưu lại khóa phiên KS để sử dụng cho liên kết sắp thiết lập và
  - gửi cho B những thông tin của KDC dành cho B – Ekb[KS || IDA]. Vì những thông tin này được mã hóa bằng KB nên chúng được bảo vệ khỏi hình thức nghe trộm. Sau khi nhận được thông điệp từ A, B biết được khóa phiên KS, và biết được phía bên kia là A từ định danh của A. Thêm vào đó, B biết được những thông tin này là do KDC cung cấp vì được mã hóa bằng KB – Ekb.
  - Như vậy từ thời điểm này, khóa phiên đã được phân phối mật tới A và B. A và B có thể sử dụng khóa phiên để trao đổi thông tin. Tuy nhiên để tăng độ tin cậy cho quá trình trao đổi thông tin và ngăn chặn các khả năng tấn công, hai bước sau có thể được áp dụng:

Quản trị và phân phối khóa trong mã hóa đối xứng

- B gửi tới cho A dấu hiệu nhận dạng N_2 bằng cách mã hóa sử dụng khóa phiên.
- Bằng cách sử dụng khóa phiên KS, A trả lời B bằng thông điệp $f(N_2)$, trong đó f là hàm biến đổi N_2.
  - Hai bước này giúp cho B biết được rằng thông điệp nhận được trong bước trước không bị phát lại.
  - Ta thấy các bước phân phối khóa bao gồm các bước từ 1 đến 3. Các bước 4, 5 cũng như bước 3 dùng vào mục đích các thực.

Quản trị và phân phối khóa trong mã hóa đối xứng



Kịch bản phân phối khóa sử dụng sơ đồ mã hóa đối xứng

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kiểm soát khóa theo phân cấp.
  - Hàm phân phối khóa không giới hạn bởi 01 KDC.
  - Một trật tự phân cấp các KDC được thiết lập:
    - Trong hệ thống có các KDC cục bộ: nằm trong các mạng cục bộ, trong các phân mạng nhỏ. KDC cục bộ có trách nhiệm phân phối khoá trong những giao dịch giữa những thành phần của một vùng.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Nếu hai thực thể thuộc hai phân vùng mạng khác nhau muốn chia sẻ khoá phiên, các KDC cục bộ phụ trách hai phân vùng đó sẽ tương tác với nhau thông qua KDC cấp cao hơn. Trong trường hợp này bất kỳ một trong ba KDC sẽ có thể sử dụng để lựa chọn khoá.
- Sơ đồ phân cấp làm giảm thiểu các nỗ lực trong việc phân phối khóa chính (master key distribution), bởi vì phần lớn các khoá chính là những khoá được chia sẻ giữa những KDC cục bộ với các thực thể thuộc vùng quản lý của chúng.
- Sơ đồ này làm giảm khả năng tổn hại tới khoá hoặc phá hoại khoá chỉ trong miền cục bộ của KDC.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Vòng đời của khoá phiên (session key lifetime).
  - Nếu khoá phiên càng được trao đổi với tần suất càng cao thì các khoá đó càng được bảo mật vì đối phương sẽ có ít văn bản mật tương ứng với từng khoá để phá mã.
  - Mặt khác quá trình phân phối khoá trước mỗi phiên làm việc sẽ làm chậm quá trình trao đổi thông tin và làm giảm hiệu năng của mạng.
  - Nhà quản trị an ninh phải lựa chọn giải pháp cân bằng hai vấn đề trên.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Đối với các giao thức hướng liên kết:
  - Sử dụng một khoá phiên cho một phiên làm việc khi liên kết đang hoạt động.
  - Sử dụng khoá phiên mới cho phiên làm việc mới.
  - Nếu liên kết vật lý tồn tại trong thời gian dài: để tăng tính cẩn mật, cần thay đổi khoá phiên một cách liên tục. Có thể lựa chọn thời gian theo một chuỗi các PDU.
- Đối với các giao thức hướng không liên kết:
  - Không có các chu trình khởi tạo và ngắt liên kết $\Rightarrow$ số lần thay đổi khoá không hiển nhiên $\Rightarrow$ sử dụng một khoá phiên mới cho mỗi lần trao đổi thông tin $\Rightarrow$ làm giảm ưu thế của giao tiếp không liên kết: tăng thời gian trễ của mỗi giao dịch.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Tính trong suốt của sơ đồ kiểm soát khoá:
  - Cung cấp khả năng mã hoá đầu cuối trên tầng mạng hoặc tâng giao vận sao cho quá trình trao đổi khoá và mã hoá trong suốt với người sử dụng.
  - Quá trình truyền thông sử dụng các giao thức hướng liên kết đầu cuối như TCP, X25.
  - Phần tử quan trọng: bộ xử lý ngoại vi (Front-end processor – FEP) cung cấp chức năng mã hoá đầu cuối và nhận các khoá phiên thay cho các trạm làm việc.

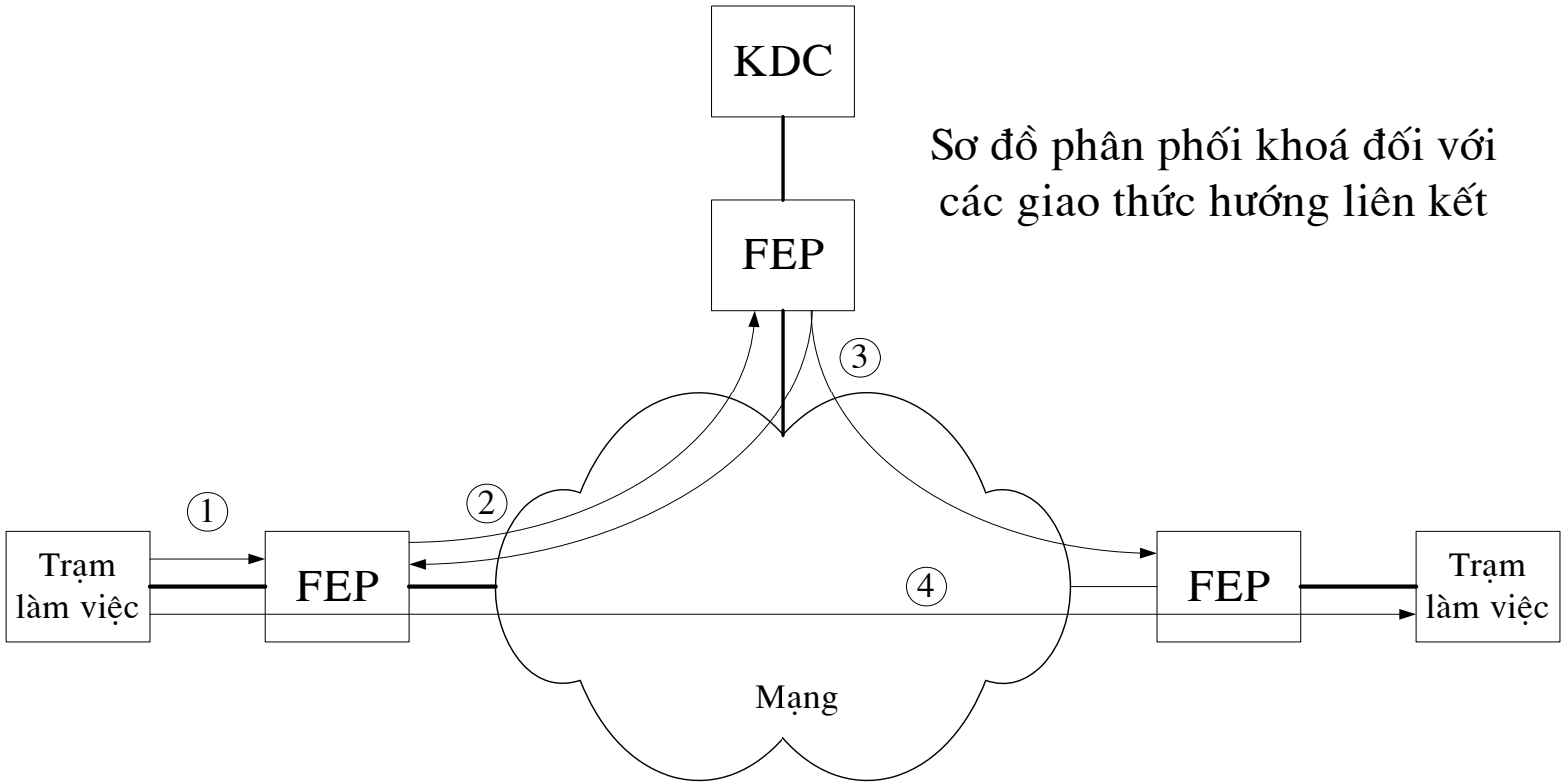
Quản trị và phân phối khóa trong mã hóa đối xứng

