Kho trắc nghiệm **AN TOÀN THÔNG TIN**

3 chương đầu 1,2,3.

Chương 1:

1. An toàn thông tin được định nghĩa là việc bảo vệ những thuộc tính nào của tài sản thông tin?
a) Tính bảo mật và tính toàn vẹn
b) Tính toàn vẹn và tính sẵn sàng
c) Tính bảo mật và tính sẵn sàng
* d) Tính bảo mật, tính toàn vẹn và tính sẵn sàng
2. Hai lĩnh vực chính của an toàn thông tin là gì?
a) An toàn phần cứng và an toàn phần mềm
* b) An toàn công nghệ thông tin và đảm bảo thông tin
c) An toàn mạng và an toàn dữ liệu
d) An toàn vật lý và an toàn logic
3. An toàn công nghệ thông tin (IT Security) còn được gọi là gì?
a) An toàn mạng
* b) An toàn máy tính (Computer Security)
c) An toàn dữ liệu
d) An toàn ứng dụng
4. An toàn công nghệ thông tin (IT Security) là gì?
a) Chỉ là việc bảo vệ phần cứng máy tính
b) Chỉ là việc bảo vệ phần mềm máy tính
* c) An toàn thông tin được áp dụng cho các hệ thống công nghệ
d) Chỉ là việc bảo vệ dữ liệu
5. An toàn thông tin bao gồm mấy thành phần chính?
a) 2 thành phần
b) 3 thành phần
* c) 4 thành phần
d) 5 thành phần
6. An toàn mạng là gì?
a) Chỉ là việc bảo vệ phần cứng mạng
* b) Đảm bảo an toàn của hệ thống mạng và thông tin truyền tải trên mạng
c) Chỉ là việc bảo vệ dữ liệu trên mạng

d) Chỉ là việc bảo vệ người dùng mạng
7. Nội dung cốt lõi của quản lý an toàn thông tin là gì?
a) Quản lý người dùng
* b) Quản lý rủi ro, trong đó quan trọng là việc nhận diện và đánh giá rủi ro
c) Quản lý phần cứng và phần mềm
d) Quản lý dữ liệu
8. Chính sách an toàn thông tin bao gồm mấy thành phần?
a) 2 thành phần
* b) 3 thành phần
c) 4 thành phần
d) 5 thành phần
9. Theo mô hình tháp, có bao nhiêu loại hệ thống thông tin dựa theo người dùng?
a) 2 loại
b) 3 loại
* c) 4 loại
d) 5 loại
10. Hệ thống xử lý giao dịch (Transactional Processing Systems) phục vụ đối tượng người dùng nào?
a) Nhà quản lý cấp trung
b) Nhà quản lý cấp cao
c) Giám đốc điều hành
* d) Nhân viên (Workers)
11. Hệ thống thông tin quản lý (Management Information Systems) phục vụ đối tượng người dùng nào?
* a) Nhà quản lý cấp trung
b) Nhân viên
c) Nhà quản lý cấp cao
d) Giám đốc điều hành
12. Hệ thống hỗ trợ quyết định (Decision Support Systems) phục vụ đối tượng người dùng nào?
a) Nhân viên
b) Nhà quản lý cấp trung
* c) Nhà quản lý cấp cao
d) Giám đốc điều hành
13. Hệ thống thông tin điều hành (Executive Information Systems) phục vụ đối tượng người dùng nào?

