Bài kiểm tra Nhập môn ATTT số 1

Immersive Reader

Nội dung ở chương mở đầu và chương mật mã khoá đối xứng

Points:
14/20

1.Dịch vụ xác thực nguồn gốc thông điệp sử dụng những cơ chế ATTT nào ?Required to answer. Single choice.

Immersive Reader

(1/1 Point)

- Bảo mật, trao đổi xác thực, kiểm soát truy cập
- Bảo mật, ký số
- Bảo mật, ký số, toàn vẹn dữ liệu

2.Chọn những ý cho thấy sự khác nhau giữa tấn công thụ động và tấn công chủ động vào hệ thống thông tin làRequired to answer. Multiple choice.

Immersive Reader

(1/1 Point)

- Cùng làm thay đổi dữ liệu và hoạt động của hệ thống
- Tấn công thụ động dẫn tới giả mạo thông tin, còn tấn công chủ động làm thay đổi hoạt động
- Tấn công chủ động thay đổi dữ liệu và hoạt động của hệ thống
- Tấn công thụ động không gây nên sự thay đổi dữ liệu, nhưng làm ảnh hưởng hoạt động httt
- Tấn công thụ động không làm thay đổi hoạt động và dữ liệu hệ thống

3.QuestionKiên trúc an toàn thông tin OSI tập trung vào các vấn đêRequired to answer. Multiple choice.

Immersive Reader

(1/1 Point)

- Tấn công, cơ chế an toàn thông tin, dịch vụ an toàn thông tin
- Tấn công, mật mã, dịch vụ bảo mật và xác thực, khả năng ngăn chặn tấn công
- Cơ chế an toàn thông tin, dịch vụ an toàn thông tin, khả năng ngăn chặn tấn công

4.Lựa chọn những dạng tấn công là chủ độngRequired to answer. Multiple choice.

Immersive Reader

(1/1 Point)

- Nghe lén, sửa đổi nội dung thông điệp
- Phân tích lưu lượng truyền tải, tấn công từ chối dịch vụ
- Tấn công từ chối dịch vụ, giả mạo thông tin
- Sửa đổi nội dung, Chặn giữ thông điệp
- Tấn công phát lại, tấn công mạo danh

5.Phân loại các dạng tấn công thụ độngRequired to answer. Multiple choice.

Immersive Reader

(1/1 Point)

- Phát lộ nội dung thông điệp
- Giả mạo thông điệp
- Đệm luồng truyền tải
- Phân tích lưu lượng luồng truyền tải
- Chặn giữ thông điệp
- Gián đoạn truyền tin

6.Lựa chọn những chức năng ATTT trong mô hình an toàn thông tin hệ thốngRequired to answer. Single choice.

Immersive Reader

(1/1 Point)

- Ngăn chặn tấn công, phát hiện tấn công, phát hiện lỗ hổng hệ thống
- Đảm bảo tính sẵn sàng, kiểm soát truy cập, kiểm tra toàn vẹn thông điệp
- Mã hoá, giải mã, chia sẻ thông tin bí mật
- Phục hồi hệ thống, ngăn chặn tấn công, xác thực thông điệp
- Phân tích luồng lưu lượng, nghe lén, tấn công từ chối dịch vụ

7.Bên thứ ba được uỷ quyền trong mô hình an toàn truyền tải dữ liệu có chức năngRequired to answer. Multiple choice.

Immersive Reader

(0/1 Point)

- Chia sẻ thông tin bí mật cho các bên
- Xác nhận các bên tham gia trao đổi thông tin
- Mã hoá, giải mã thông điệp bí mật
- Thực hiện thám mã nội dung thông điệp
- Cấp phát chứng nhận các bên
- Quản trị và trao đổi khoá bí mật

8.Bộ tạo số ngẫu nhiên trong mô hình hệ mật khoá đối xứng có tác dụng:Required to answer. Single choice.

Immersive Reader

(1/1 Point)

- Tăng kích thước của khoá
- Tăng khả năng phân tích nội dung thông điệp
- Làm giảm kích thước của bản tin mật
- Tăng tính nhập nhằng trong mã hoá
- Tăng tốc độ tính toán khi thực hiện mã hoá-giải mã

9.Tính mật thực tiễn phụ thuộc vàoRequired to answer. Multiple choice.

Immersive Reader

(1/1 Point)

- [ ] Thời gian giải mật của bản tin mật
- [ ] Thời gian cần giữ bí mật thông điệp
- [ ] Giá trị của nội dung thông điệp
- [ ] Khả năng đối phương biết được khoá
- [ ] Những thông tin đối phương biết về bản tin rõ

10.Cấu trúc hệ mật khoá đối xứng gồm những thành phần nào dưới đâyRequired to answer. Multiple choice.

Immersive Reader

(0/3 Points)

- [ ] Khối mã hoá, khối giải mã
- [ ] Nguồn tin
- [ ] Thám mã
- [ ] Nhận tin
- [ ] Mạng máy tính
- [ ] Khối tạo sinh khoá
- [ ] Kênh truyền tin
- [ ] Khối tạo số ngẫu nhiên
- [ ] Kênh mật
- [ ] Kênh mật phân phối khoá

11.Phương pháp DES cóRequired to answer. Single choice.

Immersive Reader

(1/1 Point)

- Khoá dài hơn bản rõ
- Khoá bằng bản rõ
- Khoá ngắn hơn bản rõ

12.Thuật toán mật mã cần đủ mạnh để chống lại dạng tấn công nàoRequired to answer. Single choice.

Immersive Reader

(0/1 Point)

- Tấn công "Chỉ biết bản tin mật"
- Tấn công "Bản rõ đã biết"
- Tấn công "Bản rõ chọn trước"
- Tấn công "Bản mã chọn trước"
- Tấn công "Văn bản tuỳ chọn"

13.Điều kiện cần để hệ mật hoàn hảo làRequired to answer. Single choice.

Immersive Reader

(1/1 Point)

- Bản mật chứa một phần thông tin về bản rõ
- Bản mật và bản rõ độc lập thống kê
- Khoá phải phải có độ dài đủ lớn
- Khoá có thể được dùng nhiều lần

14.Làm thế nào để tăng tính an toàn của hệ mật không hoàn hảoRequired to answer. Multiple choice.

Immersive Reader

(0/1 Point)

- [ ] Khoá có độ dài bằng độ dài bản tin rõ
- [ ] Khoá sử dụng một lần
- [ ] Bản tin mật được nén lại
- [ ] Nén bản tin rõ
- [ ] Giảm entropy của bản tin rõ

15.Những câu nào dưới đây có trong mô tả cấu trúc mã khốiRequired to answer. Multiple choice.

Immersive Reader

(1/1 Point)

- [ ] Tính nhập nhằng dựa trên quan hệ tuyến tính
- [ ] Hàm thay thế dùng để tăng tính nhập nhằng
- [ ] Toàn bộ nội dung thông tin bản rõ phải được chứa trong các bit đầu tiên của bản mật
- [ ] Cấu trúc nhập nhằng dựa trên hàm phi tuyến
- [ ] Thông tin bản rõ được khuếch tán vào tất cả các bít của bản tin mật

16.Cho hệ mã Caesar mở rộng C=E([n,k],p)=np+k mod 26, p là ký tự bản rõ. Hãy thực hiện mã chuỗi ký tự "affine" với n=5, k=7. Chuỗi ký tự mã "rveqbo" tương ứng với bản rõ nào ? Ghi kết quả cách nhau bằng dấu ",".Required to answer. Single line text.

Immersive Reader

(3/3 Points)

Enter your answer

hggvub, cipher