- Ưu điểm: làm giảm nhẹ ảnh hưởng của quá trình mã hoá, trao đổi khoá đối với các trạm đầu cuối.
- Từ khía cạnh máy trạm, FEP có thể coi là một phần của nút chuyển mạch gói $\Rightarrow$ giao tiếp giữa trạm và mạng không đổi.
- Từ hướng mạng, FEP có thể coi là một trạm $\Rightarrow$ giao tiếp chuyển mạch gói từ mạng tới trạm không đổi.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kịch bản:
  - Khi một trạm A mong muốn thiết lập liên kết với trạm khác, trạm A gửi một gói tin yêu cầu liên kết (bước 1).
  - Bộ xử lý ngoại vi FEP nhận gói tin và gửi tới KDC để nhận quyền khởi tạo kết nối (bước 2).
  - Liên kết và trao đổi thông tin giữa FEP và KDC được mã hoá bằng khoá chính được chia sẻ giữa FEP và KDC.

Quản trị và phân phối khóa trong mã hóa đối xứng



Sơ đồ phân phối khoá đối với các giao thức hướng liên kết

Quản trị và phân phối khóa trong mã hóa đối xứng

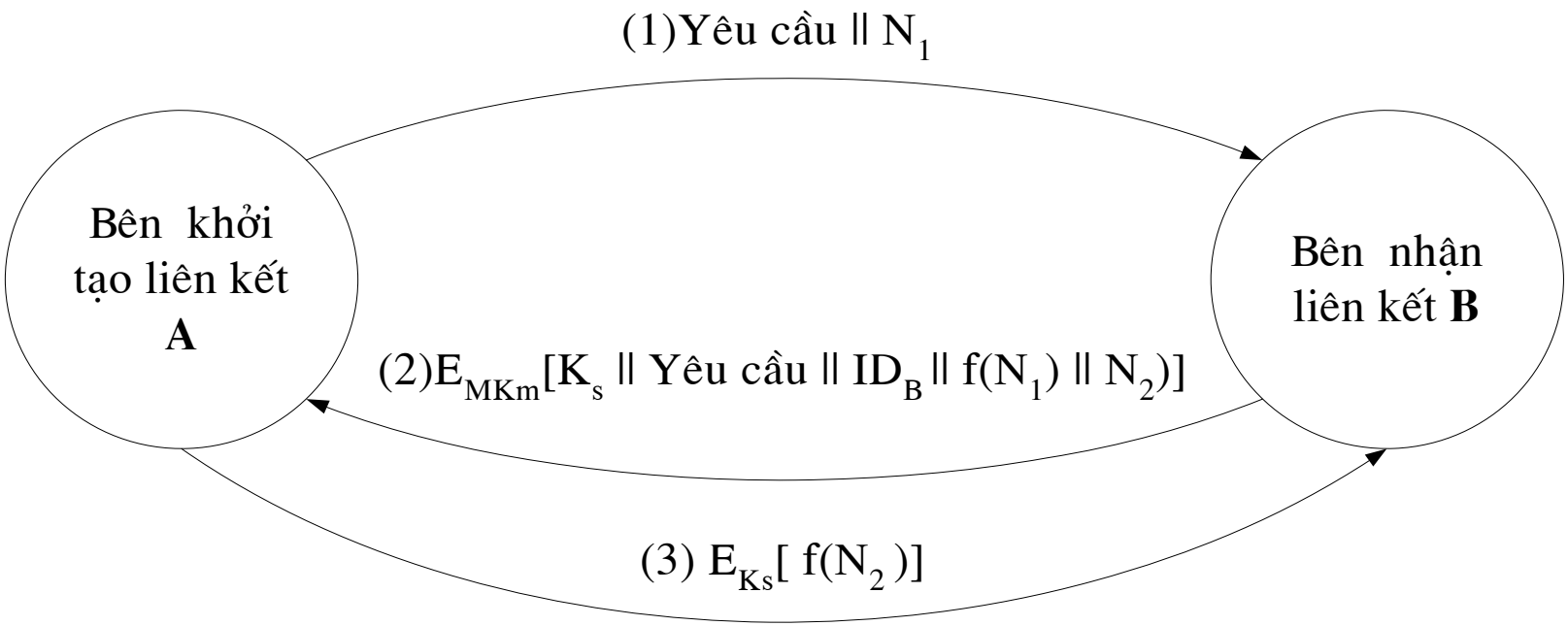
- Nếu KDC phê chuẩn yêu cầu liên kết, KDC sẽ tạo khoá phiên và phân phối tới hai FEP tương ứng sử dụng khoá duy nhất cố định cho mỗi giao tiếp (bước 3).
- Bộ xử lý ngoại vi FEP đã đưa ra yêu cầu có thể gửi gói tin yêu cầu thiết lập liên kết và liên kết sẽ được thiết lập giữa hai trạm đầu cuối (bước 4).
- Tất cả các dữ liệu được truyền giữa hai trạm đầu cuối sẽ được mã hoá do hai bộ xử lý ngoại vi tương ứng sử dụng khoá phiên sử dụng một lần.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kiểm soát khoá không tập trung:
  - Sử dụng trung tâm phân phối khoá KDC đưa ra yêu cầu đối với KDC: KDC phải được uỷ nhiệm và phải được bảo vệ khỏi các tấn công.
  - Các yêu cầu này có thể loại bỏ nếu sử dụng sơ đồ phân phối khoá không tập trung.

