1. **Hình thức tấn công thụ động chống lại nguyên tắc cốt lõi nào của an toàn thông tin?**
   a. Bí mật
   b. Toàn vẹn
   c. Sẵn sàng
   d. Xác thực
2. **Tấn công DOS (Denial of Service) thuộc loại tấn công nào trong kiến trúc an ninh OSI ?**
   a. Tấn công từ xa (Remote Attack)
   b. Tấn công chủ động (Active Attack)
   c. Tấn công thụ động (Passive Attack)
   d. Cả câu (a) và câu (b) đều đúng
3. **Cơ chế nào sau đây không cần thiết sử dụng để chống lại tấn công từ chối dịch vụ?**
   a. Mã hóa dữ liệu (encipherment)
   b. Quản lý định tuyến (routing control)
   c. Trao đổi xác thực (authentication exchange)
   d. Quản lý truy cập (access control)
4. **Cơ chế nào không sử dụng chodịch vụ xác thực?**
   a. Mã hóa dữ liệu (encipherment)
   b. Chữ ký số (digital signature)
   c. Trao đổi xác thực (authentication exchange)
   d. Quản lý truy cập (access control)
5. **Cho biết Code Red thuộc vào loại mã độc nào sau đây:**
   a. Virus
   b. Trojan
   c. Worm
   d. Là một loại mã độc lai ghép

1. **Hệ mã Cesar mã hóa x∈[0; 25] thành y = x + 3 mod 26. Hãy cho biết nếu giá trị bản rõ là 10 thì giá trị bản mã tương ứng là:**
   a. 5 b. 7 c. 13 d. 15
2. **Hệ mã Affine mã hóa x∈[0; 25] thành y = 3x + 5 mod 26. Hãy cho biết nếu giá trị bản mã là 10 thì giá trị bản rõ tương ứng là:**
   a. 9 b. 14 c. 19 d. 23
3. **Đối với mã hóa DES, trong các phát biểu sau phát biểu nào là sai?**
   a. DES sử dụng khóa có chiều dài 64 bits.
   b. Dữ liệu được mã hóa trong các khối có chiều dài 64 bits.
   c. S-box là một hàm thay thế không tuyến tính làm tăng độ phức tạp của phép biến đổi.
   d. DES dùng bộ tạo khóa để tạo ra các khóa con dùng cho mỗi vòng và chúng có chiều dài là 48 bits.
4. **Hệ mã Double DES(2DES) không an toàn do tấn công gì?**
   a. Tấn công "man in the midle"
   b. Tấn công "meet in the midle"
   c. Tấn công brute force
   d. Tấn công DOS
5. **Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt?**
   a. ECB
   b. CBC
   c. CFB
   d. OFB

4. Hãy cho biết kết quả của (7^{2010} mod 13):

a. 1
b. 12
c. 7
d. Các giá trị trên đều sai

5. Cho biết giá trị hàm phi Euler ϕ(440) là:

a. 439
b. 240
c. 160
d. Tất cả các câu trên đều sai

6. Hãy cho biết kết quả của (3^{2086} mod 440):

a. 1 b. 3 c. 81 d. 289

7. Đối với mã hóa khóa công khai, khóa nào được sử dụng để tạo chữ ký số trên một thông điệp:

a. Khóa công khai của người nhận
b. Khóa riêng của người nhận
c. Khóa công khai của người gửi
d. Khóa riêng của người gửi

8. Đối với mã hóa khóa công khai, khóa nào được sử dụng để mã hóa một thông điệp:

a. Khóa công khai của người nhận
b. Khóa riêng của người nhận
c. Khóa công khai của người gửi
d. Khóa riêng của người gửi

(Dữ liệu dùng cho câu 6 và 7)
Thực hiện mã hóa và giải mã với thuật toán RSA và p = 3; q = 11, e = 7; bản mã C = 5

9. Giá trị của d là:

a. 7 b. 5 c. 3 d. 2

10. Giá trị của bản rõ M tương ứng là:

a. 26 b. 24 c. 5 d. 1

(Dữ liệu dùng cho câu 10, 11, 12)
A và B dùng kỹ thuật trao đổi khóa Diffie-Hellman với q = 71 và α = 7.

11. Nếu A có khóa riêng X_A = 5, hãy cho biết khóa công khai của A (Y_A)?

a. 4 b. 5 c. 30 d. 51

12. Nếu B có khóa riêng X_B = 12, hãy cho biết khóa công khai của B (Y_B)?

a. 4 b. 5 c. 30 d. 51

13. Nếu A có khóa riêng X_A = 5 và B có khóa riêng X_B = 12, hãy cho biết khóa bí mật dùng chung giữa A và B(K_{AB})?

a. 4
b. 5
c. 30
d. 51

14. DAA(Data Authentication Algorithm) tạo ra mã xác thực thông điệp có kích thước là:

a. 128 bits
c. 128 bytes
b. 64 bits
d. 64 bytes

15. Cho một hàm băm với kết quả băm có chiều dài là 128 bits. Hãy cho biết cần sửa đổi ít nhất bao nhiêu chỗ trong văn bản P sao cho xác xuất để có hai văn bản P_1 và P_2 mà giá trị băm của chúng bằng nhau là 0.5

a. 128 b. 64 c. 2^{64} d. 2^{128}

16. Mã xác thực thông điệp dựa trên hàm băm MD5 tạo ra mã xác thực thông điệp có kích thước là :

a. 128 bits
b. 64 bits
c. 128 bytes
d. 64 bytes

17. Chữ ký số là một cơ chế xác thực nhằm:
a. Xác minh tính toàn vẹn của thông điệp.
b. Xác nhận danh tính của người tạo ra thông điệp.
c. Chống thoái thác về xuất xứ
d. Cả ba câu trên đều đúng

