Quản lý và trao đổi khoá

Ký hiệu

- $X \rightarrow Y : \{ Z \,||\, W \}\, k_{X,Y}$
  - X gửi Y gói tin tạo bởi nối Z và W sau đó mã hoá với khoá $k_{X,Y}$, là khoá chung của X và Y
- $A \rightarrow T : \{ Z \}\, k_A \,||\, \{ W \}\, k_{A,T}$
  - A gửi T 1 gói tin là nối của bản mã Z với khoá k_A, khoá bí mật của A, và bản mã W với khoá $k_{A,T}$, là khoá chung của A và T
- r_1, r_2 là các số ngẫu nhiên (số ngẫu nhiên không lặp lại)

Khoá phiên – khoá trao đổi
Session key - Interchange key

- Alice muốn gửi bản tin *m* cho Bob
  - Giả sử 2 bên sử dung hệ mã công khai
  - Alice biết khoá công khai của Bob, Z_B
- Ví dụ về việc dung khoá phiên
  - Alice tạo 1 khoá ngẫu nhiên k_s dùng để mã hoá bản tin *m*
    - Khoá này chỉ dung để mã hoá bản tin
    - Được gọi là khoá phiên - *session key*
  - Alice mã hoá k_s với khoá công khai của Bob, Z_B
    - Z_B được dung để mã hoá toàn bộ khoá phiên trao đổi giữa Alice và Bob
    - Được gọi là khoá trao đổi - *interchange key*
  - Alice gửi Bob: $\{ m \} k_s \{ k_s \} Z_B$

Session key - Interchange key

- Khoá phiên - session key
  - Gắn với 1 phiên giao dịch
  - Chỉ dung để mã hoá thông tin, không dùng để xác thực chủ thể
    - Tại sao?
- Khoá trao đổi - Interchange key
  - Gắn với 1 chủ thể
  - Có thể dùng để xác thực chủ thể

Tại sao cần dùng khoá phiên

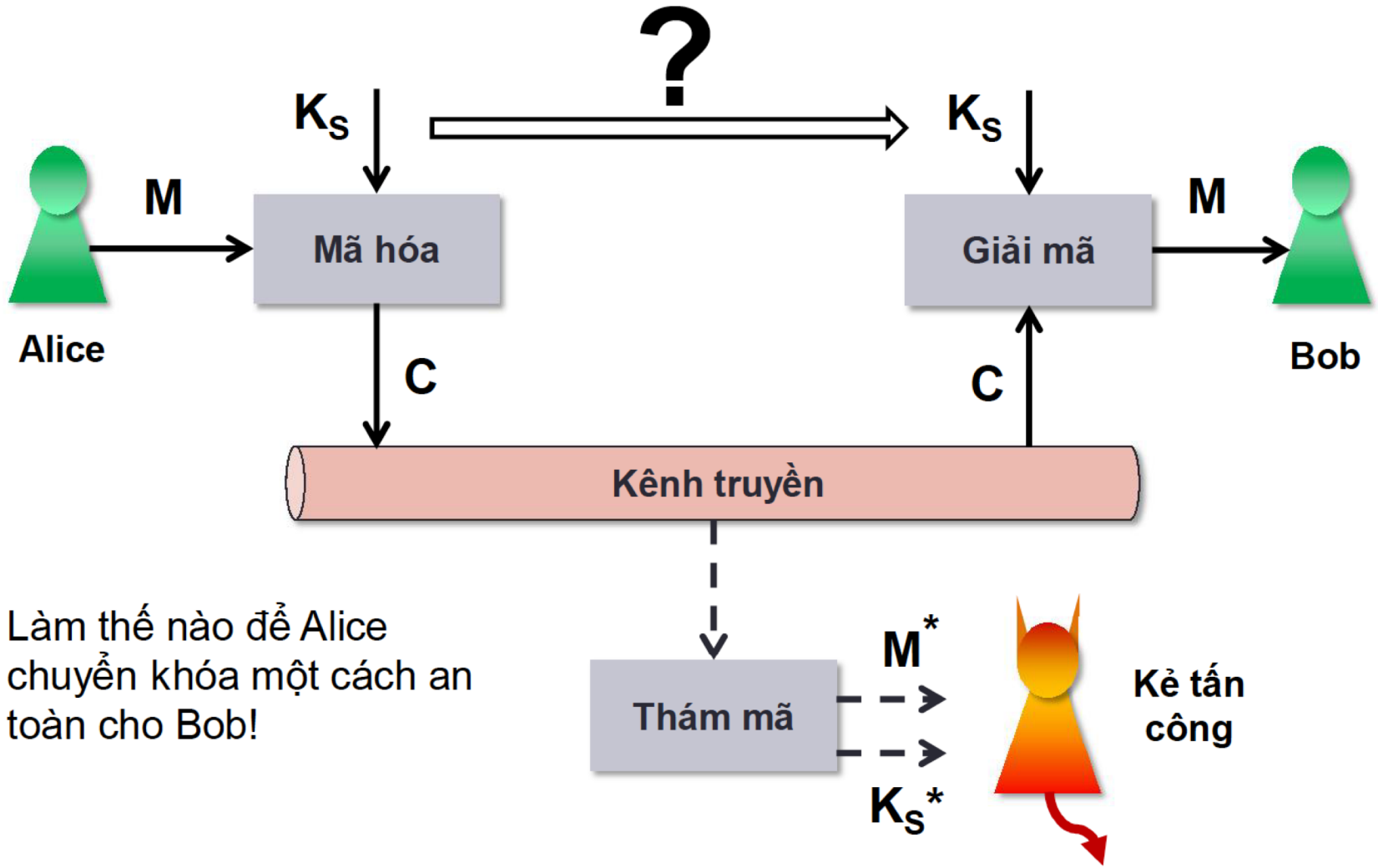
- Để hạn chế lượng thông tin được mã hoá với cùng 1 khoá
- Đảm bảo tính mới của khoá

