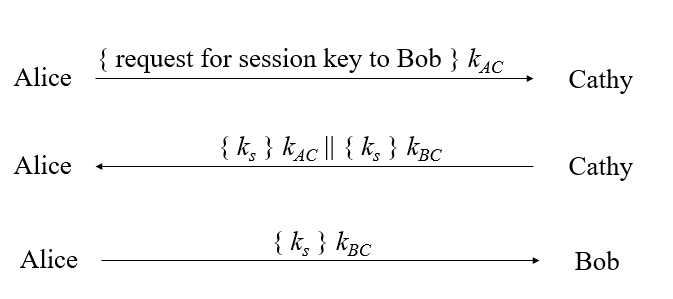
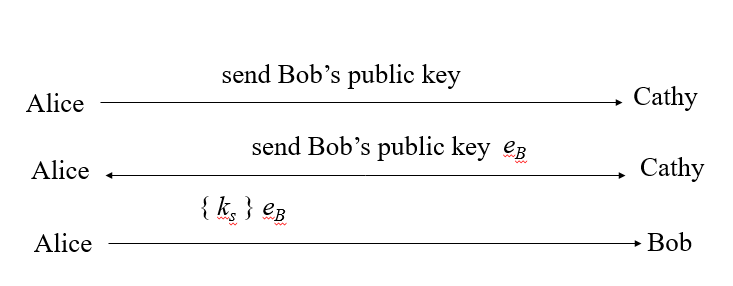
**BUỔI 4: QUẢN LÝ KHÓA – ĐỀ CƯƠNG**

1. Tại sao cần sử dụng khóa phiên
2. Ý nghĩa của trong giao thức Needham-Shroeder. Trình bày chi tiết tấn công với giao thức Needham-Shroeder khi không có
3. Vai trò của bước 4,5 trong giao thức Needham-Shroeder. Trình bày chi tiết tấn công với giao thức Needham-Shroeder khi không hai bước này.
4. Giao thức Needham-Shroeder có điểm yếu gì, có thể khắc phục như thế nào
5. Giả sử A và B có cùng một bên tin cậy thứ 3 là C. A và B muốn thông qua C để thiết lập một khóa phiên với giao thức như sau:



Hãy cho biết giao thức này có điểm yếu gì, có thể khắc phục như thế nào

1. Giả sử A và B không biết khóa công khai của nhau. Tuy nhiên A và B lại có cùng một bên tin cậy thứ 3 là C. A và B muốn thông qua C để lấy khóa công khai của đối phương với giao thức như sau:



Hãy cho biết giao thức này có điểm yếu gì, có thể khắc phục bằng cách nào ?

**BUỔI 4 – GỢI Ý TRẢ LỜI**

*Chú ý: các gợi ý dưới đây chỉ là các ý chính, không phải là câu trả lời đầy đủ. Sinh viên cần tự mình suy nghĩ để tìm ra câu trả lời hoàn chỉnh, đầy đủ.*

1. Các lý do cần sử dụng khóa phiên:

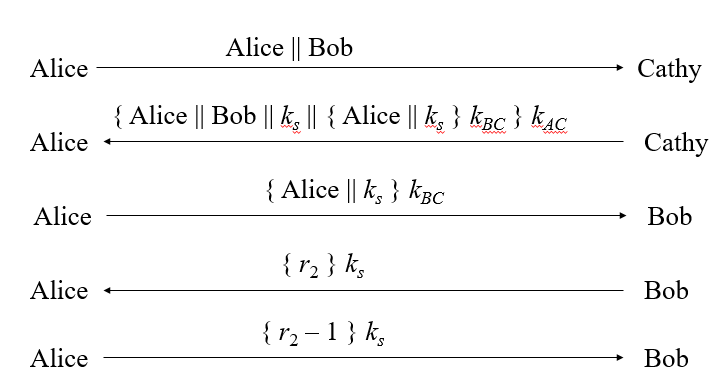
+ Tránh cho các khóa quan trọng bị sử dụng nhiều lần dẫn đến khả năng bị lộ khóa cao (cần nêu thêm lý lẽ chặt chẽ cho nhận định này) .

+ Giúp tính toán đơn giản, nhanh gọn vì mã hóa với khóa phiên là mã hóa đối xứng.

+ Khóa phiên thay đổi liên tục, vì vậy nếu khóa của 1 phiên giao dịch bị lộ sẽ không ảnh hưởng đến các phiên khác

1. là để kiểm tra tính mới của gói tin thứ 2, qua đó chống việc tấn công dùng lại gói tin thứ 2 và giả maọ Cathy.