Quản trị và phân phối khóa trong mã hóa đối xứng

Kịch bản phân phối khóa không tập trung



Quản trị và phân phối khóa trong mã hóa đối xứng

- Các yêu cầu của phân phối khoá không tập trung:
  - Mỗi hệ thống giao tiếp theo liên kết mật với tất cả các hệ thống trạm khác với mục đích phân phối khoá phiên.
  - Số lượng khoá phiên cực đại có thể có sẽ bằng: $n(n - 1) / 2$.
- Kịch bản phân phối khoá không tập trung.
  - A gửi yêu cầu khoá phiên tới cho B cùng với dấu hiệu nhận dạng N_1;
  - B trả lời bằng thông điệp được mã hoá bằng khoá chính chung (shared master key). Trong câu trả lời chứa khoá phiên do B lựa chọn Ks, định danh của B, giá trị $f(N_1)$, và đấu hiệu nhận dạng N_2.
  - Sử dụng khoá phiên mới, A gửi trả $f(N_2)$ cho B.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Phân tích:
  - Mỗi nút cần phải có ít nhất (n – 1) khoá chính (master key) và một số lượng khoá phiên tuỳ ý có thể được tạo ra và sử dụng.
  - Do thông điệp được truyền sử dụng khoá chính khá ngắn $\Rightarrow$ việc thám mã là khó khăn.
  - Giống như trường hợp quản lý khoá tập trung, khoá phiên chỉ được sử dụng trong một khoảng thời gian ngắn để bảo vệ khoá.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kiểm soát việc sử dụng khoá.
  - Khái niệm phân cấp khóa và kỹ thuật phân phối khóa tự động làm giảm mạnh số lượng khóa cần xử lý bằng tay và phân phối bằng tay.
  - Đặt vấn đề: thiết lập sự kiểm soát những phương pháp phân phối khóa tự động.
    - Ví dụ: để phân tách khóa chính và khóa phiên, chúng ta có thể cần một số các khóa phiên khác nhau tùy theo cách sử dụng:
      - Khóa để mã hóa dữ liệu dùng cho truyền dữ liệu qua mạng;
      - Khóa PIN (personal identification number) sử dụng trong việc truyền các quỹ điện tử, các ứng dụng bán lẻ
      - Khóa để mã hóa file đối với những file được lưu trữ tại những thư mục public.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kỹ thuật kiểm soát khoá bằng vectơ kiểm soát (control vector):
  - Mỗi khoá phiên được đặt tương ứng với một vectơ kiểm soát bao gồm:
    - Số lượng các trường để đặc trưng cho việc sử dụng khoá và
    - Các giới hạn đối với khoá phiên đang xét.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Vectơ kiểm soát được mã hoá mật gắn kết với khoá vào thời điểm khoá được sinh ra tại KDC.
- Sơ đồ hoạt động:
  - Vectơ kiểm soát được đưa vào hàm băm, hàm băm này sinh ra một giá trị có độ dài bằng độ dài của khoá mã mật. Hàm băm sẽ ánh xạ một giá trị từ một khoảng lớn vào một khoảng có độ dài nhỏ hơn.
  - Giá trị băm được thực hiện XOR với khoá chính và kết quả sẽ đi vào khối mã hoá khoá phiên.

    Giá trị băm = H = h(CV);

    Key input = Km $\oplus$ H;

    Mã mật = $EKm_{\oplus H}[Ks]$.

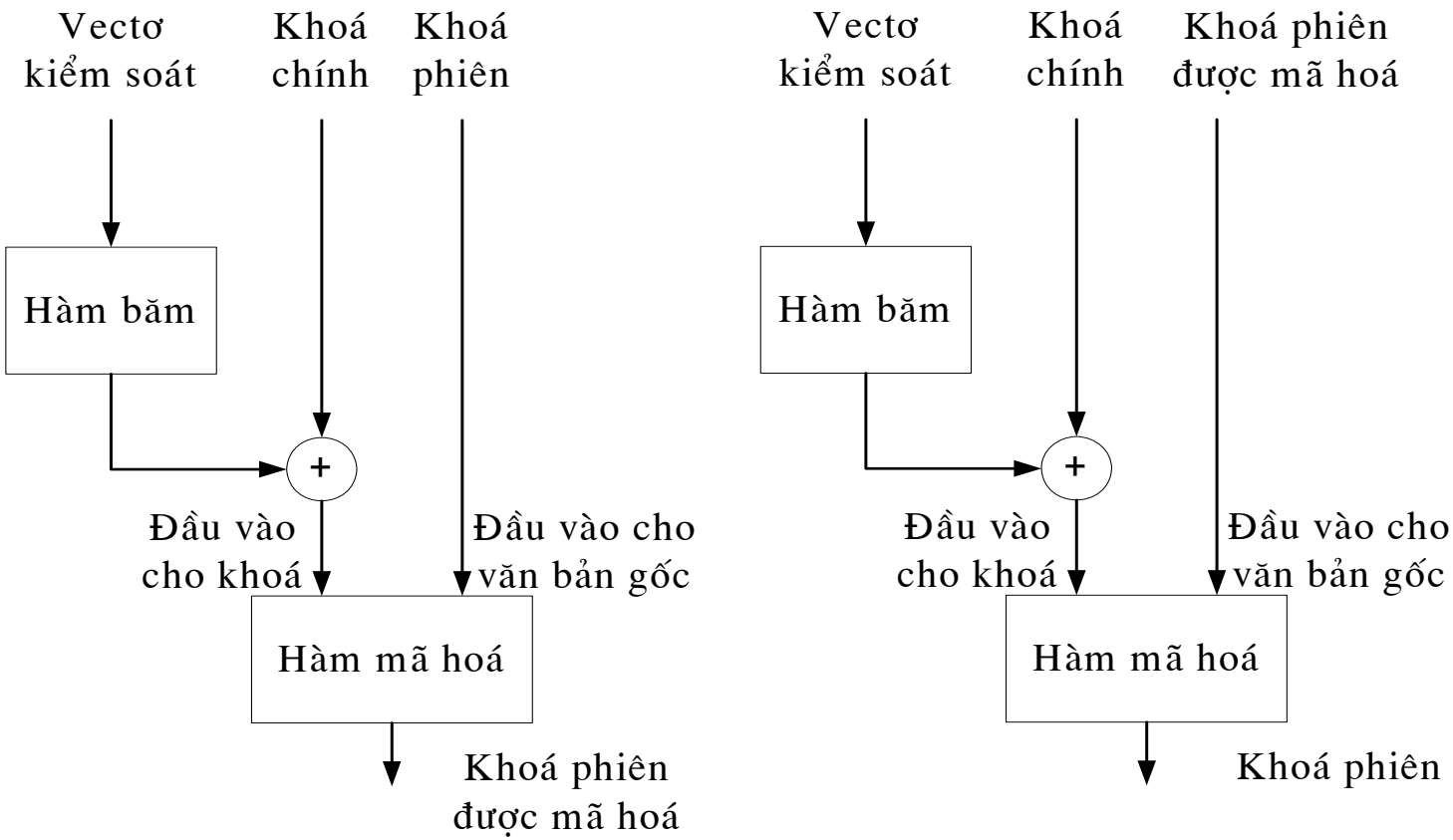
    Km: khoá chính và Ks: khoá phiên.
  - Khoá phiên sẽ được khôi phục từ mã mật bằng sơ đồ giải mã:

    Ks = $DKm_{\oplus H}[EKm_{\oplus H}[Ks]]$.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Khi khoá phiên được phân phối tới người sử dụng, khoá sẽ được kết hợp với vectơ kiểm soát. Khoá phiên chỉ có thể khôi phục được nếu có cả khoá chính (được chia sẻ) lẫn vectơ kiểm soát.

Quản trị và phân phối khóa trong mã hóa đối xứng



Mã hoá và giải mã vectơ kiểm soát khoá

Quản trị và phân phối khóa trong mã hóa đối xứng

- Ưu điểm của việc sử dụng vectơ kiểm soát khoá đối với việc sử dụng các thẻ 8-bit:
  - Không có giới hạn về độ dài của vectơ kiểm soát;
  - Vectơ kiểm soát tồn tại dưới dạng tường minh tại mọi bước thao tác.

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: Khoá được A lựa chọn và phân phối vật lý tới B.
  - Phân phối khóa tập trung: Người thứ ba C lựa chọn khoá 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

- Nếu A và B trước đây và hiện nay đã dùng khoá, một phía có thể gửi khoá mới dùng khoá cũ để mã hoá.
- Nếu A và B có kết nối mã mật với phía thứ ba C, C có thể phân phối khoá theo đường mã mật tới A và B.

– Phân cấp khoá:
  - Việc sử dụng trung tâm phân phối khoá dựa trên cơ sở của việc phân cấp các khoá.

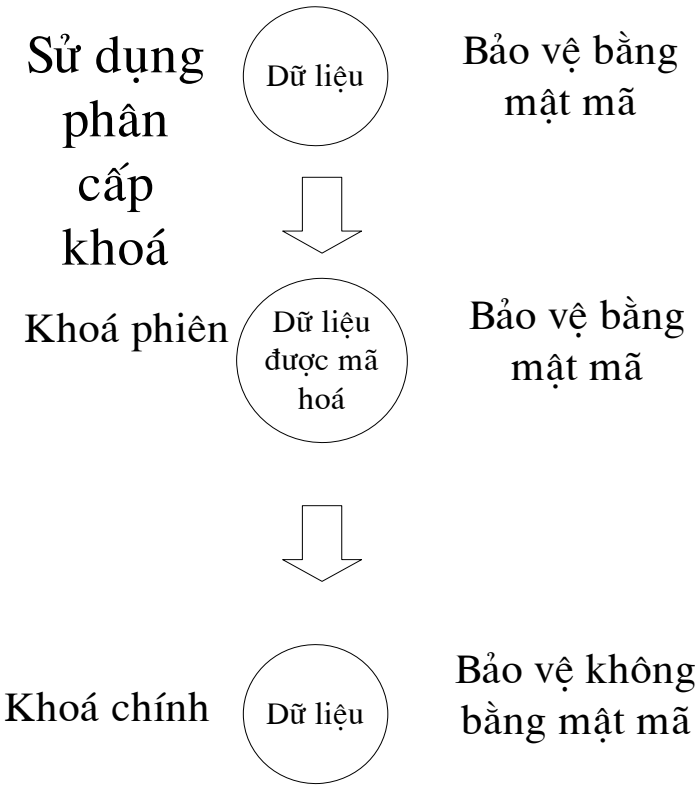
Quản trị và phân phối khóa trong mã hóa đối xứng

- Trên cấp độ tối thiểu, sẽ có hai cấp khoá được sử dụng:
  - Việc giao tiếp giữa hai tram 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 lôgic như trong mạng ảo hoặc liên kết vận chuyển, sau đó sẽ được loại bỏ.
  - Mỗi khoá phiên sẽ được nhận từ trung tâm phân phối khoá KDC trên cùng một hạ tầng mạng với kết nối đầu cuối.
  - 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

- Mỗi trạm đầu cuối sẽ có một khoá chính được chia sẻ với KDC.
- Các khoá chính này phải được chia sẻ theo một cách nào đó giữa KDC và máy trạm. Số lượng các khoá chính có thể kiểm soát được:
  - Nếu có N đối tượng cần tương tác với nhau theo cặp, như vậy cần có nhiều nhất N(N-1) /2 khoá phiên sẽ được sử dụng một lúc. Nhưng khi đó chỉ cần N khoá chính cho mỗi đối tượng. Như vậy các khoá chính có thể được phân phối theo đường không phải mật mã nhưphân phối vật lý.

Quản trị và phân phối khóa trong mã hóa đối xứng



Quản trị và phân phối khóa trong mã hóa đối xứng

- Kịch bản quá trình phân phối khóa.
  - Giả thiết: mội 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 lôgic 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 KA, khóa này chỉ có A và KDC biết.
    - Phía B có khóa mật KB, khóa này chỉ có B và KDC biết.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kịch bản phân phối khóa:
  - A yêu cầu KDC khóa phiên để bảo mật liên kết lôgic với B.
    - Trong thông điệp này chứa định danh của A và B cùng với dấu hiệu nhận diện N_1.
    - Dấu hiệu nhận diện N_1 này chỉ được sử dụng một lần trong trường hợp này.
    - Dấu hiệu nhận diện N_1 có thể là dấu thời gian, bộ đếm, hoặc là một số ngẫu nhiên.
    - Yêu cầu tối thiểu đối với dấu nhận diện: dấu hiệu này phải khác nhau đối với từng yêu cầu.
    - Để ngăn chặ sự giả mạo, dấu hiệu nhận diện phải khó bị iối phương dự đoán. Như vậy, số ngẫu nhiện là lựa chọn tốt.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Trung tâm phân phối khóa KDC trả lời A bằng thông điệp được mã hóa bằng khóa KA. Như vậy chỉ có A là người duy nhất có thể giải mã thành công thông điệp và A cũng xác định được nguồn gốc của thông điệp (A xác định được thông điệp là do KDC gửi tới do khóa KA chỉ có duy nhất A và KDC biết).