Các thuật toán trao đổi khoá

- Mục tiêu: Alice, Bob thống nhất được khoá phiên (wo/ interchange key)
  - Khoá phiên không thể gửi dưới dạng plain text
    - Kẻ tấn công có thể đánh cắp
    - Khoá được mã hoá, hoặc được tạo ra từ thông tin trao đổi + một số thông tin bí mật giữa 2 bên (kẻ tấn công không thể biết)
  - Alice, Bob có thể sử dung bên thứ 3 tin cậy
  - Thuật toán cần đảm bảo an toàn với giả sử rằng toàn bộ thuật toán là public
    - Dữ lieu duy nhất không public là các khoá, các thông tin bí mật chỉ Alice và Bob biết
    - Giả sử rang kẻ tấn công có thể lấy được các thông tin trên đường truyền

Các giao thức trao đổi khoá sử dụng hệ mã đối xứng

Sơ đồ bảo mật sử dụng khoá đối xứng



Giao thức trao đổi khoá không tập trung

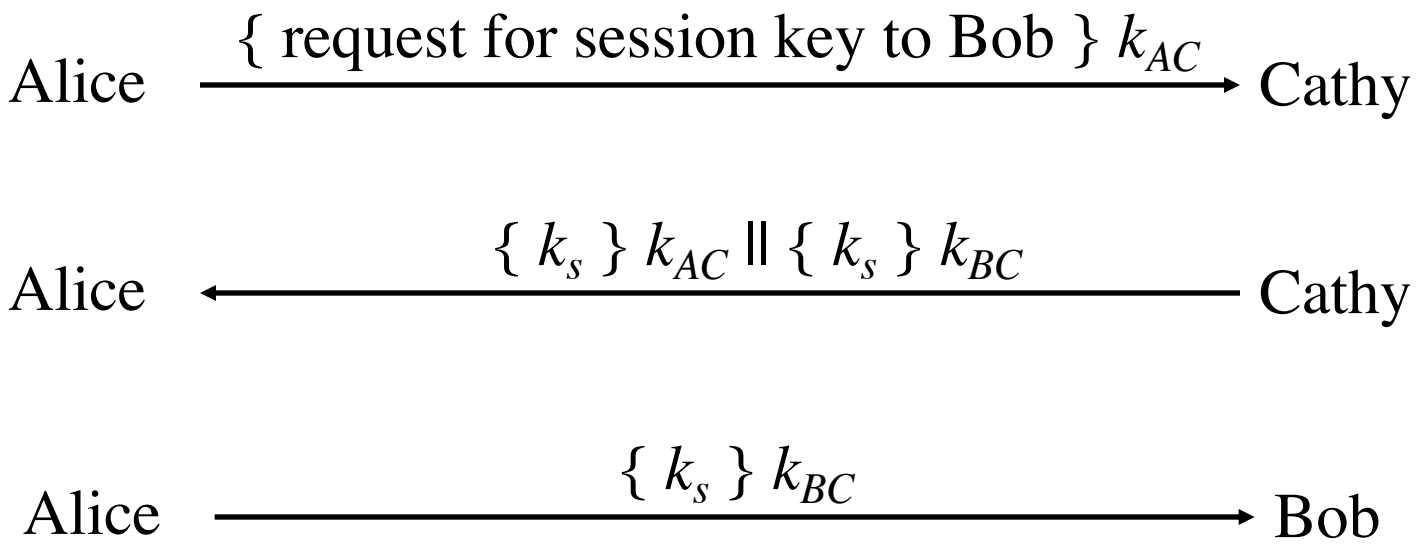
- Khóa chính: K_M đã được A và B chia sẻ an toàn
  - Làm thế nào vì đây chính là bài toán đang cần giải quyết?
  - Khóa chính được sử dụng để trao đổi khóa phiên K_S
- Khóa phiên K_S : sử dụng để mã hóa dữ liệu trao đổi
- Giao thức 1.1
  1. A → B: ID_A
  2. B → A: $E_{K_M}(ID_B, K_S)$
- Giao thức này đã đủ an toàn chưa?
  - Tấn công nghe lén
  - Tấn công thay thế
  - Tấn công giả mạo
  - Tấn công phát lại

