CÂU HỎI ÔN TẬP

1. . Văn bản sau khi được mã hóa, được gọi là gì ?

   a. Văn bản mã

   b. Khóa công khai

   c. Mật mã đối xứng

   d. Chứng chỉ

2. . Đặc tính nào sau đây không thuộc chức năng bảo mật thông tin trong các hệ thống mật mã ?

   a. Hiệu quả

   b. Bảo mật

   c. Toàn vẹn

   d. Không chối từ

3. . Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng cùng một khóa mã khi mã hóa và giải mã ?

   a. Không đối xứng

   b. Đối xứng

   c. RSA

   d. Diffie-Hellman

4. . Chuẩn nào sau đây được chính phủ Mỹ sử dụng thay thế cho DES như là một chuẩn mã hoá dữ liệu?

   a. DSA

   b. ECC

   c. 3DES

   d. AES

5. . Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng các khóa khác nhau khi mã hóa và giải mã ?

   a. Đối xứng

   b. Không đối xứng

   c. Blowfish

   d. Skipjack

6. . Các giao thức mã hóa và các thuật toán nào sau đây được sử dụng như là nền tảng của hạ tầng cơ sở hạ tầng khóa công khai (PKI)?

   a. MD4

   b. SHA

   c. Diffie-Hellman

   d. Skipjack

7. . Khi giá trị hàm băm của hai thông điệp khác nhau có giá trị tương tự nhau, ta gọi hiện tượng này là gì ?

   a. Tấn công vào ngày sinh

   b. Xung đột

c. Chữ ký số

d. Khóa công khai

8. . Thực thể nào sau đây cho phép phát hành , quản lý, và phân phối các chứng chỉ số ?

a. Quyền cấp chứng chỉ (Certificate Authority)

b. Quyền đang ký (Registation Authority)

c. Chính phủ (NSA)

d. PKI

9. . Các phương pháp sinh trắc học nào sau đây được coi là an toàn nhất ?

a. Phân tích chữ ký

b. Quét tiếng

c. Lấy dấu bàn tay / Lấy dấu ngón tay

d. Không quan trọng

10. . Một user gọi điện đến cho ta (với tư cách là người quản lý) thông báo họ bị mất mật khẩu và cần truy cập ngay lập tức. Ta nên làm gì ?

a. Cung cấp truy cập ngay lập tức, và sau đó kiểm tra chứng cứ của họ

b. Tạo một login và mật khẩu tạm thời để họ sử dụng

c. Xác minh định danh của họ trước khi cấp quyền truy cập

d. Cho họ một mật khẩu riêng tạm thời

11. . Phương pháp xác thực nào sử dụng một KDC để thực hiện xác thực ?

a. Kerberos

b. Chap

c. Sinh trắc học

d. Thẻ thông minh

12. . Phương pháp xác thực nào gởi trả lại một "yêu cầu" (request) cho máy trạm và" yêu cầu" đó được mã hóa và gởi trở lại máy chủ ?

a. Kerberos

b. Các mã thông báo bảo mật

c. DAC

d. CHAP

13. . Giao thức nào sau đây tuy không phải là một giao thức đường hầm nhưng nó sử dụng các giao thức đường hầm để bảo mật trên mạng?

a. IPSec

b. PPTP

c. L2TP

d. L2F

14. . Một socket là sự kết hợp của các thành phần nào ?

a. IP và session number

b. IP và port number

c. UDP và port number

d. TCP và port number

15. . Thiết bị nào giám sát lưu lượng mạng theo cách thụ động ?

    a. IDS

    b. Firewall

    c. Sniffer

    d. Web browser

16. . Bạn nhận được một email từ Microsoft, trong đó có một file đính kèm. Trong thư nói rằng có một số lỗi đã được phát hiện và sửa chữa , bạn phải chạy chương trình được đính kèm trong thư để sửa những lỗi đó. Trong trường hợp này bạn sẽ làm gì để bảo đảm an toàn?

    a. Lưu chương trình đó lại và dùng chương trình diệt virus để quét, nếu không phát hiện thấy virus, sẽ chạy chương trình đó để sửa lỗi

    b. Mở chương trình và chạy nó ngay. Chương trình đó thật sự an toàn vì nó được gửi từ Microsoft

    c. Xoá email đó ngay. Microsoft và các nhà cung cấp không bao giờ gửi chương trình sửa lỗi qua email.

    d. Tất cả đều sai

17. . PKC được thực hiện bằng cách sử dụng các chức năng nào ?

    a. Chuyển giao các khóa công khai an toàn

    b. Chuyển giao các khóa cá nhân an toàn

    c. Bảo mật dữ liệu ở hai đầu mút

    d. Sử dụng hai khóa khác nhau để mã hóa và giải mã

18. . Khái niệm nào sau đây được sử dụng để mô tả sự không thể chối từ của người gửi khi gửi thông điệp ?

    a. Toàn vẹn

    b. Tính không chối từ (non-repudiation)

    c. Xác thực

    d. Bảo mật

19. . Khái niệm nào sau đây được dùng để xác định chuẩn thực thi các hệ thống mã hóa diện rộng ?

    a. PKE

    b. PKI

    c. Đối xứng

    d. Không đối xứng

20. . Điều nào sau đây là điểm yếu của IP ?

    a. Mã nguồn độc hại

    b. Giả mạo IP

    c. Tấn công dạng "Man in the middle"

    d. Tấn công chuyển tiếp

21. . Qui trình xác định topology của mạng được gọi là gì ?

    a. In dấu chân

    b. Thiết bị làm nhiễu

    c. Quét mạng

d. Liệt kê

22. . Qui trình chiếm quyền truy cập đến tài nguyên mạng (đặc biệt như là các tập tin user và nhóm) được gọi là gì ?

a. In dấu chân

b. Quét

c. Thiết bị làm nhiễu

d. Liệt kê