1.Dịch vụ xác thực nguồn gốc thông điệp sử dụng những cơ chế ATTT nào ?
(1/1 Points)

- 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 là
(1/1 Points)

- 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.Kiến trúc an toàn thông tin OSI tập trung vào các vấn đề
(1/1 Points)

- ***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 động
(0/1 Points)

- 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 động
(0/1 Points)

- ***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 thống
(1/1 Points)

- ***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 năng

(1/1 Points)

- **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:

(1/1 Points)

- 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 vào

(1/1 Points)

- 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 đây

(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
- [x] **Kênh mật phân phối khoá**

11.Phương pháp DES có
(1/1 Points)

- ( ) 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 nào
(0/1 Points)

- (•) 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 là
(1/1 Points)

- ( ) 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 hảo
(1/1 Points)

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

15.Những câu nào dưới đây có trong mô tả cấu trúc mã khối
(1/1 Points)

- [ ] Tính nhập nhằng dựa trên quan hệ tuyến tính
- [x] **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
- [x] **Cấu trúc nhập nhằng dựa trên hàm phi tuyến**
- [x] **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 ",".
(0/3 Points)

hqqvub,cipher

Correct answers: **hggvub,cipher**, hggvub, cipher, "hggvub","cipher", "hggvub", "cipher", hggvub cipher, hggvub,cipher.

Chương 2: Mật mã khóa công khai

1.Cơ sở của các hệ mật khoá công khai dựa trên:
Bắt buộc trả lời
Một lựa chọn
(1/1 Điểm)

- Phép thế, hoán vị, hàm một chiều
- **Bài toán khó, hàm một chiều, thông tin cửa bẫy**
- Bài toán khó, hàm một chiều, hàm phi tuyến
- Hàm một chiều, khả năng khó giả mạo, khoá khó đoán

2.Quá trình xác thực nguồn gốc thông điệp trong truyền tin từ A đến B
Bắt buộc trả lời
Một lựa chọn
(1/1 Điểm)

- Sử dụng khoá riêng của B
- Sử dụng khoá công khai của A
- Sử dụng khoá công khai của B
- **Sử dụng khoá riêng của A**

3.Tong hệ mật khoá công khai, để bảo mật truyền dữ liệu gửi từ A đến B cần:
Bắt buộc trả lời
Một lựa chọn
(1/1 Điểm)

- Sử dụng khoá công khai của A
- **Sử dụng khoá công khai của B**
- Sử dụng khoá phiên do A tạo ra
- Xin cấp phát khoá phiên từ bên thứ 3

- Sử dụng khoá riêng được phân phối của B

4.Khoá chính (master key) thường dùng trong
Bắt buộc trả lời
Một lựa chọn
(1/1 Điểm)

- **Phân phối khoá phiên**
- Xác thực khoá công khai
- Phân phối khoá riêng kèm chứng thư số

5.Lựa chọn những câu trả lời đúng: Hệ mật RSA là
Bắt buộc trả lời
Nhiều lựa chọn
(1/1 Điểm)

- [x] **Phương pháp mật mã khối**
- [ ] Sử dụng thay thế để làm tăng tính nhập nhằng
- [x] **Sử dụng bài toán khó phân tích số**
- [ ] Sử dụng khoá mật có độ dài 256 bit
- [ ] Sử dụng đường cong Elliptic

6.Hãy tính d trong quá trình sinh khoá RSA vớp p=53, q=83, chọn e=17.
Bắt buộc trả lời
Văn bản một dòng
(3/3 Điểm)

1505

1505
7.Trong quá trình sinh khoá RSA, tính khó trong dự đoán khoá riêng phụ thuộc vào

Bắt buộc trả lời
Một lựa chọn
(2/2 Điểm)

- Giải phương trình nghiệm nguyên tìm d khi biết e
- **Độ lớn của các số nguyên tố p và q**
- Phép toán luỹ thừa trong quá trình mã hoá, giải mã

8.Tác dụng của các số N1, N2 trong sơ đồ phân phối khoá đối xứng giữa hai bên A và

B là
Bắt buộc trả lời
Nhiều lựa chọn

(2/2 Điểm)

- [x] **N1 dùng để xác thực phiên làm việc, N2 dùng để xác thực hai bên**
- [x] **N1 dùng để chống tấn công Replay**
- [ ] N2 dùng để định danh cho bên B
- [ ] N1 là định danh của yêu cầu tạo khoá
- [x] **Khoá phiên từ KDC tới B do A gửi**

9.Cơ chế cân bằng tải lượng giao dịch trong sơ đồ phân phối khoá đối xứng để
Bắt buộc trả lời
Nhiều lựa chọn
(2/2 Điểm)

- [x] **Đảm bảo hiệu năng hoạt động của hệ thống**
- [x] **Để chống tấn công phân tích và định vị**
- [ ] Giảm khả năng giả mạo trong hệ thống phân phối khoá
- [ ] Chống tấn côgn replay
- [ ] Giảm nguy cơ rò rỉ thông tin

10.Qúa trình xác thực trong sơ đồ phân phối khoá đối xứng tập trung nằm ở các pha:

Bắt buộc trả lời
Một lựa chọn
(2/2 Điểm)

- ○ Pha xác thực lẫn nhau hai bên qua giao thức challenge/response
- ◉ **Pha xác thực lẫn nhau hai bên qua giao thức challenge/response, pha xác thực các bên với trung tâm KDC**
- ○ Pha gửi khoá phiên giữa KDC và các bên tham gia trao đổi dữ liệu

11.Chứng thư số dùng để
Bắt buộc trả lời
Nhiều lựa chọn
(0/1 Điểm)

- [x] **Chống giả mạo khoá công khai**
- [ ] Giảm nguy cơ tấn công vào khoá riêng
- [x] **Giảm tải cho trung tâm quản lý giao dịch**
- [ ] Xác định thông tin người sử dụng

12.Danh sách chứng thư số bị thu hồi CRL:
Bắt buộc trả lời
Một lựa chọn

(1/1 Điểm)

- Chứa thời hạn hiệu lực của chứng thư số
- Chứa các chứng thư số hết hạn
- **Chứa chứng thư số bị thu hồi trước hạn**

13.Bên cấp phát chứng thư số bảo vệ danh sách CRL bằng
Bắt buộc trả lời
Một lựa chọn
(1/1 Điểm)

- Bảo mật danh sách CRL
- **Chống giả mạo và sửa đổi danh sách bằng chữ ký số**
- DÙng cả hai phương pháp trên

14.Trên chứng thư số, việc chống giả mạo khoá công khai được xác định qua
Bắt buộc trả lời
Nhiều lựa chọn
(1/1 Điểm)

- **Chữ ký số của bên cấp phát chứng thư số**
- **Khoá riêng của bên cấp phát chứng thư số**
- Định danh của người được cấp phát
- Khoá công khai của người sở hữu chứng thư số
- Thời gian hiệu lực của chứng thư số

Quay lại trang cảm ơn