18. Cho biết phát biểu sai khi nói về các lược đồ tạo chữ ký số:
a. Lược đồ DSA tạo chữ ký có chiều dài 512 bits.
b. Lược đồ DSA tạo và xác minh chữ ký nhanh hơn so với lược đồ RSA.
c. Lược đồ RSA tạo chữ ký có chiều dài lớn hơn so với lược đồ DSA.
d. DSA không thể dùng cho các vấn đề mã hóa dữ liệu và trao đổi khóa.

19. Một môi trường Kerberos đầy đủ dịch vụ bao gồm:
a. Một máy chủ Kerberos
b. Một máy chủ Kerberos và một số máy trạm
c. Một máy chủ Kerberos và một số máy chủ ứng dụng
d. Một máy chủ Kerberos, một số máy trạm, một số máy chủ ứng dụng

20. Đối với Kerberos, mỗi người dùng có:
a. Một vé TGT và một vé SGT cho tất cả các dịch vụ mà người dùng truy cập đến
b. Một vé TGT và mỗi vé SGT cho mỗi dịch vụ mà người dùng truy cập đến
c. Một vé SGT và mỗi vé TGT cho mỗi dịch vụ mà người dùng truy cập đến
d. Mỗi vé SGT và mỗi vé TGT cho mỗi dịch vụ mà người dùng truy cập đến

21. Dịch vụ xác thực X.509 dùng mã hóa dạng gì?
a. Mã hóa đối xứng
b. Mã hóa khóa bí mật
c. Mã hóa khóa công khai
d. Cả câu (b) và (c)

22. Chữ ký số trong chứng chỉ X.509 được tạo dùng khóa nào sau đây :
a. Khóa công khai của người sở hữu chứng chỉ.
b. Khóa riêng của người sở hữu chứng chỉ.
c. Khóa công khai của đơn vị phát hành chứng chỉ.
d. Khóa riêng của đơn vị phát hành chứng chỉ.

23. Thủ tục xác thực nào được dùng để dùng cho các kết nối có tương tác ?
a. Xác thực một chiều.
b. Xác thực hai chiều.
c. Xác thực ba chiều.
d. Cả câu (b) và (c) đều đúng.

24. 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.

25. 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.

26. 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.

27. Chế độ hoạt động của PGP khi thực hiện mã hóa đối xứng là:

a. CBC
b. ECB
c. CFB
d. OFB

28. 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

29. 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

30. 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.

31. 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 nhiềuphiên 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.

32. 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.

33. 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.

34. Cho biết mục tiêu nào sau đây là mục tiêu thiết kế một bức tường lửa?

a. Tất cả thông tin từ bên trong ra bên ngoài và ngược lại phải đi qua bức tường lửa.
b. Tất cả thông tin di chuyển bên trong một mạng cục bộ phải đi qua bức tường lửa.
c. Chỉ các loại thông tin được cấp quyền thông qua chính sách an ninh cục bộ mới được phép đi qua bức tường lửa.
d. Các câu (a) và (c) đều đúng.
e. Các câu (a), (b) và (c) đều đúng.

35. Chọn phát biểu sai khi nói về bộ lọc gói (packet filter):

a. Nó không xem xét dữ liệu ở tầng ứng dụng trong mô hình TCP/IP.
b. Nó khôngthểngăn chặncác cuộc tấn côngsử dụngcác lỗ hổngứng dụngcụ thể.
c. Nó có khả năng phát hiện các tấn công dạng giả mạo địa chỉ ở tầng mạng
d. Chức năng ghi nhật ký (logging) của nó bị hạn chế.

36. Chọn phát biểu sai trong các phát biểu sau khi nói về các loại bức tường lửa.

a. Packet fiter quyết định lọc gói dựa trên thông tin các trường trong IP và TCP header.
b. Circuit-level gateway cho phép thiết lập một kết nối TCP end to end.
c. Application-level gateway còn được gọi là proxy server.
d. Application-level gateway an toàn hơn Packet fitering router.

37. Cho biết cấu hình bức tường lửa nào sau đây có khả năng ngăn chặn các vi phạm an ninh mạng khi bộ lọc gói trên bộ định tuyến kết nối với Internet bị thương tổn hay đã thỏa hiệp.

a. single-homed bastion host
b. dual-homed bastion host
c. screened subnet
d. Câu (b) và (c) đều đúng

38. Cách thức để hạn chế tấn công SYN-Flooding trên bức tường lửa là:
a. Cho phép nhận một lượng nhất định gói SYN trong một giây.
b. Chặn những IP kết nối thất bại nhiều lần.
c. Chỉ cho phép gói SYN trên một số port nhất định.
d. Tất cả đều đúng.