a) Nhân viên
b) Nhà quản lý cấp trung
c) Nhà quản lý cấp cao
* d) Giám đốc điều hành
14. Hệ thống thông tin dựa trên máy tính bao gồm bao nhiêu thành phần chính?
a) 3 thành phần
* b) 5 thành phần
c) 6 thành phần
d) 7 thành phần
15. Thành phần nào sau đây KHÔNG phải là thành phần của hệ thống thông tin dựa trên máy tính?
a) Phần cứng
b) Phần mềm
c) Cơ sở dữ liệu
* d) Người quản trị
16. An toàn hệ thống thông tin (ISS) đảm bảo những thuộc tính nào của hệ thống thông tin?
a) Chỉ tính bảo mật
b) Chỉ tính toàn vẹn và tính sẵn sàng
* c) Tính bảo mật, tính toàn vẹn và tính sẵn sàng
d) Chỉ tính xác thực
17. Trong mô hình tháp của hệ thống thông tin, hệ thống nào nằm ở vị trí cao nhất?
a) Hệ thống xử lý giao dịch
b) Hệ thống thông tin quản lý
c) Hệ thống hỗ trợ quyết định
* d) Hệ thống thông tin điều hành
18. Mục đích chính của an toàn hệ thống thông tin (ISS) là gì?
a) Chỉ để bảo vệ phần cứng
b) Chỉ để bảo vệ phần mềm
c) Chỉ để bảo vệ dữ liệu
* d) Đảm bảo các thuộc tính an toàn và bảo mật của hệ thống thông tin

20. Ba thuộc tính quan trọng của an toàn thông tin bao gồm:
a) Bảo mật, Toàn vẹn, Xác thực
b) Toàn vẹn, Sẵn sàng, Xác thực
* c) Bảo mật, Toàn vẹn, Sẵn sàng

d) Bảo mật, Sẵn sàng, Phân quyền
21. Thuộc tính mở rộng quan trọng khác của an toàn thông tin là gì?
a) Phân quyền
b) Kiểm soát truy cập
* c) Xác thực
d) Mã hóa
22. Dữ liệu được coi là toàn vẹn khi:
a) Chỉ khi dữ liệu không bị thay đổi
b) Chỉ khi dữ liệu hợp lệ
c) Chỉ khi dữ liệu chính xác
* d) Dữ liệu không bị thay đổi, hợp lệ và chính xác

25. Bốn loại tấn công chính bao gồm:
* a) Giả mạo, Đánh chặn, Gián đoạn, Sửa đổi
b) Giả mạo, Đánh chặn, Gián đoạn, Xóa bỏ
c) Giả mạo, Đánh chặn, Sửa đổi, Xóa bỏ
d) Giả mạo, Gián đoạn, Sửa đổi, Xóa bỏ
26. Tấn công giả mạo địa chỉ (Address spoofing) là gì?
a) Tấn công tràn bộ đệm
* b) Tấn công giả mạo địa chỉ nguồn để che giấu danh tính hoặc để vượt qua các biện pháp bảo mật
c) Tấn công mật khẩu
d) Tấn công từ chối dịch vụ
27. Tấn công thụ động (Passive attack) bao gồm những hành động nào?
a) Sửa đổi dữ liệu trên đường truyền
b) Sửa đổi dữ liệu trong tệp
* c) Không gây ra thay đổi trên hệ thống, nghe lén, theo dõi lưu lượng trên đường truyền
d) Truy cập trái phép vào máy tính hoặc mạng
28. Tấn công người đứng giữa (Man-in-the-middle) là gì?
* a) Tấn công trong đó kẻ tấn công bí mật chuyển tiếp và có thể thay đổi thông tin liên lạc giữa hai bên
b) Tấn công tràn bộ đệm
c) Tấn công mật khẩu
d) Tấn công từ chối dịch vụ
29. Tấn công mật khẩu là gì?
a) Tấn công nhằm làm hỏng mật khẩu

* b) Hình thức tấn công nhằm đánh cắp mật khẩu và thông tin tài khoản để lạm dụng
c) Tấn công nhằm thay đổi mật khẩu
d) Tấn công nhằm xóa mật khẩu
30. Tấn công bom thư (Mail bomb) là gì?
a) Tấn công tràn bộ đệm
* b) Tấn công gửi một lượng lớn email đến một địa chỉ nhằm làm tràn hòm thư hoặc làm sập máy chủ
c) Tấn công mật khẩu
d) Tấn công từ chối dịch vụ
31. An toàn thông tin là gì?
a) Chỉ là việc bảo vệ dữ liệu khỏi bị xóa
b) Chỉ là việc bảo vệ phần cứng máy tính
* c) Là việc bảo vệ chống lại truy cập trái phép, sử dụng, tiết lộ, sửa đổi hoặc phá hủy thông tin
d) Chỉ là việc bảo vệ mạng máy tính