Giao thức khi không có sẽ như sau:



+ giả sử tại một thời điểm nào đó trong khóa khứ, ví dụ năm 2000, Alice và Bob dùng giao thức trên để trao đổi khóa phiên .

Tại thời điểm đó, kẻ tấn công Eve chưa phá được khóa nên phiên giao dịch lúc đó an toàn.

Tuy nhiên, sau đó một thời gian, ví dụ năm 2016, bằng cách nào đấy kẻ tấn công Eve đã lấy được khóa và lấy được toàn bộ các gói tin đã được trao đổi ở phiên giao dịch năm 2000.

Đến nắm 2017, Alice và Bob sử dụng giao thức trên để trao đổi khóa.

Lúc này, Eve sẽ giả mạo Cathy để lừa Alice và Bob như sau:

Eve chặn gói tin số 1 để không đến được Cathy,

Sau đó, Eve giả mạo Cathy gửi lại gói tin số 2 đã được sử dụng năm 2000.

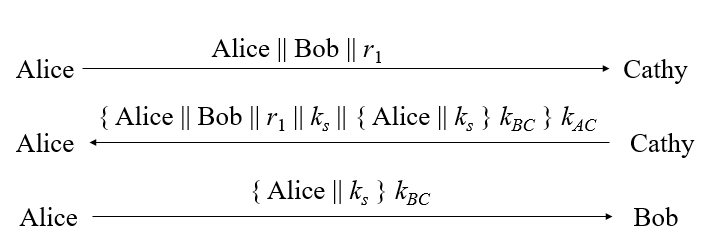
Alice nhận được gói tin gửi từ Eve nhưng cứ nghĩ đấy là gói tin được gửi từ Cathy, vì gói tin này được mã hóa bằng khóa bí mật của Alice và Cathy.

Sau đó, Alice, Bob sẽ tiến hành trao đổi các gói tin 3,4,5 theo đúng giao thức.

Kết quả Alice và Bob sẽ sử dụng lại khóa đã dùng năm 2000. Nguy hiểm ở chỗ, khóa này Eve đã biết. Và như vậy Eve có thể nghe được toàn bộ nội dung trao đổi giữa Alice, Bob hoặc giả mạo 2 Alice, bob.

1. Vai trò của 2 bước 4,5: xem sách giáo trình

Giao thức khi không hai bước 4,5 sẽ như sau:



Với giao thức như thế này, kẻ tấn công có thể tấn công như sau:

Giả sử ở một thời điểm nào đó trong quá khứ, ví dụ năm 2000, Alice và Bob dùng giao thức trên để trao đổi khóa .

Kẻ tấn công Eve bằng cách nào đó thu được toàn bộ các gói tin gửi đi trong cuộc nói chuyện đấy.

Vì Eve muốn chọc phá Bob, nên sau đó, ví dụ năm 2016, đột nhiên gửi gói tin thứ 3 trong giao thức trên cho Bob.

Theo đúng giao thức, Bob sẽ tin đây là gói tin gửi từ Alice. Vì vậy, bob sẽ sử dụng khóa để trao đổi thông tin với Eve (vì nghĩ Eve là Alice).

Eve vì không biết khóa nên không thể giải mã gói tin, nhưng Eve cứ phát lại các gói tin mà Alice đã gửi cho Bob ở phiên giao dịch năm 2000.

Bởi vì các gói tin năm 2000 đều được mã hóa bằng nên khi Bob nhận được, Bob giải mã ra thì vẫn là các bản tin có nghĩa. Vì vậy Bob sẽ tốn thời gian nói chuyện với Eve một cách vô ích.

1. Gợi ý câu trả lời:

+ Ở bước thứ 3, Bob không biết mình nói chuyện với ai.

+ Kẻ tấn công có thể dễ dàng tấn công theo kiểu gửi lại gói tin với kịch bản tương tự như câu 3

+Kẻ tấn công, nếu biết một khóa phiên đã được sử dụng trong quá khứ, có thể tấn công giả mạo Cathy như trong câu 2.

Cách khắc phục: tham khảo giao thức Needham-schoeder. Sử dụng các số số ngẫu nhiên để kiểm tra tính mới của gói tin.

1. Giao thức này có thể dễ dàng bị tấn công theo kiểu kẻ ngồi giữa, xem slide để biết chi tiết cách thức tấn công.

Khắc phục điểm yếu: Giả sử Alice và Bob đều biết khóa công khai của Cathy -> thêm chữ ký điện tử của Cathy vào các gói tin.