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)

- [x] Chữ ký số của bên cấp phát chứng thư số
- [x] 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