33. Sao lưu ngoại tuyến (Offsite backup) được sử dụng trong đảm bảo thông tin để làm gì?
a) Để tăng tốc độ truy cập dữ liệu
b) Để giảm chi phí lưu trữ dữ liệu
* c) Để sao lưu dữ liệu thông tin từ hệ thống gốc vào các thiết bị lưu trữ vật lý đặt ở một vị trí khác
d) Để mã hóa dữ liệu quan trọng
34. An toàn máy tính và dữ liệu là gì?
a) Chỉ là việc bảo vệ phần cứng máy tính
b) Chỉ là việc bảo vệ dữ liệu
* c) Đảm bảo an toàn của phần cứng, phần mềm và hệ thống dữ liệu trên máy tính
d) Chỉ là việc bảo vệ phần mềm máy tính
35. Các kỹ thuật và công cụ thường được sử dụng trong an toàn mạng bao gồm:
a) Chỉ tường lửa và proxy
b) Chỉ mạng riêng ảo và các kỹ thuật an toàn thông tin
c) Chỉ các kỹ thuật và hệ thống phát hiện và ngăn chặn tấn công
* d) Tường lửa, proxy, mạng riêng ảo, các kỹ thuật an toàn thông tin, hệ thống phát hiện và ngăn chặn tấn công, giám sát mạng
36. Quản lý an toàn thông tin là gì?

a) Chỉ là việc quản lý người dùng
b) Chỉ là việc quản lý phần cứng và phần mềm
* c) Quản lý và giám sát việc thực hiện các biện pháp đảm bảo an toàn thông tin
d) Chỉ là việc quản lý dữ liệu
37. Hệ thống thông tin (IS) là gì?
a) Một hệ thống chỉ dùng để lưu trữ dữ liệu
b) Một hệ thống chỉ dùng để xử lý thông tin
* c) Một hệ thống tích hợp các thành phần để phục vụ việc thu thập, lưu trữ, xử lý và truyền tải thông tin, tri thức và sản phẩm số
d) Một hệ thống chỉ dùng để bảo vệ thông tin
38. Doanh nghiệp và tổ chức sử dụng hệ thống thông tin (IT) để thực hiện và quản lý các hoạt động nào?
a) Chỉ để tương tác với khách hàng
b) Chỉ để quảng bá thương hiệu và sản phẩm
c) Chỉ để cạnh tranh với đối thủ trên thị trường
* d) Tương tác với khách hàng, nhà cung cấp, cơ quan chính phủ, quảng bá thương hiệu và cạnh tranh với đối thủ
39. Hệ thống thông tin dựa trên máy tính (Computer-Based Information System) là gì?
a) Hệ thống chỉ sử dụng phần cứng máy tính
b) Hệ thống chỉ sử dụng phần mềm máy tính
* c) Hệ thống thông tin sử dụng công nghệ máy tính để thực hiện các nhiệm vụ
d) Hệ thống chỉ sử dụng mạng máy tính
40. Trong hệ thống thông tin dựa trên máy tính, "Phần cứng" được định nghĩa là gì?
* a) Thiết bị phần cứng để thu thập, lưu trữ, xử lý và biểu diễn dữ liệu
b) Phần mềm chạy trên thiết bị phần cứng để xử lý dữ liệu
c) Nơi lưu trữ dữ liệu
d) Hệ thống truyền tải thông tin/dữ liệu
41. Trong hệ thống thông tin dựa trên máy tính, "Thủ tục" được định nghĩa là gì?
a) Các bước để cài đặt phần mềm
b) Các bước để bảo trì phần cứng
* c) Tập hợp các lệnh kết hợp các phần đã đề cập để xử lý dữ liệu, đưa ra kết quả mong muốn
d) Các bước để thiết lập mạng
42. Thông tin bảo mật có thể bao gồm:

a) Chỉ dữ liệu cá nhân
b) Chỉ thông tin thuộc quyền sở hữu trí tuệ
c) Chỉ thông tin liên quan đến an ninh quốc gia
* d) Dữ liệu cá nhân, thông tin thuộc quyền sở hữu trí tuệ, thông tin liên quan đến an ninh quốc gia