Giao thức trao đổi khoá không tập trung

- Giao thức 1.2
  - Sử dụng các yếu tố chống tấn công phát lại (replay attack)
    - A→ B: ID_A, R_1
    - B→ A:$E_{K_M}(ID_B, K_S, R_1, R_2)$
    - A→ B: $E_{K_S}(R_2)$
    - B: kiểm tra lại R_2
- Hạn chế của phân phối khoá không tập trung là gì?

Giao thức trao đổi khoá tập trung

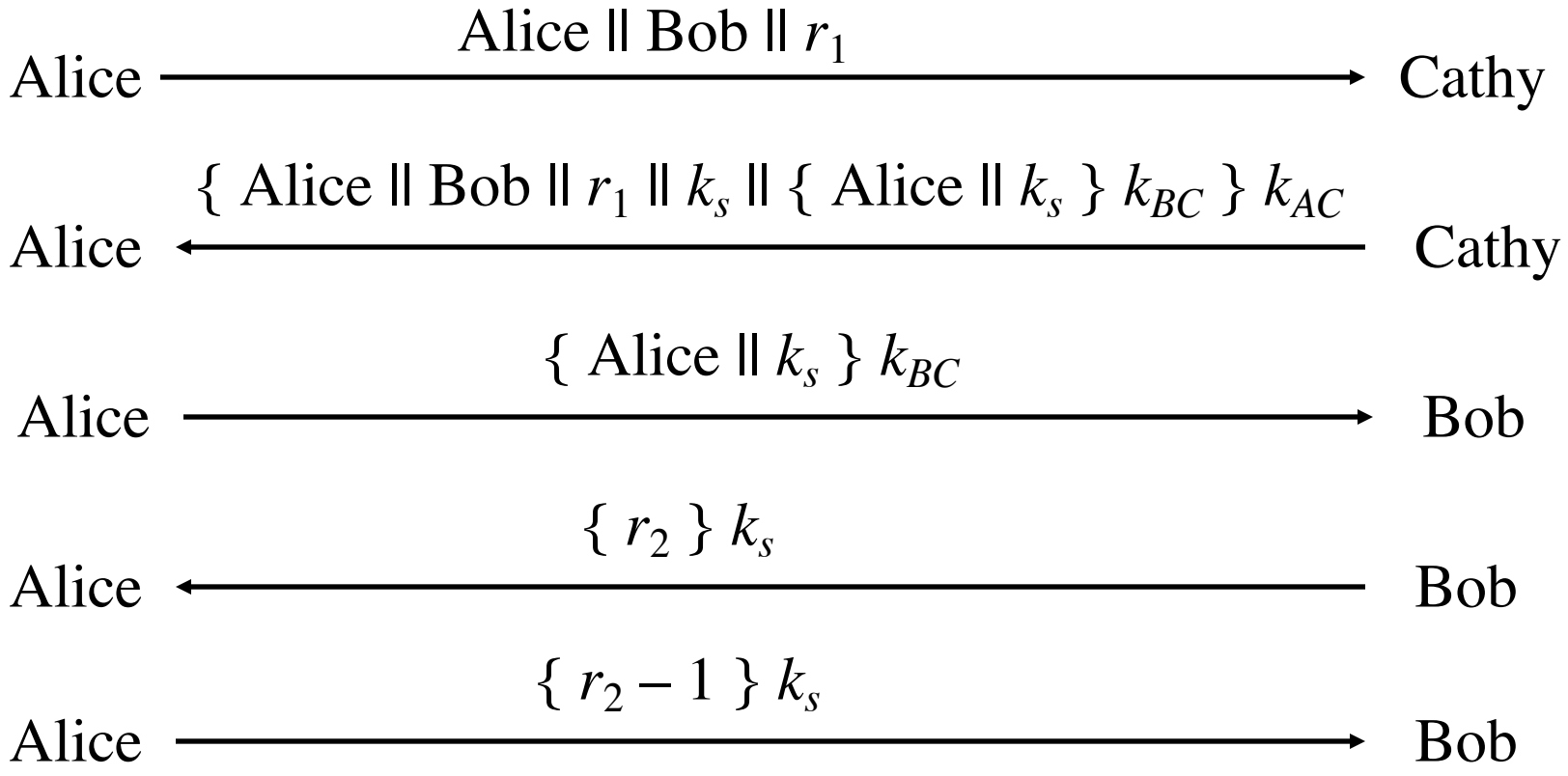
- Các thành phần tham gia
  - Alice, Bob
  - Cathy (Trọng tài): trung tâm phân phối khoá Key Distribution Center (KDC)
- Alice, bob có khoá chung với KDC trước khi tiến hành giao thức