  Trong thông điệp chứa những thông tin dành cho A:

  - Khóa phiên sử dụng một lần KS;
  - Thông điệp gốc cùng với dấu hiệu nhận dạng N_1. Các thông tin này cho phép A so sánh câu trả lời từ KDC với yêu cầu ban đầu.

Quản trị và phân phối khóa trong mã hóa đối xứng

Như vậy, A có thể kiểm tra rằng yêu cầu ban đầu không bị thay đổi trước khi KDC nhận được và do có dấu hiệu nhận dạng N_1 nên thông điệp này không phải là phiên bản phát lại của một yêu cầu nào đó trước đó.

Trong thông điệp cũng có những thông tin dành cho B:

- Khóa phiên sử dụng một lần KS;
- Định danh của A – IDA.

Hai thông tin này được mã hóa với khóa mật KB chia sẻ giữa B và KDC. Những thông tin này được gửi cho B để thiết lập liên kết và chứng minh định danh của A.

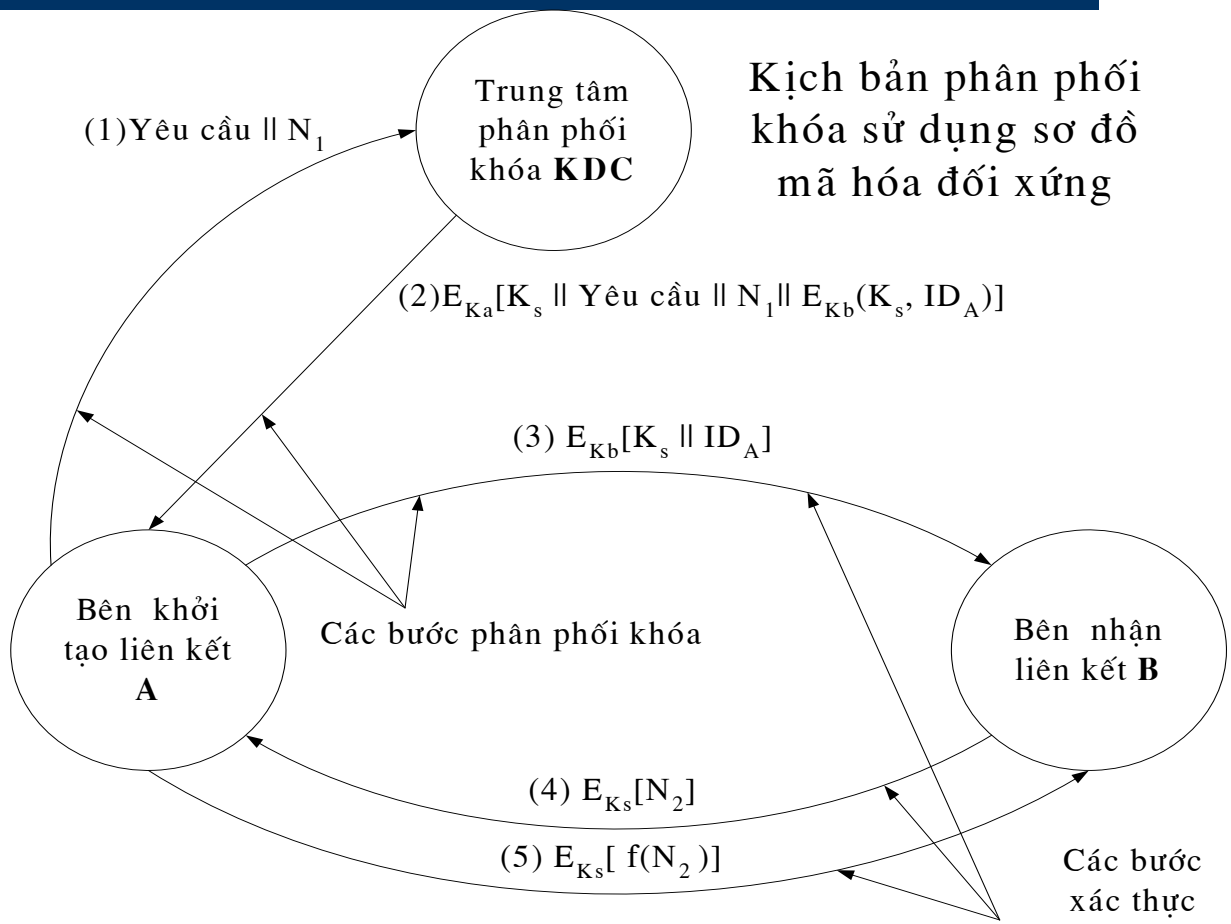
Quản trị và phân phối khóa trong mã hóa đối xứng

- A lưu lại khóa phiên KS để sử dụng cho liên kết sắp thiết lập và
  - gửi cho B những thông tin của KDC dành cho B – Ekb[KS || IDA]. Vì những thông tin này được mã hóa bằng KB nên chúng được bảo vệ khỏi hình thức nghe trộm. Sau khi nhận được thông điệp từ A, B biết được khóa phiên KS, và biết được phía bên kia là A từ định danh của A. Thêm vào đó, B biết được những thông tin này là do KDC cung cấp vì được mã hóa bằng KB – Ekb.
  - Như vậy từ thời điểm này, khóa phiên đã được phân phối mật tới A và B. A và B có thể sử dụng khóa phiên để trao đổi thông tin. Tuy nhiên để tăng độ tin cậy cho quá trình trao đổi thông tin và ngăn chặn các khả năng tấn công, hai bước sau có thể được áp dụng:

Quản trị và phân phối khóa trong mã hóa đối xứng

- B gửi tới cho A dấu hiệu nhận dạng N_2 bằng cách mã hóa sử dụng khóa phiên.
- Bằng cách sử dụng khóa phiên KS, A trả lời B bằng thông điệp $f(N_2)$, trong đó f là hàm biến đổi N_2.
  - Hai bước này giúp cho B biết được rằng thông điệp nhận được trong bước trước không bị phát lại.
  - Ta thấy các bước phân phối khóa bao gồm các bước từ 1 đến 3. Các bước 4, 5 cũng như bước 3 dùng vào mục đích các thực.