44. Tính toàn vẹn liên quan đến:
a) Chỉ tính hợp lệ của dữ liệu
b) Chỉ tính chính xác của dữ liệu
* c) Tính hợp lệ và chính xác của dữ liệu
d) Chỉ tính bảo mật của dữ liệu
45. Tình huống nào cần đảm bảo tính xác thực?
a) Chỉ xác minh danh tính người dùng khi đăng nhập vào hệ thống
b) Chỉ kiểm tra tính hợp lệ và nguồn gốc của dữ liệu
c) Chỉ đảm bảo phần mềm hoặc bản cập nhật được cung cấp bởi nhà phát triển hợp pháp
* d) Tất cả các tình huống trên
46. Nguyên tắc "Defence in Depth" trong an toàn thông tin là gì?
a) Chỉ sử dụng một lớp bảo vệ mạnh
* b) Tạo nhiều lớp bảo vệ, kết hợp tác dụng của mỗi lớp để đảm bảo an toàn tối đa
c) Chỉ sử dụng tường lửa để bảo vệ hệ thống
d) Chỉ sử dụng phần mềm diệt virus để bảo vệ hệ thống
47. Mối đe dọa (Threat) là gì?
a) Một lỗi hoặc khiếm khuyết tồn tại trong hệ thống
* b) Bất kỳ hành động nào có thể gây thiệt hại cho tài nguyên hệ thống
c) Điểm yếu trong hệ thống cho phép mối đe dọa gây hại
d) Kết quả của việc khai thác lỗ hổng
48. Tấn công từ điển (Dictionary attack) là gì?
a) Tấn công sử dụng từ điển để tìm lỗi trong mã nguồn
* b) Tấn công dựa trên việc thử các từ thường được sử dụng làm mật khẩu trong từ điển
c) Tấn công nhằm đánh cắp từ điển dữ liệu
d) Tấn công sử dụng từ điển để mã hóa dữ liệu
49. Điểm yếu (Weakness) là gì?
a) Bất kỳ hành động nào có thể gây thiệt hại cho tài nguyên hệ thống
b) Điểm yếu trong hệ thống cho phép mối đe dọa gây hại

* c) Một lỗi hoặc khiếm khuyết tồn tại trong hệ thống
d) Kết quả của việc khai thác mối đe dọa

51. Lỗ hổng (Vulnerability) là gì?
a) Bất kỳ hành động nào có thể gây thiệt hại cho tài nguyên hệ thống
* b) Điểm yếu trong hệ thống cho phép mối đe dọa gây hại
c) Một lỗi hoặc khiếm khuyết tồn tại trong hệ thống
d) Kết quả của việc khai thác mối đe dọa

53. Mối quan hệ giữa Mối đe dọa và Lỗ hổng là gì?
a) Mối đe dọa luôn tạo ra lỗ hổng
b) Lỗ hổng luôn tạo ra mối đe dọa
* c) Mối đe dọa thường khai thác một hoặc nhiều lỗ hổng đã biết để thực hiện các cuộc tấn công phá hoại
d) Mối đe dọa và lỗ hổng không liên quan đến nhau

56. Tấn công chủ động (Active attack) bao gồm những hành động nào?
a) Chỉ nghe lén và theo dõi lưu lượng trên đường truyền
b) Chỉ sửa đổi dữ liệu trên đường truyền
c) Chỉ truy cập trái phép vào máy tính hoặc mạng
* d) Sửa đổi dữ liệu trên đường truyền, sửa đổi dữ liệu trong tệp, truy cập trái phép vào máy tính hoặc mạng
57. Tấn công nghe lén (Eavesdropping) thuộc loại tấn công nào?
a) Tấn công chủ động
* b) Tấn công thụ động
c) Tấn công giả mạo
d) Tấn công gián đoạn
58. Mối quan hệ giữa tấn công thụ động và tấn công chủ động là gì?
a) Tấn công thụ động luôn xảy ra sau tấn công chủ động
* b) Tấn công thụ động thường là giai đoạn đầu tiên của tấn công chủ động
c) Tấn công thụ động và tấn công chủ động không liên quan đến nhau
d) Tấn công chủ động luôn xảy ra sau tấn công thụ động
59. Tấn công vét cạn (Brute force attack) là gì?
a) Tấn công sử dụng từ điển để đoán mật khẩu
* b) Tấn công sử dụng tổ hợp ký tự và thử tự động
c) Tấn công sử dụng kỹ thuật xã hội để lấy mật khẩu
d) Tấn công sử dụng phần mềm độc hại để đánh cắp mật khẩu