Giao thức trao đổi khoá tập trung

- Vấn đề
  - Làm thế nào để Bob biết người đang nói chuyện với mình là Alice?
  - Replay attack: Eve có thể bắt các gói tin, sau đó gửi lại cho Bob, Bob có thể nghĩ đó là Alice, nhưng không phải
  - Sử dụng lại khoá phiên
    - Bằng cách nào đó Eve biết được khoá phiên trước đó
    - Eve sử dụng lại các gói tin ở step 3→ Bob sử dụng lại khoá phiên
- Giao thức phải có cơ chế xác thực và chống lại replay attack

Giao thức Needham-Schroeder



Giao thức Needham-Schroeder

- Ý nghĩa các bước
  - Gói tin thứ 2
    - Sử dụng khoá chỉ có Alice và cathy biết
    - Cathy và chỉ cathy mới giải mã được
  - Quan hệ với gói tin thứ 1
    - r_1 trong gói thứ 2 chính là r_1 trong gói thứ nhất
  - Gói tin thứ 3
    - Sử dụng khoá bí mật chỉ có bob và cathy biết
      - Chỉ có Bob mới đọc được
      - Chỉ có bob mới biết khoá k_s tất cả các gói tin được mã hoá bởi khoá k_s sau này là từ Bob

Giao thức Needham-Schroeder

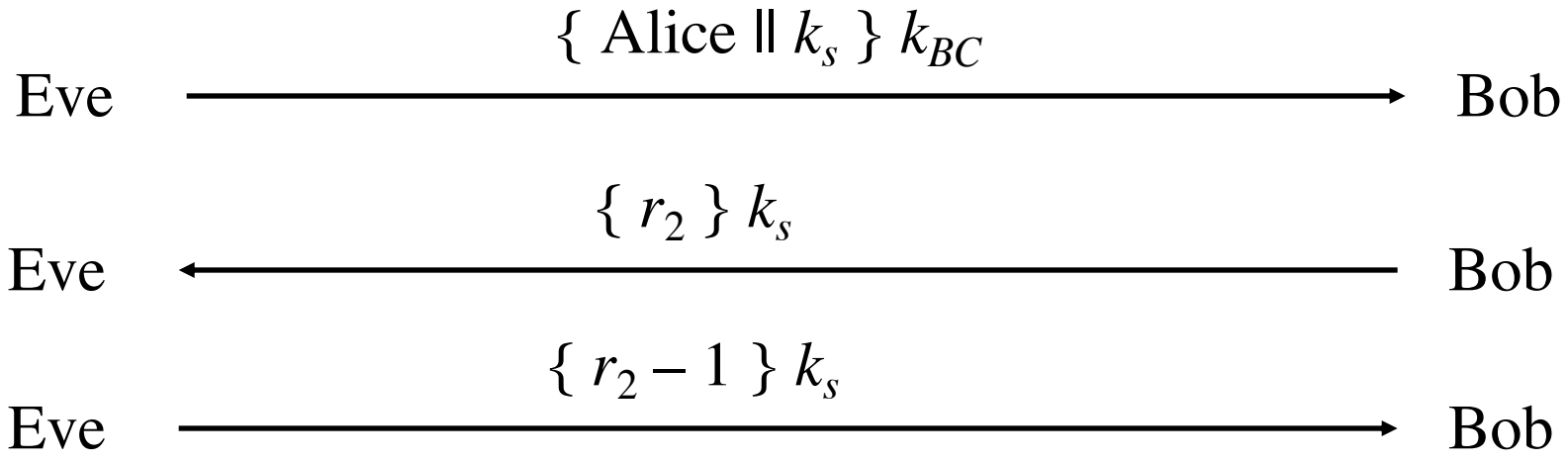
- Ý nghĩa các bước
  - Gói tin thứ 3
    - Sử dụng khoá bí mật chỉ có bob và cathy biết
      - Người mã hoá phải là Cathy
      - Phía trong có tên của Alice và khoá phiên
      - Bob kết luận rằng cathy là người cung cấp khoá, và cathy nói rằng khoá này là dùng cho phiên trao đổi với alice
  - Gói tin thứ 4 và 5:
    - Sử dụng khoá phiên để phát hiện nếu có tấn công replay attack từ eve
    - Nếu không phải là tấn công, Alice phản hồi gói tin thứ 5
    - Nếu là tấn công, Eve không thể giải mã được r_2 vì vậy không thể phản hồi đúng gói tin thứ 5

