Started on	Sunday, 12 March 2023, 9:46 PM
State	Finished
Completed on	Sunday, 12 March 2023, 10:01 PM
Time taken	14 mins 54 secs

Question **1**

Complete

Marked out of 1.00

Thuật toán Euclide mở rộng, hay GCD mở rộng là:

- [x] Có thể sử dụng để tính nghịch đảo đồng dư trong điều kiện thích hợp
- [ ] Là công cụ đảm bảo cho tính an toàn của hệ mật mã RSA
- [x] Tính ước chung lớn nhất g của 2 số và a & b và tìm biểu diễn dạng tổ hợp tuyến tính của g theo a&b
- [ ] Tính ước số chung lớn nhất của 2 số a & b rồi qua đó tìm nghịch đảo của a theo b

Question **2**

Complete

Marked out of 1.00

Hãy cho biết đâu là chuỗi sắp xếp theo thứ tự về mức độ bảo mật

a. Adhoc security, Computational Security, Unconditional security , Provable Security

b. Unconditional security, Adhoc security, Provable Security, Computational Security

c. Computational Security, Provable Security, Unconditional security

d. Provable Security, Computational Security, Unconditional security

Question **3**

Complete

Marked out of 1.00

Hai chế độ mật mã nào có khả năng đáp ứng tính toán song song

a. ECB và OFB

b. CBC và CTR

c. ECB và CTR

d. OFB và CTR

Question **4**

Complete

Marked out of 1.00

Hãy tìm mệnh đề đúng nhất dưới đây

Người ta giả mạo văn bản có chữ ký điện tử thông qua một quá trình:

a. Xuất phát từ một văn bản gốc, tìm cách thêm/bớt các dấu trắng ở rất nhiều vị trí để sinh ra nhiều văn bản, từ đó tìm được 2 văn bản có cùng giá trị băm

b. Người ta xây dựng 2 tập văn bản có nội dung là đối lập nhau theo 1 nghĩa nào đó và đồng thời băm rồi tìm 2 văn bản có cùng giá trị băm

c. Tìm hai văn bản có nội dung khác nhau mà có giá trị băm giống nhau

d. Tìm hai văn bản có cùng giá trị băm và có nội dung cùng chủ đề nhưng khác biệt trên một vài yếu tố quan trọng

Question **5**

Complete

Marked out of 1.00

Hãy chọn ra mệnh đề đúng

a. Nghịch đảo của 7 theo mod 20 là 3 và theo mod 37 là 16

b. Với p=11, q=13 và e= 7 thì ta xác định d= 105

c. Nghịch đảo của 7 theo mod 50 là 7 và theo mod 37 là 16

d. Nghịch đảo của 7 theo mod 105 là không xác định vì 105 không phải là số nguyên tố

e. Nghịch đảo của 7 theo mod 105 là 3 và theo mod 37 là 16

Question **6**

Complete

Marked out of 2.00

Một hệ thống điều khiển truy nhập theo mô hình $RBAC_1$ có 4 tệp hệ thống A, B, C, D và có các vai trò được ký hiệu là P,Q,R,S. Trong biểu diễn toán học của mô hình này, người ta xác định quan hệ Permission Assignment (PA) là tập các phần tử bộ 3 xác định quyền khai thác (permission) như sau:

(P, A, RW), (P, B, RX), (P,C, RWX), (Q,A, RX), (Q,B,O), (Q,C,RX), (Q,D,O), (R, A, RWX), (R,B, ORX), (R, C, RWX), (S, A, R), (S,B,RX), (S, C,RX), (R,D,O)

Trong giai đoạn khởi đầu hệ thống này chỉ có 4 người khai thác với các vai trò như sau: Alice có vai trò R, Bob có vai trò P, Cathy có vai trò Q, còn Dave có vai trò S.
Em hãy tìm ra những mệnh đề có khả năng đúng dưới đây.

- [ ] a. Bob không là sếp của ai cả
- [x] b. Alice là sếp của Bob nhưng không phải của Cathy
- [ ] c. Alice có quyền Read, Write và eXecute với tệp hệ thống A
- [ ] d. Tệp hệ thống D chỉ có 1 người làm chủ
- [x] e. Dave làm việc dưới quyền của tất cả những người khác
- [ ] f. Bob không làm việc dưới quyền Cathy nhưng dưới quyền Alice
- [ ] g. Alice có thể là sếp của tất cả

Question **7**

Not answered

Marked out of 3.00

Một thầy giáo nêu lên một vấn đề chung là cần xây dưng giải pháp xác thực thông tin (thông điệp) trong hầu hết các dich vụ và ứng dụng mạng trong thực tế, tuy nhiên tùy theo từng tình huống thực tế, công cụ mật mã được lựa chọn để xây dựng giải pháp xác thực có thể khác nhau. Thầy yêu cầu sinh viên thử nêu lên những vấn đề ứng dụng cụ thể và công cụ mật mã cho xác thực thông điệp phù hợp. Alice nêu ứng dụng thư điện tử email và Bob nêu một ứng dụng truyền thông đa phương tiện với những giải pháp xác thực sử dụng công cụ mật mã khác nhau. Thầy giáo đồng ý với cả 2 bạn. Em hãy thử suy đoán xem các công cụ mật mã nào được 2 bạn đề xuất cho bài toán ứng dụng tương ứng và phân tích sự hợp lý của mỗi lựa chọn.

◄ Announcements

Jump to...