Quản trị và phân phối khóa trong mã hóa đối xứng



Kịch bản phân phối khóa sử dụng sơ đồ mã hóa đối xứng

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kiểm soát khóa theo phân cấp.
  - Hàm phân phối khóa không giới hạn bởi 01 KDC.
  - Một trật tự phân cấp các KDC được thiết lập:
    - Trong hệ thống có các KDC cục bộ: nằm trong các mạng cục bộ, trong các phân mạng nhỏ. KDC cục bộ có trách nhiệm phân phối khoá trong những giao dịch giữa những thành phần của một vùng.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Nếu hai thực thể thuộc hai phân vùng mạng khác nhau muốn chia sẻ khoá phiên, các KDC cục bộ phụ trách hai phân vùng đó sẽ tương tác với nhau thông qua KDC cấp cao hơn. Trong trường hợp này bất kỳ một trong ba KDC sẽ có thể sử dụng để lựa chọn khoá.
- Sơ đồ phân cấp làm giảm thiểu các nỗ lực trong việc phân phối khóa chính (master key distribution), bởi vì phần lớn các khoá chính là những khoá được chia sẻ giữa những KDC cục bộ với các thực thể thuộc vùng quản lý của chúng.
- Sơ đồ này làm giảm khả năng tổn hại tới khoá hoặc phá hoại khoá chỉ trong miền cục bộ của KDC.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Vòng đời của khoá phiên (session key lifetime).
  - Nếu khoá phiên càng được trao đổi với tần suất càng cao thì các khoá đó càng được bảo mật vì đối phương sẽ có ít văn bản mật tương ứng với từng khoá để phá mã.
  - Mặt khác quá trình phân phối khoá trước mỗi phiên làm việc sẽ làm chậm quá trình trao đổi thông tin và làm giảm hiệu năng của mạng.
  - Nhà quản trị an ninh phải lựa chọn giải pháp cân bằng hai vấn đề trên.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Đối với các giao thức hướng liên kết:
  - Sử dụng một khoá phiên cho một phiên làm việc khi liên kết đang hoạt động.
  - Sử dụng khoá phiên mới cho phiên làm việc mới.
  - Nếu liên kết vật lý tồn tại trong thời gian dài: để tăng tính cẩn mật, cần thay đổi khoá phiên một cách liên tục. Có thể lựa chọn thời gian theo một chuỗi các PDU.
- Đối với các giao thức hướng không liên kết:
  - Không có các chu trình khởi tạo và ngắt liên kết $\Rightarrow$ số lần thay đổi khoá không hiển nhiên $\Rightarrow$ sử dụng một khoá phiên mới cho mỗi lần trao đổi thông tin $\Rightarrow$ làm giảm ưu thế của giao tiếp không liên kết: tăng thời gian trễ của mỗi giao dịch.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Tính trong suốt của sơ đồ kiểm soát khoá:
  - Cung cấp khả năng mã hoá đầu cuối trên tầng mạng hoặc tâng giao vận sao cho quá trình trao đổi khoá và mã hoá trong suốt với người sử dụng.
  - Quá trình truyền thông sử dụng các giao thức hướng liên kết đầu cuối như TCP, X25.
  - Phần tử quan trọng: bộ xử lý ngoại vi (Front-end processor – FEP) cung cấp chức năng mã hoá đầu cuối và nhận các khoá phiên thay cho các trạm làm việc.

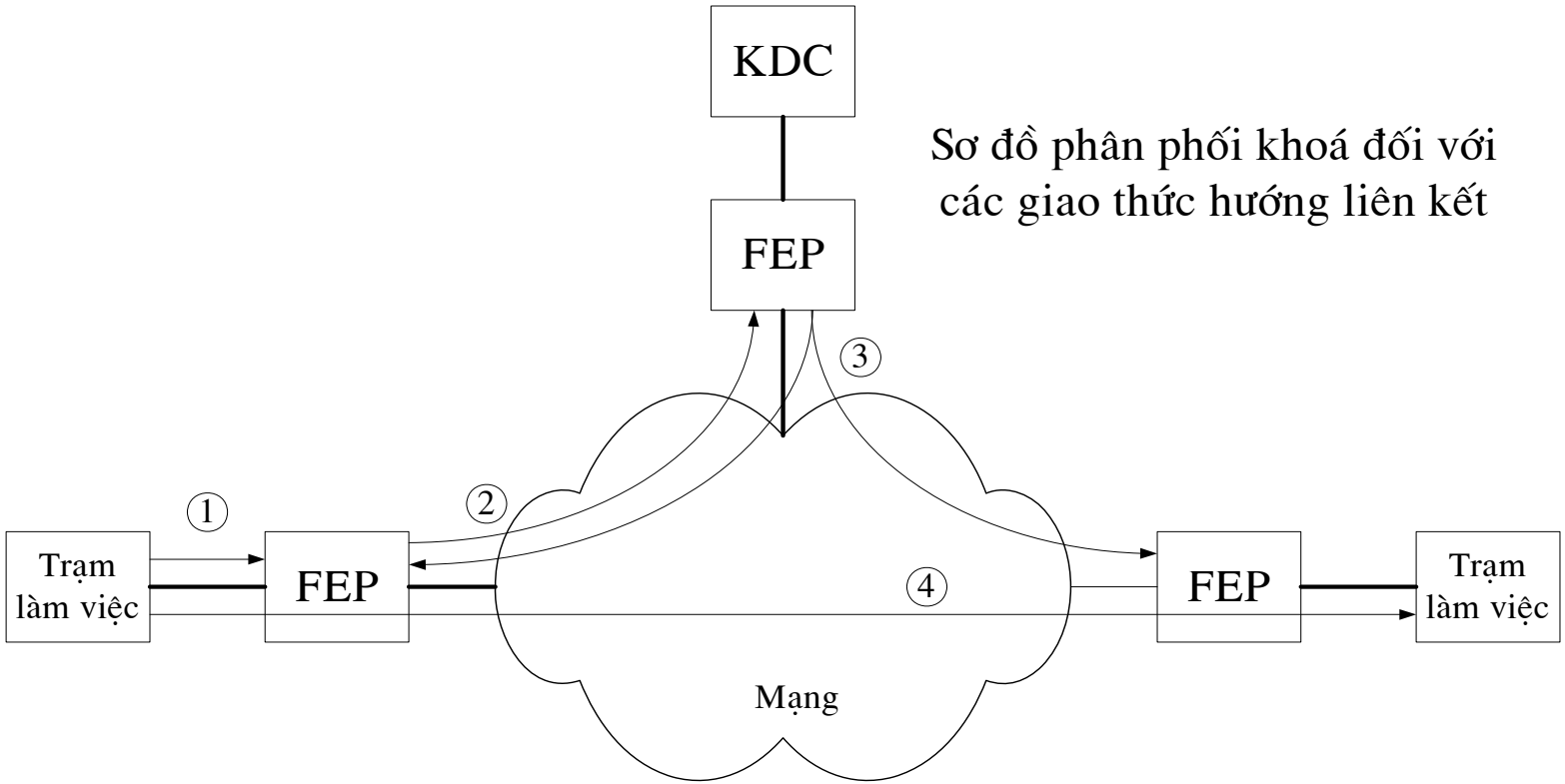
Quản trị và phân phối khóa trong mã hóa đối xứng

- Ưu điểm: làm giảm nhẹ ảnh hưởng của quá trình mã hoá, trao đổi khoá đối với các trạm đầu cuối.
- Từ khía cạnh máy trạm, FEP có thể coi là một phần của nút chuyển mạch gói $\Rightarrow$ giao tiếp giữa trạm và mạng không đổi.
- Từ hướng mạng, FEP có thể coi là một trạm $\Rightarrow$ giao tiếp chuyển mạch gói từ mạng tới trạm không đổi.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kịch bản:
  - Khi một trạm A mong muốn thiết lập liên kết với trạm khác, trạm A gửi một gói tin yêu cầu liên kết (bước 1).
  - Bộ xử lý ngoại vi FEP nhận gói tin và gửi tới KDC để nhận quyền khởi tạo kết nối (bước 2).
  - Liên kết và trao đổi thông tin giữa FEP và KDC được mã hoá bằng khoá chính được chia sẻ giữa FEP và KDC.