60. Tấn công tràn bộ đệm (Buffer overflow) là gì?
a) Tấn công nhằm làm đầy bộ nhớ của hệ thống
* b) Lỗi xảy ra khi ứng dụng cố gắng ghi dữ liệu vượt quá phạm vi bộ đệm
c) Tấn công nhằm xóa dữ liệu trong bộ đệm
d) Tấn công nhằm đọc dữ liệu từ bộ đệm
61. Các thành phần của an toàn thông tin bao gồm:
a) An toàn máy tính, an toàn mạng, an toàn ứng dụng
b) An toàn phần cứng, an toàn phần mềm, an toàn dữ liệu, an toàn mạng
* c) An toàn máy tính và dữ liệu, an toàn mạng, quản lý an toàn thông tin, chính sách an toàn thông tin
d) An toàn vật lý, an toàn logic, an toàn kỹ thuật, an toàn quản lý
62. Tính bảo mật (Confidentiality) được định nghĩa là:
a) Thông tin chỉ có thể được sửa đổi bởi người dùng được ủy quyền
b) Thông tin có thể được truy cập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu
* c) Chỉ người dùng được ủy quyền mới có thể truy cập thông tin
d) Đảm bảo thông tin, hệ thống và người dùng là thật, không bị giả mạo
63. Tính toàn vẹn (Integrity) được định nghĩa là:
* a) Thông tin chỉ có thể được sửa đổi bởi người dùng được ủy quyền
b) Thông tin có thể được truy cập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu
c) Chỉ người dùng được ủy quyền mới có thể truy cập thông tin
d) Đảm bảo thông tin, hệ thống và người dùng là thật, không bị giả mạo
64. Tính sẵn sàng (Availability) được định nghĩa là:
a) Thông tin chỉ có thể được sửa đổi bởi người dùng được ủy quyền
* b) Thông tin có thể được truy cập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu
c) Chỉ người dùng được ủy quyền mới có thể truy cập thông tin
d) Đảm bảo thông tin, hệ thống và người dùng là thật, không bị giả mạo
65. Tính sẵn sàng có thể được đo lường bằng các yếu tố nào?
a) Chỉ thời gian hoạt động và thời gian ngừng hoạt động
b) Chỉ tỷ lệ dịch vụ
c) Chỉ thời gian trung bình giữa các sự cố
* d) Thời gian hoạt động, thời gian ngừng hoạt động, tỷ lệ dịch vụ, thời gian trung bình giữa các sự cố, thời gian trung bình để dừng sửa chữa, thời gian phục hồi sau

Chương 2

2.1 Tổng quan về mật mã hoá

1. Theo từ điển Free Online Dictionary of Computing, mật mã học (cryptography) là gì?

a) Một quá trình giải mã thông điệp đã bị mã hóa

b) Một quá trình chuyển đổi dữ liệu có kích thước thay đổi về dữ liệu có kích thước cố định

*c) Việc mã hóa dữ liệu mà chỉ có thể được giải mã bởi một số người chỉ định

d) Một quá trình tạo ra các khóa mã hóa

2. Mã hóa khóa đối xứng (symmetric key cryptography) và mã hóa khóa bất đối xứng (asymmetric key cryptography) là gì?

a) Hai phương pháp giải mã khác nhau

*b) Hai loại mã hóa sử dụng các loại khóa khác nhau

c) Hai phương pháp tạo hàm băm

d) Hai phương pháp thám mã

3. Các thành phần cơ bản của một hệ thống mật mã (cryptosystem) bao gồm:

a) Bản rõ (plaintext), bản mã (ciphertext), không gian khóa (key space)

b) Giải thuật mã hóa, giải thuật giải mã, hàm băm

c) Khóa mã hóa, khóa giải mã, thám mã

*d) Bản rõ, bản mã, giải thuật mã hóa, giải thuật giải mã, khóa mã hóa và khóa giải mã

