1. Hình thức tấn công thụ động chống lại nguyên tắc cốt lõi nào của an toàn thông tin? **Bí mật**

2. Tấn công DOS (Denial of Service) thuộc loại tấn công nào trong kiến trúc an ninh OSI **? Tấn công chủ động**

3. Cơ chế nào sau đây không cần thiết sử dụng để chống lại tấn công từ chối dịch vụ**? Mã hóa dữ liệu**

ncipherment).

4. Cơ chế nào không sử dụng cho dịch vụ xác thực? **Quản lý truy cập (access control)**

5. biết Code Red thuộc vào loại mã độc nào sau đây: **Worm**

6. 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: **13**

7. 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: **19**

8. Đối với mã hóa DES, trong các phát biểu sau phát biểu nào là sai? **DES sử dụng khóa có chiều dài 64 bits.**

9. Hệ mã Double DES(2DES) không an toàn do tấn công gì? **Tấn công "meet in the middle"**

10. Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt? **ECB**

11. Hãy cho biết kết quả của (7^{2010} mod 13): **12 . a^{p-1} mod p = 1 .**

12. Cho biết giá trị hàm phi Euler ϕ(440) là: **160 . 440 = 2^3.5.11 => o(440) = 2^2.(2-1).4.10 = 160.**

13. Hãy cho biết kết quả của (3^{2086} mod 440) : **289 . $a^{o(n)}$ mod n = 1.**

14. Đối với mã hóa khóa công khai, khóa nào được sử dụng để tạo chữ ký số trên một thông điệp : Khóa riêng của người gửi

15. Đối với mã hóa khóa công khai, khóa nào được sử dụng để mã hóa một thông điệp : Khóa công khai của người nhận.

(Dữ liệu dùng cho câu 16 và 17)Thực hiện mã hóa và giải mã với thuật toán RSA và p = 3; q = 11, e = 7; bản mã C =

16. Giá trị của d là :**3 . Tính n = p*q = 33. o(n) = (p-1).(q-1) = 20 . Mà e.d mod o(n) = 1 => d =3**

17. Giá trị của bản rõ M tương ứng là: . **26 . ($M = C^d$ mod n và $C = M^e$ mod n)**

(Dữ liệu dùng cho câu 18, 19, 20) A và B dùng kỹ thuật trao đổi khóa Diffie-Hellman với q = 71 và α = 7.

18. Nếu A có khóa riêng X_A = 5, hãy cho biết khóa công khai của A (Y_A)? **51 . $Y_A = \alpha^{Xa}$ mod q**

19. Nếu B có khóa riêng X_B = 12, hãy cho biết khóa công khai của B (Y_B)? **4**

20. 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})

30 . $K = Y_A^{Xb}$ mod q = Yb^{Xa} mod q

21. DAA(Data Authentication Algorithm) tạo ra mã xác thực thông điệp có kích thước là: **64 bits**

22. 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 : **64**

23. Mã xác thực thông điệp dựa trên hàm băm MD5 tạo ra mã xác thực thông điệp có kích thước là : **c.128 bytes**

24. 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**

25. 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**

26. 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

27. Cho biết phát biểu sai trong các phát biểu sau khi nói đến hệ thống phát hiện thâm nhập bất hợp pháp:

Nếu hệ thống phát hiện một xâm nhập đủ nhanh, kẻ xâm nhập có thể được xác định trước khi bị thiệt hại

28. 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**

29. 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.

30. 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

31. 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
32. 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
33. 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)
34. 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.
35. 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**
36. 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

37. 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**
38. 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
39. Chế độ hoạt động của PGP khi thực hiện mã hóa đối xứng là: **CFB**
40. Thuật toán mã hóa nào sau đây là phù hợp với mã hóa đối xứng của PGP: **3DES với 2 khóa và AES**
41. SSL có không có khả năng chống lại loại tấn công nào sau đây: **SYN flooding**
42. Cho biết giao thức nào sau đây không có trong SSL: **SSL message protocol**
43. 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 SL.
d.Các câu trên đều sai
44. Cho biết phát biểu sai về chữ ký đôi(dual signature) trong các phát biểu sau:
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
45. 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: **Issuer**
46. Cho biết mục tiêu nào sau đây là mục tiêu thiết kế một bức tường lửa? 2 mục tiêu
Tất cả thông tin từ bên trong ra bên ngoài và ngược lại phải đi qua bức tường lửa
Chỉ các loại thông tin được cấp quyền thông qua chính sách an ninh cục bộ mới được phép đi qua bức tường lửa
47. Chọn phát biểu sai khi nói về bộ lọc gói (packet filter):

Nó có khả năng phát hiện các tấn công dựng giả mạo địa chỉ ở tầng mạng
48. Chọn phát biểu sai trong các phát biểu sau khi nói về các loại bức tường lửa.
Circuit-level gateway cho phép thiết lập một kết nối TCP end to end (thực sự có 2 kết nối)
49. 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? **screened subnet và dual-homed bastion host**
50. 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
51.VPN là viết tắt của: **Virtual Private Network**
52.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
53.Trong VPN thuật ngữ "tunneling" đề cập đến: **Đóng gói các gói tin bên trong các gói tin của một giao thức hác để tạo và duy trì mạch ảo**
54.Những giao thức nào sau đây là giao thức VPN tunneling
a.PPTP b.L2TP c.IPSec **d. Tất cả đều đúng**
55. Khác biệt giữa Firewall và VPN là gì : **Firewall chặn các thông điệp còn VPN thì mở đường cho các thông ệp hợp lệ đi qua.**
56.WEP được viết tắt của**: Wired Equivalent Privacy**
57.Điểm yếu thật sự của WEP trong vấn đề mã hóa là: **Thuật toán lập trình khóa của RC4**
58. Tiêu chuẩn an ninh mạnh mẽ hơn được phát triển bởi IEEE để giải quyết các lỗ hổng chuẩn WLAN IEEE 802.11 : **IEEE 802.11 1i**
59. Khác biệt giữa WPA và WPA2 là : **WPA mã hóa dùng RC4 với TKIP/MIC, WPA2 mã hóa dùng AES.**
60. Chọn phát biểu sai trong các phát biểu sau:
a.WPA là một tập con của IEEE 802.1 1i b.AES là mã hóa đối xứng
c.WPA2 cho phép các client AES và TKIP được hoạt động trên cùng WLAN **d.IEEE 802.1 1i thực thi ı toàn trên port**

Chế độ nào của IPSec không bảo vệ IP header : **Transport**
Các giao thức được thiết kế bởi IETF nào an toàn cho gói dữ liệu ở tầng mạng trong mô hình OSI : **IPSec** ,
Tham số nào của sự kết hợp bảo mật SA gồm các thông số xác thực,khóa, và thời gian sống của khóa : **AH ıformation, ESP Information**
Giao thức IKE tạo các kết hợp bảo mật nào sau đây :**SSL và IPSec**
SSL không cung cấp dịch vụ nào sau đây : **Compresion (key point**)
Giao thức nào của IPSec cung cấp dịch vụ xác thực và mã hóa thông tin trong Internet trong mô hình TCP/IP: **ESP**