Quản trị và phân phối khóa trong mã hóa đối xứng



Sơ đồ phân phối khoá đối với các giao thức hướng liên kết

Quản trị và phân phối khóa trong mã hóa đối xứng

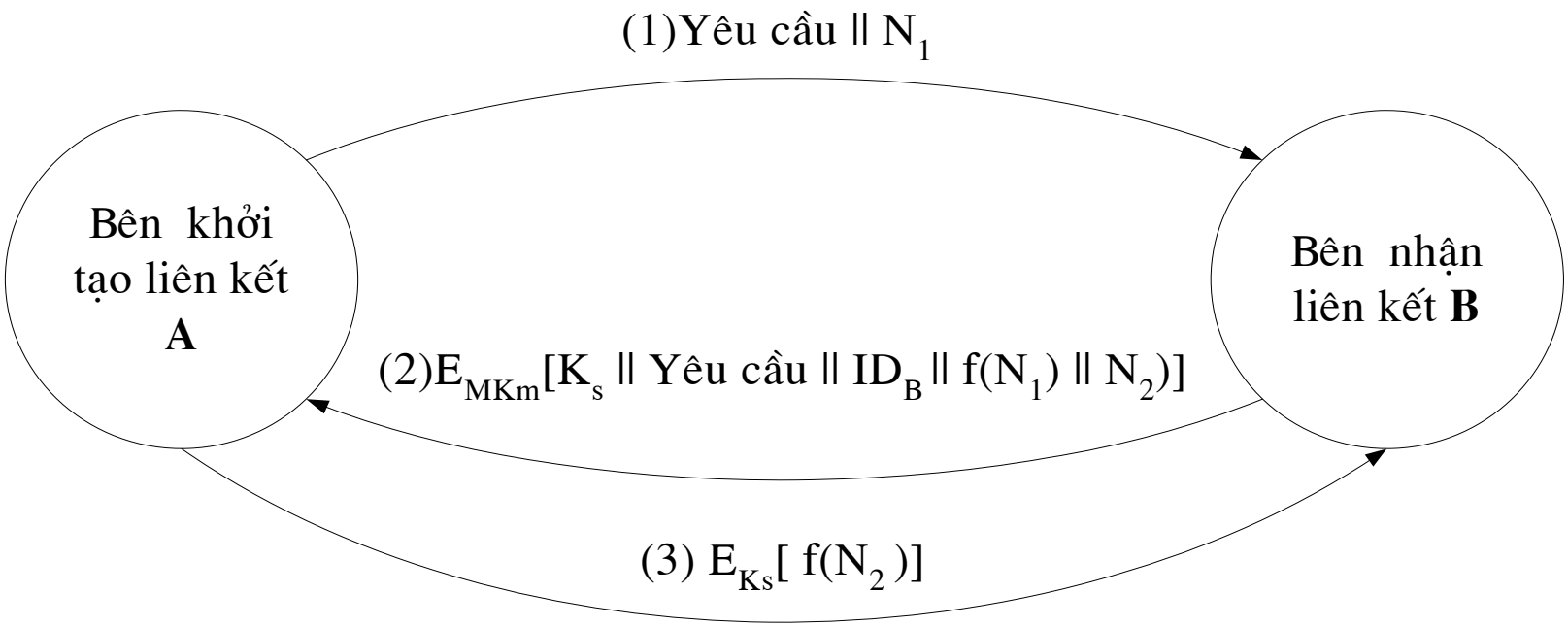
- Nếu KDC phê chuẩn yêu cầu liên kết, KDC sẽ tạo khoá phiên và phân phối tới hai FEP tương ứng sử dụng khoá duy nhất cố định cho mỗi giao tiếp (bước 3).
- Bộ xử lý ngoại vi FEP đã đưa ra yêu cầu có thể gửi gói tin yêu cầu thiết lập liên kết và liên kết sẽ được thiết lập giữa hai trạm đầu cuối (bước 4).
- Tất cả các dữ liệu được truyền giữa hai trạm đầu cuối sẽ được mã hoá do hai bộ xử lý ngoại vi tương ứng sử dụng khoá phiên sử dụng một lần.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kiểm soát khoá không tập trung:
  - Sử dụng trung tâm phân phối khoá KDC đưa ra yêu cầu đối với KDC: KDC phải được uỷ nhiệm và phải được bảo vệ khỏi các tấn công.
  - Các yêu cầu này có thể loại bỏ nếu sử dụng sơ đồ phân phối khoá không tập trung.