Giao thức Needham-Schroeder

- Nguy cơ tấn công vào Needham-Schroeder ?

Vấn đề Denning-Sacco

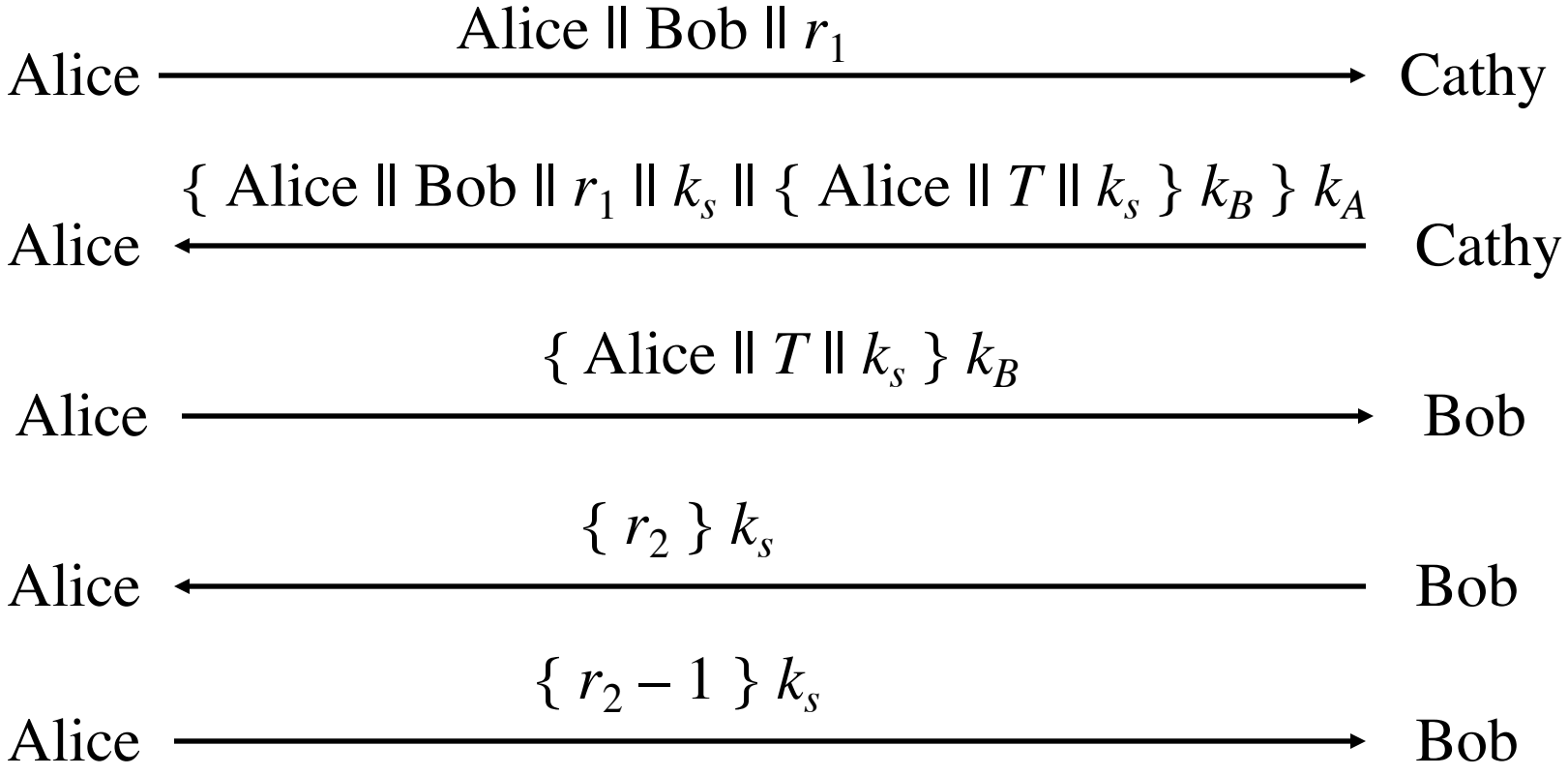
- Nếu bằng cách nào đó, sau đấy Eve biết được khoá k_s. Eve tấn công như sau
  - Eve giả làm Alice, giả mạo bước thứ 3



