CÂU HỎI CHƯƠNG VI
Môn: MẬT MÃ VÀ AN NINH MẠNG
-o0o-

I. Câu hỏi
1. Các dịch vụ được PGP cung cấp là gì?
2. Vì sao PGP tạo chữ ký trước khi thực hiện nén dữ liệu?
3. Cho biết thuật toán Radix-64 làm gì?
4. Cho biết các giao thức trong SSL.
5. Cho biết khác biệt giữa một kết nối SSL và một phiên SSL.
6. Liệt kê và và định nghĩa ngắn gọn các thành phần trong SET.
7. Chữ ký đôi là gì và mục đích của nó?

II. Câu hỏi trắc nghiệm
1. Chọn phát biểu sai trong các phát biểu sau khi PGP được sử dụng trong một hệ thống E-mail:
a. Hệ thống E-mail nói trên sẽ cung cấp các dịch vụ xác thực, bí mật, nén, tương thích e-mail và phân mảnh.
b. Nếu dùng dịch vụ bí mật thì thông điệp gởi đi sẽ có mã hóa ở một số khối dữ liệu.
c. Nếu chỉ dùng dịch vụ xác thực thì thông điệp gởi đi sẽ không có mã hóa ở bất kỳ khối dữ liệu nào.
d. Nếu dùng dịch vụ tương thích e-mail thì mỗi nhóm 3 byte dữ liệu nhị phân được ánh xạ thành 4 ký tự ASCII.

2. Khi cần truyền một thông điệp và dùng cả hai dịch vụ bí mật và xác thực của PGP thì phần nào sẽ được mã hóa đối xứng bằng khóa phiên?
a. Thông điệp.
b. Tóm tắt thông điệp.
c. Chữ ký số trên thông điệp.
d. Thông điệp và chữ ký số trên thông điệp.

3. Khóa được sử dụng để mã hóa khóa phiên trong PGP khi dùng trên hệ thống E-mail là:
a. Khóa công khai của người gởi.
b. Khóa riêng của người gởi.
c. Khóa công khai của người nhận.
d. Khóa riêng của người nhận.

4. Chế độ hoạt động của PGP khi thực hiện mã hóa đối xứng là:
a. CBC b. ECB c. CFB d. OFB

5. Thuật toán mã hóa nào sau đây là phù hợp với mã hóa đối xứng của PGP:
a. DES
b. 3DES với 2 khóa
c. AES
d. Cả câu (b) và (c) đều đúng

6. SSL có không có khả năng chống lại loại tấn công nào sau đây:
a. Password Sniffing
b. Man-in-the-Middle
c. Replay
d. SYN Flooding

DDoS

7. Cho biết giao thức nào sau đây không có trong SSL:
a. SSL Message Protocol.
b. SSL Record Protocol.

c. SSL Handshake Protocol.
d. SSL Change Cipher Spec Protocol.

8. Chọn phát biểu sai trong các phát biểu sau khi nói về kết nối SSL(SSL connection) và phiên SSL(SSL session):
a. Một kết nối SSL có một hoặc nhiều phiên SSL.
b. Một kết nối SSL định nghĩa một bộ các tham số liên quan đến mã hóa và được chia sẻ giữa nhiều phiên SSL.
c. Kết nối SSL được sử dụng để tránh tốn kém trong việc đàm phán các tham số liên quan đến bảo mật cho mỗi phiên SSL.
d. Các câu trên đều sai.

9. Cho biết phát biểu sai về chữ ký đôi(dual signature) trong các phát biểu sau:
a. Mục đích của dual signature là để liên kết hai thông điệp dành cho hai nơi nhận khác nhau.
b. Đối với giao dịch điện tử an toàn, dual signature được dùng để ký trên hai tài liệu gồm thông tin thanh toán (payment information – PO) và thông tin đặt hàng (order information – OI).
c. Đối với giao dịch điện tử an toàn, dual signature được dùng nhằm để ngân hàng không thể biết được mã băm của tài liệu đặt hàng.
d. Dual signature được dùng để ký trên hai tài liệu nối với nhau và mỗi tài liệu này có mã băm riêng.

10. Cho biết thành phần tham gia trong giao dịch điện tử an toàn (SET- Secure Electronic Transaction) có trách nhiệm thanh toán các khoản mua hàng của chủ thẻ.
a. Cardholder.
b. Issuer.
c. Merchant.
d. CA.