4. Mối quan hệ giữa mật mã học và toán học là gì?

a) Mật mã học phát triển độc lập với toán học

*b) Mật mã học là con đẻ của toán học và phát triển đi liền với sự phát triển của toán học

c) Toán học là ứng dụng của mật mã học

d) Mật mã học và toán học không có mối liên hệ với nhau

5. Bản rõ (plaintext) trong hệ thống mật mã là gì?

*a) Thông điệp gốc trước khi được mã hóa

b) Thông điệp sau khi đã được mã hóa

c) Khóa dùng để mã hóa thông điệp

d) Giải thuật dùng để mã hóa thông điệp

6. Bản mã (ciphertext) trong hệ thống mật mã là gì?

a) Thông điệp gốc trước khi được mã hóa
*b) Thông điệp sau khi đã được mã hóa
c) Khóa dùng để mã hóa thông điệp
d) Giải thuật dùng để mã hóa thông điệp

7. Khóa mã hóa (encryption key) trong hệ thống mật mã có tác dụng gì?
a) Giải mã bản mã thành bản rõ
*b) Mã hóa bản rõ thành bản mã
c) Tạo ra hàm băm
d) Phân tích và phá vỡ mã

8. Không gian khóa (key space) trong hệ thống mật mã là gì?
a) Kích thước của khóa mã hóa
b) Số lượng bit trong khóa
*c) Tập hợp tất cả các khóa có thể có
d) Vị trí lưu trữ khóa mã hóa

9. Hàm băm (hash function) trong an toàn thông tin là gì?
a) Một giải thuật mã hóa dữ liệu
b) Một giải thuật giải mã dữ liệu
*c) Một ánh xạ chuyển các dữ liệu có kích thước thay đổi về dữ liệu có kích thước cố định
d) Một phương pháp phân phối khóa mã hóa

10. Thám mã (cryptanalysis) là gì?
a) Quá trình tạo ra các khóa mã hóa mới
b) Quá trình mã hóa thông điệp
*c) Quá trình giải mã thông điệp đã bị mã hóa mà không cần có trước thông tin về giải thuật mã hóa và khóa mã
d) Quá trình tạo ra các giải thuật mã hóa mới

11. Mối quan hệ giữa không gian khóa và độ an toàn của hệ thống mật mã là gì?
a) Không gian khóa càng nhỏ, hệ thống mật mã càng an toàn
b) Không gian khóa không ảnh hưởng đến độ an toàn của hệ thống mật mã
*c) Không gian khóa càng lớn, hệ thống mật mã càng an toàn
d) Không gian khóa và độ an toàn của hệ thống mật mã không có mối liên hệ

12. Trong mã hóa khóa đối xứng (symmetric key cryptography), đặc điểm của khóa là gì?
*a) Khóa mã hóa và khóa giải mã giống nhau
b) Khóa mã hóa và khóa giải mã hoàn toàn khác nhau
c) Chỉ sử dụng một khóa duy nhất cho mọi người dùng
d) Không sử dụng khóa trong quá trình mã hóa

13. Trong mã hóa khóa bất đối xứng (asymmetric key cryptography), đặc điểm của khóa là gì?

a) Khóa mã hóa và khóa giải mã giống nhau

*b) Khóa mã hóa và khóa giải mã khác nhau và không thể dễ dàng suy ra từ nhau

c) Chỉ sử dụng một khóa duy nhất cho mọi người dùng

d) Không sử dụng khóa trong quá trình mã hóa

14. Ứng dụng chính của mã hóa khóa đối xứng (symmetric key cryptography) là gì?

a) Chỉ dùng để xác thực người dùng

b) Chỉ dùng để tạo chữ ký số

*c) Mã hóa dữ liệu với tốc độ nhanh và hiệu quả

d) Chỉ dùng để phân phối khóa

15. Ứng dụng chính của mã hóa khóa bất đối xứng (asymmetric key cryptography) là gì?