- Giải pháp ?

Needham-Schroeder with Denning-Sacco Modification

- Thêm timestamp



Needham-Schroeder with Denning-Sacco Modification

- Vấn đề
  - Nếu đồng hồ của các bên không đồng kỳ, các bên có thể reject các gói tin hợp pháp hoặc ngược lại, chấp nhận các gói tin bất hợp pháp
- Sử dung giao thức Use Otway-Rees
  - Tự tìm hiểu

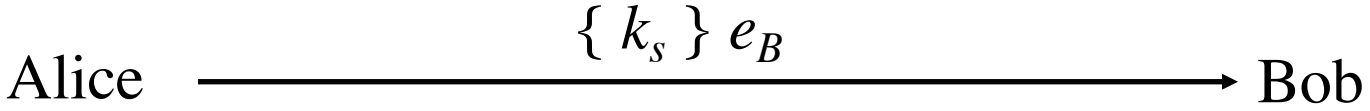
Các giao thức trao đổi khoá sử dụng hệ mã công khai

Trao đổi khoá với mã công khai

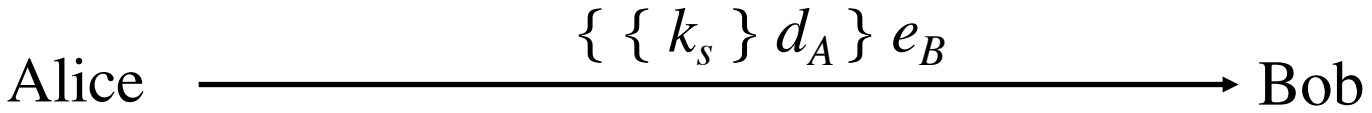
- Giả thiết
  - e_A, e_B: Khoá công khai của Alice và Bob → công khai cho tất cả mọi người
  - d_A, d_B : Khoá bí mật của Alice and → chỉ Alice và Bob biết

Giao thức phân phối khóa không tập trung

- Giao thức đơn giản
  - k_s : khoá phiên



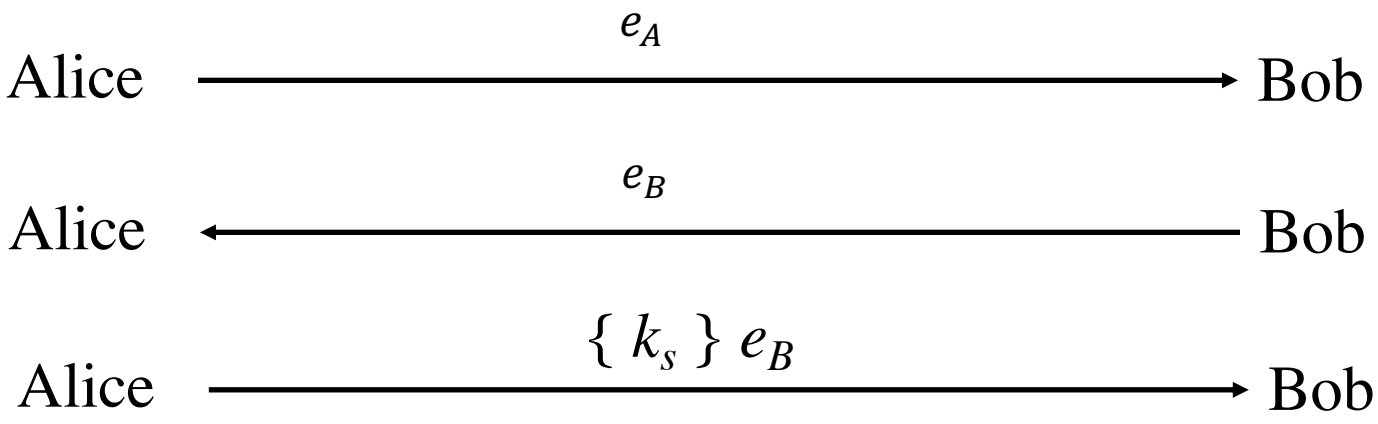
  - Vấn đề
    - Bởi vì e_B là công khai → Bob không biết được đối phương có phải là Alice không
  - Giải pháp đơn giản
    - Sử dụng mã bí mật của Alice