39. Hướng phát hiện thâm nhập bất hợp pháp nào liên quan đến việc thu thập hành vi người dùng hợp pháp trong một khoảng thời gian và sau đó phân tích đánh giá:
a. Phát hiện dựa trên thống kê
b. Phát hiện dựa trên quy tắc
c. Lai tạo
d. Các câu trên đều sai

40. Cho biết phát biểu sai trong các phát biểu sau khi nói đến hệ thống phát hiện thâm nhập bất hợp pháp:
a. Để xây dựng hệ thống phát hiện thâm nhập bất hợp pháp ta có hai hướng tiếp cận là rule-based detection và behavior-based detection.
b. Nếu hệ thống phát hiện một xâm nhập đủ nhanh, kẻ xâm nhập có thể được xác định trước khi bị thiệt hại.
c. Một hệ thống phát hiện thâm nhập bất hợp pháp hiệu quả có thể kết hợp với bức tường lửa để ngăn chặn ngay các xâm nhập.
d. Nó cho phép ta thu thập thông tin về các kỹ thuật xâm nhập đã được sử dụngđể tăng cường cho công tác phòng chống xâm nhập.

41. Đối với việc khởi tạo một IDS, sau khi đã xác định mục tiêu ta phải làm gì tiếp theo?
a. Chọn đáp ứng thích hợp
b. Xét các ngưỡng
c. Hiện thực chính sách
d. Chọn thành phần, hệ thống để theo dõi

42. Nếu một tổ chức muốn bảo vệ một máy chủ tránh bị người dùng hợp pháp phá hoại, hệ thống phát hiện thâm nhập bất hợp pháp nào là lựa chọn tốt nhất?
a. NIDS
b. HIDS
c. Lai tạo
d. Các câu trên đều sai

43. Nếu một tổ chức muốn phát hiện các tấn công với chi phí thấp thì hệ thống phát hiện thâm nhập bất hợp pháp nào là lựa chọn tốt nhất?
a. NIDS
b. HIDS
c. Lai tạo
d. Các câu trên đều sai

C10:

44. VPN là viết tắt của:

a. Virtual Public Network
b. Virtual Private Network
c. Virtual Protocol Network
d. Virtual Perimeter Network

45. Lợi ích chính của VPN so với các mạng chuyên dụng như frame relay, leased line hay dial-up truyền thống là gì?

a. Hiệu suất mạng tốt hơn
b. Ít bị lỗi hơn
c. Giảm chi phí
d. Cải thiện an ninh

46. Trong VPN, thuật ngữ "tunneling" đề cập đến:

e. Một tính năng tùy chọn làm tăng hiệu suất mạng.
f. Đóng gói các gói tin bên trong các gói tin của một giao thức khác để tạo và duy trì mạch ảo
g. Phương pháp quản trị hệ thống sử dụng để phát hiện tin tặc trên mạng
h. Một chiến lược tiếp thị để bán các sản phẩm VPN

47. Những giao thức nào sau đây là giao thức VPN tunneling?

a. PPTP
b. L2TP
c. IPSec
d. Tất các các câu trên đều đúng

48. Khác biệt giữa Firewall và VPN là gì?

a. Firewall có thể cấu hình còn VPN thì không cấu hình được.
b. Firewall là một loại mới của VPN.
c. Firewall chặn các thông điệp còn VPN thì mở ra con đường cho các thông điệp hợp lệ đi qua.
d. Không có khác biệt giữa Firewall và VPN.

C11:

49. WEP được viết tắt là:

Wireless Encryption Protocol
Wireless Encryption Privacy
Wired Equivalent Privacy
Wired Equivalent Protocol

50. Điểm yếu thật sự của WEP trong vấn đề mã hóa là:

a. Dùng thuật toán RC4
b. Dùng khóa chung quá ngắn
c. Thuật toán lập lịch khóa của RC4
d. Không xác thực người dùng

51. Tiêu chuẩn an ninh mạnh mẽ hơn được phát triển bởi IEEE để giải quyết các lỗ hổng chuẩn WLAN IEEE 802.11 là:

a. IEEE 802.16.2
b. IEEE 802.11e
c. IEEE 802.11i
d. IEEE 802.11n

52. Khác biệt giữa WPA và WPA2 là:

a. WPA mã hóa dùng RC4, WPA2 mã hóa dùng AES.
b. WPA mã hóa dùng RC4 với TKIP/MIC, WPA2 mã hóa dùng AES.
c. WPA xác thực dùng PSK, WPA2 xác thực dùng 802.1x/EAP.
d. WPA xác thực dùng ICV, WPA2 xác thực dùng 802.1x/EAP.

53. Chọn phát biểu sai trong các phát biểu sau:

a. WPA là một tập con của IEEE 802.11i
b. AES là mã hóa đối xứng.
c. WPA2 cho phép các client AES và TKIP được hoạt động trên cùng WLAN.
d. IEEE 802.11i thực thi an ninh trên port.