a) Chỉ dùng để mã hóa dữ liệu với tốc độ cao

*b) Xác thực, chữ ký số và trao đổi khóa an toàn

c) Chỉ dùng để tạo hàm băm

d) Chỉ dùng để thám mã

16. Vai trò của giải thuật mã hóa (encryption algorithm) trong hệ thống mật mã là gì?

a) Tạo ra khóa mã hóa

b) Phân phối khóa mã hóa

*c) Chuyển đổi bản rõ thành bản mã bằng cách sử dụng khóa mật mã

d) Phân tích và phá vỡ mã

17. Tại sao việc tăng kích thước khóa làm tăng độ an toàn của hệ thống mật mã?

a) Vì nó làm tăng tốc độ mã hóa

b) Vì nó làm giảm kích thước của bản mã

*c) Vì nó mở rộng không gian khóa, khiến việc tấn công vét cạn (brute force) trở nên khó khăn hơn

d) Vì nó làm giảm độ phức tạp của giải thuật mã hóa

18. Sự phát triển của mật mã học hiện đại có mối liên hệ như thế nào với toán học?

a) Mật mã học hiện đại phát triển độc lập với toán học

b) Mật mã học hiện đại chỉ dựa vào lý thuyết thông tin

c) Mật mã học hiện đại chỉ dựa vào lý thuyết độ phức tạp tính toán

*d) Mật mã học hiện đại dựa trên các bài toán khó trong toán học như phân tích thừa số số nguyên lớn và logarithm rời rạc

2.2 Mật mã hoá khoá đối xứng

1. Mã hóa khóa đối xứng (symmetric key cryptography) có đặc điểm gì?
   a) Sử dụng hai khóa khác nhau để mã hóa và giải mã
   *b) Sử dụng cùng một khóa để mã hóa và giải mã
   c) Không sử dụng khóa trong quá trình mã hóa và giải mã
   d) Chỉ sử dụng khóa công khai (public key)
2. Ưu điểm chính của mã hóa khóa đối xứng (symmetric key cryptography) là gì?
   a) Dễ dàng trong việc quản lý khóa
   b) Không cần bảo vệ tính bí mật của khóa
   *c) Tốc độ mã hóa và giải mã nhanh, hiệu quả với dữ liệu lớn
   d) Không cần trao đổi khóa trước khi truyền thông
3. Nhược điểm chính của mã hóa khóa đối xứng (symmetric key cryptography) là gì?
   *a) Khó khăn trong việc trao đổi khóa an toàn giữa các bên
   b) Tốc độ mã hóa và giải mã chậm
   c) Không thể mã hóa dữ liệu lớn
   d) Không thể đảm bảo tính toàn vẹn dữ liệu
4. Mã hóa khối (block cipher) là gì?
   a) Phương pháp mã hóa từng bit một của bản rõ
   *b) Phương pháp mã hóa chia bản rõ thành các khối có kích thước cố định và mã hóa từng khối
   c) Phương pháp mã hóa không sử dụng khóa
   d) Phương pháp mã hóa chỉ áp dụng cho dữ liệu văn bản
5. Mã hóa dòng (stream cipher) là gì?
   *a) Phương pháp mã hóa từng bit hoặc từng byte một của bản rõ
   b) Phương pháp mã hóa chia bản rõ thành các khối có kích thước cố định
   c) Phương pháp mã hóa không sử dụng khóa
   d) Phương pháp mã hóa chỉ áp dụng cho dữ liệu nhị phân
6. Thuật toán DES (Data Encryption Standard) có kích thước khóa (không tính các bit kiểm tra) là bao nhiêu?
   a) 128 bit
   b) 192 bit
   *c) 56 bit

