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

1 2 3 4 5
6 7 8 9 10

Quiz 8 - Hàm băm và ứng dụng

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

Question #d4cce

1/1 point (graded)

Câu 1. Giả sử H(m) là một hàm băm mật mã an toàn. Người ta muốn tạo ra một hàm băm mới H'(x). Cách thiết kế hàm băm nào sau đây thỏa mãn là hàm 1 chiều?

- [ ] H'(m) = m*m;
- [x] H'(m) = H(H(m))
- [ ] H'(m) = 1/2 số bit đầu tiên của m
- [ ] H'(m) = H(m) mod 100
- [x] H'(m) = H(m) || "end"

✔

Submit

Question #0e936

1/1 point (graded)

Câu 2. Giả sử H(m) là một hàm băm mật mã an toàn. Người ta muốn tạo ra một hàm băm mới H'(x). Cách thiết kế hàm băm nào sau đây có khả năng chống đụng độ?(Chọn tất cả đáp án đúng)

- [ ] H'(m) = m*m;
- [x] H'(m) = H(H(m))
- [ ] H'(m) = 1/2 số bit đầu tiên của m
- [ ] H'(m) = H(m) mod 100
- [x] H'(m) = H(m) || "end"

✔

Submit

Question #b89a9

1/1 point (graded)

Câu 3. Giả sử Alice và Bob đã chia sẻ một khóa bí mật k. Alice gửi cho Bob bản tin E(k, m) || H(E(k, m)), trong đó E là mã hóa AES-CBC còn H là hàm băm mật mã an toàn. Sơ đồ này thỏa mãn (những)yêu cầu nào?

- [x] Tính bí mật (Confidentiality)
- [ ] Tính xác thực toàn vẹn (Integrity)
- [ ] Tính xác thực danh tính (Authenticity)

- [ ] Không thỏa mãn yêu cầu nào

✔

Submit

Question #23b9f

1/1 point (graded)

Câu 4. Giả sử Alice và Bob đã chia sẻ một khóa bí mật k. Alice gửi cho Bob bản tin E(k, m) || H(k || E(k, m)), trong đó E là mã hóa AES-CBC còn H là hàm băm SHA-1. Sơ đồ này thỏa mãn yêu cầu nào?

- [x] Tính bí mật (Confidentiality)
- [ ] Tính xác thực toàn vẹn (Integrity)
- [ ] Tính xác thực danh tính (Authenticity)
- [ ] Tất cả các yêu cầu

✔

Submit

Question #c6452

1/1 point (graded)

Câu 5. Một hàm băm mật mã an toàn có kích thước đầu ra là 50 bit. Chọn trước 1 giá trị băm là x thì xác suất xuất hiện của bản tin m có H(m) = x là bao nhiêu?

- (•) 2^{-50}
- ( ) 2^{-25}
- ( ) 0.02

✔

Submit

Question #cdfd3

1/1 point (graded)

Câu 6. Một hàm băm mật mã an toàn có kích thước đầu ra là 60 bit. Nếu chúng ta có hệ thống máy tính có khả năng thực hiện hàm băm trong 1 ns (nanosecond) thì mất bao nhiêu năm để tìm ra được bản tin m sao cho H(m) = x với x chọn trước?(Ghi đáp án là phần nguyên)

36 ✔

36

Submit

Question #20824

1/1 point (graded)

Câu 7. Khi tấn công dựa trên nghịch lý ngày sinh vào hàm băm SHA-1 để tìm ra các bản tin đụng độ, theo kỳ vọng thì số lượng bản tin phải kiểm tra sẽ giảm đi bao nhiêu lần?

- ( ) 2^{40}
- ( ) 2

- ○ 80
- ○ 2^{80}
- ◉ 2^{79}

✔

Submit

Question #3e0c7

1/1 point (graded)

Câu 8. Một sơ đồ mật mã sử dụng chế độ CBC với khóa k = (k1, k2). Trong đó, k1 được sử dụng để tạo giá trị IV = HMAC(k1, m) còn k2 được sử dụng để mã hóa bản tin E(k2, m). Nếu khóa k được dùng nhiều lần, phát biểu nào sau đây là đúng?

- ○ Sơ đồ này chống được tấn công CCA
- ◉ Sơ đồ này không chống được tấn công CPA
- ○ Sơ đồ này không chống được tấn công KPA
- ○ Sơ đồ này không chống được tấn công CCA nhưng chống được tấn công CPA

✔

Submit

Question #e37c9

1/1 point (graded)

Câu 9. Khóa nào trong cặp khóa được sử dụng để tạo chữ ký số dùng mật mã khóa công khai?

- ◉ Khóa riêng của người gửi
- ○ Khóa công khai của người gửi
- ○ Khóa công khai của người nhận
- ○ Khóa riêng của người nhận

✔

Submit

Question #a1c78

1/1 point (graded)

Câu 10. Chữ ký số cung cấp được (những) dịch vụ gì mà các hàm MAC không có?

- ☑ Chống từ chối (Nonrepudiation)
- ☐ Chống tấn công phát lại
- ☐ Toàn vẹn (Integrity)
- ☐ Xác thực (Authenticity)

✔

Submit
