20225261
bao.kv225261@sis.hust.edu.vn

1 2 3 4 5
6 7 8 9

Quiz 9. Các giao thức phân phối khóa đối xứng

Homework due Jul 1, 2025 07:00 +07 ***Completed***

Question #5eeb3

1/1 point (graded)

Câu 1. Giá trị khóa nhóm trong sơ đồ trao đổi khóa Diffie-Hellman là (17, 6). Nếu chọn X = 8 thì Y là bao nhiêu?

16 ✔

16

Submit

Question #fa2a0

1/1 point (graded)

Câu 2. Giá trị khóa nhóm trong sơ đồ trao đổi khóa Diffie-Hellman là (17, 6). Nếu Alice chọn XA = 11 và nhận được YB = 12 từ Bob thì giá trị khóa bí mật mà Alice chọn được là bao nhiêu?

6 ✔

6

Submit

Question #70844

1/1 point (graded)

Câu 3. Phát biểu nào sau đây là đúng về sơ đồ trao đổi khóa Diffie-Hellman?

- [ ] Sơ đồ dùng để phân phối khóa công khai một cách tin cậy
- [x] Kẻ tấn công không thể xác định được giá trị riêng X từ giá trị công khai Y
- [x] Nếu kẻ tấn công lấy cắp được giá trị bí mật X, chúng tính được giá trị khóa bí mật Ks của phiên hiện tại
- [ ] Nếu kẻ tấn công lấy cắp được giá trị bí mật X, chúng tính được các giá trị khóa đối xứng Ks của các phiên cũ
- [ ] Nếu kẻ tấn công lấy cắp được giá trị bí mật X, chúng tính được các giá trị khóa đối xứng Ks của các phiên sắp tới khi mà khóa nhóm còn chưa đổi
- [x] Sơ đồ không an toàn do có lỗ hổng các bên không xác thực giá trị công khai Y nhận được

✔

Submit

Question #dc566

1/1 point (graded)

Câu 4. Trong sơ đồ trao đổi khóa Needham-Schroeder, các giá trị dùng 1 lần (nonce) được sử dụng cho mục đích gì?

- [x] Chống tấn công phát lại (Reply attack)
- [x] Khẳng định hai bên sử dụng khóa giống nhau
- [ ] Chống tấn công CPA vào hàm mã hóa
- [ ] Là nhân (seed) để KDC sinh khóa phiên

✔

Submit

Question #8d035

1/1 point (graded)

Câu 5. Trong sơ đồ trao đổi khóa Needham-Schroeder, tại sao cần dùng hàm f(x) để biến đổi giá trị nonce N2?

- [ ] Chống tấn công phát lại (Replay attack)
- [x] Chống tấn công phản xạ (Reflection attack)
- [ ] Chống tấn công CPA vào hàm mã hóa
- [ ] Sinh giá trị khóa phiên

✔

Submit

Question #825c3

1/1 point (graded)

Câu 6. Trong sơ đồ trao đổi khóa cải tiến của Denning, nhãn thời gian T được sử dụng để làm gì?

- [x] Chống tấn công phát lại (Reply attack)
- [ ] Chống tấn công phản xạ (Reflection attack)
- [ ] Sinh giá trị IV (Initial Vector) cho các hàm mã hóa ở chế độ CTR
- [ ] Là nhân (seed) để KDC sinh khóa phiên

✔

Submit

Question #4130c

1/1 point (graded)

Câu 7. Bên cạnh việc sử dụng các cơ chế mật mã một cách an toàn, những thách thức khác cần giải quyết khi triển khai sơ đồ trao đổi khóa của Denning là gì?

- ( ) Đồng bộ đồng hồ giữa các bên
- ( ) Ước lượng thời gian trễ khi truyền tin và xử lý dữ liệu
- (•) Cả 2 vấn đề trên

✔

Submit

Question #9d95e

1/1 point (graded)

Câu 8. Cải tiến của Kehne trong giao thức trao đổi khóa đã giải quyết vấn đề gì khi so sánh với sơ đồ của Denning?

- (•) Đồng bộ đồng hồ giữa các bên
- ( ) Ước lượng thời gian trễ
- ( ) Cả 2 vấn đề trên

✔

Submit

Question #b2a31

1/1 point (graded)

Câu 9. Hạn chế chung của các giao thức phân phối khóa đối xứng dựa trên các hệ mật mã khóa đối xứng là gì?

- [x] Không thỏa mãn yêu cầu về PFS (Perfect Forward Secrecy)
- [ ] Không có cơ chế xác thực thông điệp
- [ ] Số lượng khóa chính tăng theo hàm bậc 2

✔

Submit