Quản trị và phân phối khóa trong mã hóa đối xứng

Kịch bản phân phối khóa không tập trung



Quản trị và phân phối khóa trong mã hóa đối xứng

- Các yêu cầu của phân phối khoá không tập trung:
  - Mỗi hệ thống giao tiếp theo liên kết mật với tất cả các hệ thống trạm khác với mục đích phân phối khoá phiên.
  - Số lượng khoá phiên cực đại có thể có sẽ bằng: $n(n - 1) / 2$.
- Kịch bản phân phối khoá không tập trung.
  - A gửi yêu cầu khoá phiên tới cho B cùng với dấu hiệu nhận dạng N_1;
  - B trả lời bằng thông điệp được mã hoá bằng khoá chính chung (shared master key). Trong câu trả lời chứa khoá phiên do B lựa chọn Ks, định danh của B, giá trị $f(N_1)$, và đấu hiệu nhận dạng N_2.
  - Sử dụng khoá phiên mới, A gửi trả $f(N_2)$ cho B.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Phân tích:
  - Mỗi nút cần phải có ít nhất (n – 1) khoá chính (master key) và một số lượng khoá phiên tuỳ ý có thể được tạo ra và sử dụng.
  - Do thông điệp được truyền sử dụng khoá chính khá ngắn $\Rightarrow$ việc thám mã là khó khăn.
  - Giống như trường hợp quản lý khoá tập trung, khoá phiên chỉ được sử dụng trong một khoảng thời gian ngắn để bảo vệ khoá.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kiểm soát việc sử dụng khoá.
  - Khái niệm phân cấp khóa và kỹ thuật phân phối khóa tự động làm giảm mạnh số lượng khóa cần xử lý bằng tay và phân phối bằng tay.
  - Đặt vấn đề: thiết lập sự kiểm soát những phương pháp phân phối khóa tự động.
    - Ví dụ: để phân tách khóa chính và khóa phiên, chúng ta có thể cần một số các khóa phiên khác nhau tùy theo cách sử dụng:
      - Khóa để mã hóa dữ liệu dùng cho truyền dữ liệu qua mạng;
      - Khóa PIN (personal identification number) sử dụng trong việc truyền các quỹ điện tử, các ứng dụng bán lẻ
      - Khóa để mã hóa file đối với những file được lưu trữ tại những thư mục public.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Kỹ thuật kiểm soát khoá bằng vectơ kiểm soát (control vector):
  - Mỗi khoá phiên được đặt tương ứng với một vectơ kiểm soát bao gồm:
    - Số lượng các trường để đặc trưng cho việc sử dụng khoá và
    - Các giới hạn đối với khoá phiên đang xét.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Vectơ kiểm soát được mã hoá mật gắn kết với khoá vào thời điểm khoá được sinh ra tại KDC.
- Sơ đồ hoạt động:
  - Vectơ kiểm soát được đưa vào hàm băm, hàm băm này sinh ra một giá trị có độ dài bằng độ dài của khoá mã mật. Hàm băm sẽ ánh xạ một giá trị từ một khoảng lớn vào một khoảng có độ dài nhỏ hơn.
  - Giá trị băm được thực hiện XOR với khoá chính và kết quả sẽ đi vào khối mã hoá khoá phiên.

    Giá trị băm = H = h(CV);

    Key input = Km $\oplus$ H;

    Mã mật = $EKm_{\oplus H}[Ks]$.

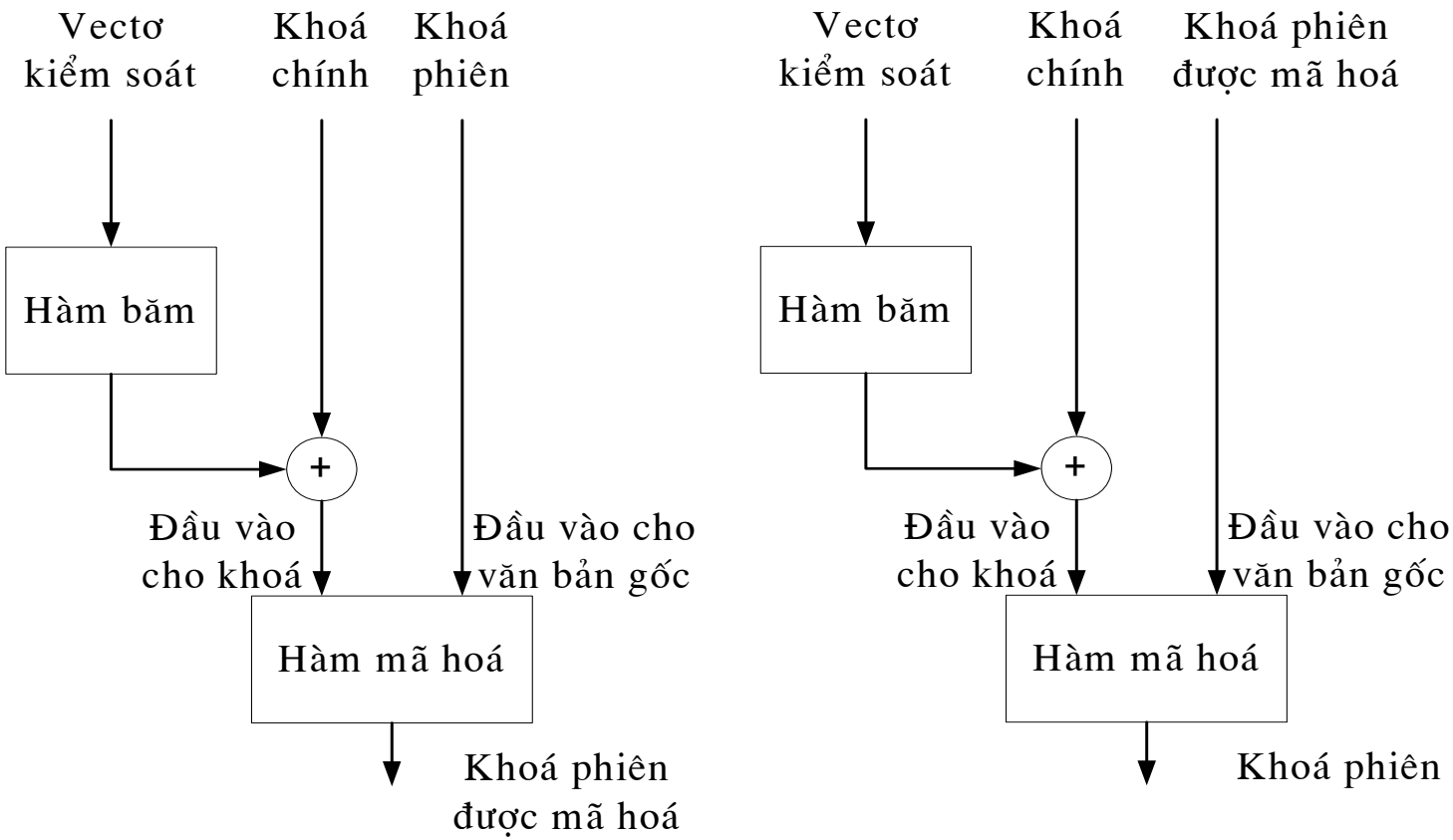
    Km: khoá chính và Ks: khoá phiên.
  - Khoá phiên sẽ được khôi phục từ mã mật bằng sơ đồ giải mã:

    Ks = $DKm_{\oplus H}[EKm_{\oplus H}[Ks]]$.

Quản trị và phân phối khóa trong mã hóa đối xứng

- Khi khoá phiên được phân phối tới người sử dụng, khoá sẽ được kết hợp với vectơ kiểm soát. Khoá phiên chỉ có thể khôi phục được nếu có cả khoá chính (được chia sẻ) lẫn vectơ kiểm soát.

Quản trị và phân phối khóa trong mã hóa đối xứng



Mã hoá và giải mã vectơ kiểm soát khoá

Quản trị và phân phối khóa trong mã hóa đối xứng

- Ưu điểm của việc sử dụng vectơ kiểm soát khoá đối với việc sử dụng các thẻ 8-bit:
  - Không có giới hạn về độ dài của vectơ kiểm soát;
  - Vectơ kiểm soát tồn tại dưới dạng tường minh tại mọi bước thao tác.