    - Giao thức này có lỗ hổng nào không ?

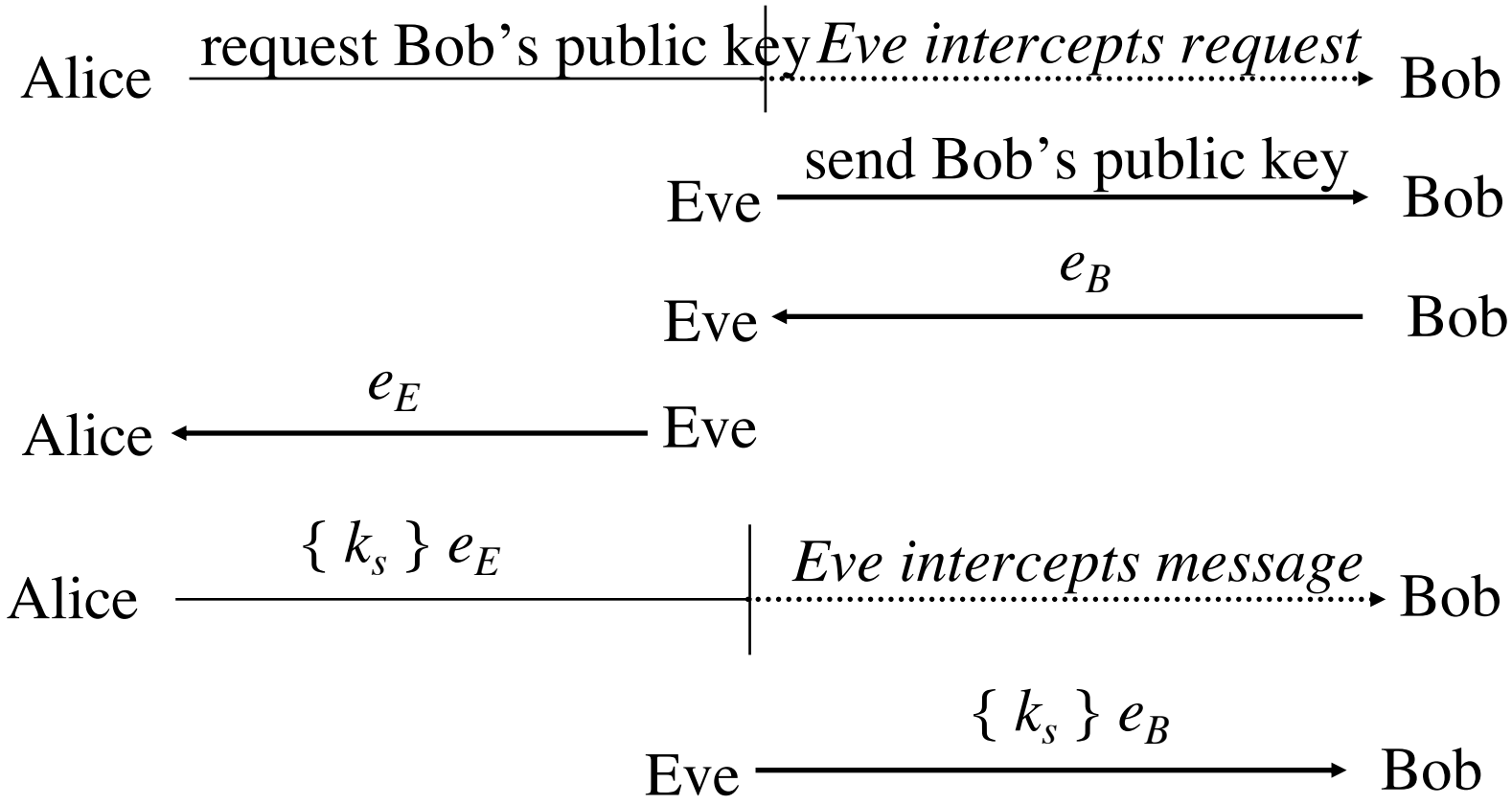
Giao thức phân phối khóa không tập trung

- Nếu Alice và Bob không biết khoá công khai của nhau
  - Trước khi giao dịch, Alice và Bob gửi khoá công khai trực tiếp cho nhau



Tấn công kẻ ngồi giữa
Man-in-the-middle attack

- Eve giả vờ là Bob khi nói chuyện với Alice, giả vờ là Alice khi nói chuyện với Bob



Chống tấn công kẻ ngồi giữa

- Interlock: đề xuất bởi Ron Rivest and AdiShamir
  1. Alice gửi khoá công khai của Alice cho Bob
  2. Bob gửi khoá công khai của Bob cho Alice
  3. Alice mã hoá gói tin của mình bằng khoá công khai của Bob. Alice gửi 1 nửa bản mã cho Bob
  4. Bob mã hoá gói tin của mình bang khoá công khai của Alice. Bob gửi 1 nửa bản mã cho Alice
  5. Alice gửi nửa còn lại của bản mã cho Bob
  6. Bob ghép 2 nửa bản mã lại, giải mã dùng khoá bí mật của Bob. Nếu bản mã được giải mã thành công Bob gửi lại nửa bản mã còn lại ở step 4 cho Alice
  7. Alice ghép 2 nửa bản mã nhận được từ Bob và giải mã
  8. Câu hỏi
     1. Tại sao interlock chống được man in the middle attack

Giao thức phân phối khóa tập trung

- Sử dụng bên thứ 3 tin cậy – PKA (Public Key Authority)
  - Có cặp khóa (e_{PKA}, d_{PKA})
  - Có công khai của A (e_A) và B (e_B)
  - A và B đều có khóa công khai e_{PKA} của PKA
- Giao thức 1
  1. A → PKA: Alice || Bob
  2. PKA → A: $\{Bob||e_B\}d_{KPA}$
  3. A → B: $\{r_1\}e_B$
  4. B → PKA: Alice || Bob
  5. PKA → B: $\{Alice||e_A\}d_{KPA}$
  6. B → A: $\{r_1\}e_A$
- Câu hỏi
  - Kiểm tra tính an toàn của giao thức 1
  - Hạn chế của giao thức này?

Giao thức phân phối khóa tập trung

- Giao thức 2: Bên thứ 3 được tin cậy – CA(Certificate Authority)
  - Có cặp khóa (e_{PKA}, d_{PKA})
  - Phát hành chứng thư số cho khóa công khai của các bên có dạng
    - $Cert_A = \{ID_A || e_A || Time_A\} d_{KPA}$
    - ID_A : định danh của thực thể A
    - e_A: khóa công khai của thực thể A đã được đăng ký tại CA
    - $Time_A$: Thời hạn sử dụng khóa công khai. Thông thường có thời điểm bắt đầu có hiệu lực và thời điểm hết hiệu lực

Giao thức phân phối khóa tập trung

- Giao thức 2: Bên thứ 3 được tin cậy – CA(Certificate Authority)
  1. A → CA: $ID_A||e_A||Time_A$
  2. CA → A: $Cert_A = \{ID_A||e_A||Time_A\}d_{KPA}$
  3. B → CA: $ID_B||e_B||Time_B$
  4. CA → B: $Cert_B = \{ID_B||e_B||Time_B\}d_{KPA}$
  5. A → B: $Cert_A$
  6. B → A: $Cert_B$
- Câu hỏi
  - Cải tiến giao thức trên nhằm tăng cường tính an toàn
    - Gợi ý: dùng các phương pháp kiểm tra tính toàn vẹn, …

Giao thức phân phối khóa tập trung

- Giao thức 2
  1. A → PKA: Alice || Bob || T_1 (T_1: timestamp)
  2. PKA → A: $\{Bob||e_B\}d_{KPA}$
  3. A → B: $\{r_1\}e_B$
  4. B → PKA: Alice || Bob || T_2 (T_2: timestamp)
  5. PKA → B: $\{Alice||e_A\}d_{KPA}$
  6. B → A: $\{r_1\}e_A$
- Ý nghĩa của T_1 và T_2
  - chống tấn công phát lại
- Câu hỏi: giao thức này có hạn chế gì?