d) 64 bit

7. Thuật toán AES (Advanced Encryption Standard) hỗ trợ kích thước khóa nào?

a) Chỉ 56 bit

b) Chỉ 64 bit

c) Chỉ 128 bit

*d) 128 bit, 192 bit và 256 bit

8. Chế độ ECB (Electronic Codebook) trong mã hóa khối có đặc điểm gì?

a) Mỗi khối được mã hóa phụ thuộc vào khối trước đó

*b) Mỗi khối được mã hóa độc lập với các khối khác

c) Sử dụng một vector khởi tạo (IV) để mã hóa khối đầu tiên

d) Chuyển đổi mã hóa khối thành mã hóa dòng

9. Chế độ CBC (Cipher Block Chaining) trong mã hóa khối có đặc điểm gì?

*a) Mỗi khối bản rõ được XOR với khối bản mã trước đó trước khi mã hóa

b) Mỗi khối được mã hóa độc lập với các khối khác

c) Tạo ra một dòng khóa để XOR với bản rõ

d) Chỉ mã hóa sự khác biệt giữa các khối liên tiếp

10. Chế độ CTR (Counter) trong mã hóa khối có đặc điểm gì?

a) Mỗi khối bản rõ được XOR với khối bản mã trước đó trước khi mã hóa

b) Mỗi khối được mã hóa độc lập với các khối khác

*c) Mã hóa một bộ đếm và XOR kết quả với bản rõ để tạo bản mã

d) Chỉ mã hóa sự khác biệt giữa các khối liên tiếp

11. Tại sao chế độ ECB (Electronic Codebook) không được khuyến nghị sử dụng cho dữ liệu lớn?

a) Vì tốc độ mã hóa quá chậm

b) Vì tiêu tốn quá nhiều tài nguyên hệ thống

*c) Vì các khối bản rõ giống nhau sẽ tạo ra các khối bản mã giống nhau, làm lộ mẫu dữ liệu

d) Vì không thể giải mã chính xác

12. Thuật toán 3DES (Triple DES) là gì?

a) Một thuật toán mã hóa hoàn toàn mới, không liên quan đến DES

*b) Một biến thể của DES, áp dụng thuật toán DES ba lần cho mỗi khối dữ liệu

c) Một thuật toán mã hóa sử dụng ba khóa khác nhau đồng thời

d) Một thuật toán mã hóa có tốc độ gấp ba lần DES

13. Trong AES (Advanced Encryption Standard), số vòng lặp (rounds) phụ thuộc vào yếu tố nào?

a) Kích thước của bản rõ
*b) Kích thước của khóa
c) Chế độ mã hóa được sử dụng
d) Loại dữ liệu được mã hóa

14. Chế độ OFB (Output Feedback) trong mã hóa khối có đặc điểm gì?
a) Mỗi khối bản rõ được XOR với khối bản mã trước đó trước khi mã hóa
b) Mỗi khối được mã hóa độc lập với các khối khác
*c) Tạo ra một dòng khóa bằng cách mã hóa liên tiếp đầu ra của bước trước đó, sau đó XOR với bản rõ
d) Chỉ mã hóa sự khác biệt giữa các khối liên tiếp

15. Tại sao AES (Advanced Encryption Standard) được chọn để thay thế DES (Data Encryption Standard)?
a) Vì AES dễ triển khai hơn
b) Vì AES sử dụng ít tài nguyên hệ thống hơn
*c) Vì DES có kích thước khóa nhỏ (56 bit) dễ bị tấn công vét cạn (brute force)
d) Vì DES không thể mã hóa dữ liệu nhị phân

16. Trong mã hóa khối, padding là gì?
*a) Kỹ thuật thêm dữ liệu vào khối cuối cùng để đạt đủ kích thước khối yêu cầu
b) Kỹ thuật giảm kích thước của khối để tăng tốc độ mã hóa
c) Kỹ thuật tạo ra khóa mã hóa từ mật khẩu người dùng
d) Kỹ thuật nén dữ liệu trước khi mã hóa

17. Kích thước khối (block size) của thuật toán AES là bao nhiêu?
a) 64 bit
*b) 128 bit
c) 192 bit
d) 256 bit

18. Ưu điểm của mã hóa dòng (stream cipher) so với mã hóa khối (block cipher) là gì?
a) Luôn an toàn hơn trong mọi trường hợp
b) Không cần sử dụng khóa mã hóa
*c) Thích hợp cho dữ liệu thời gian thực và có độ trễ thấp
d) Không thể bị phân tích mật mã học

20. Thuật toán RC4 là một ví dụ của loại mã hóa nào?
a) Mã hóa khối (block cipher)

*b) Mã hóa dòng (stream cipher)
c) Mã hóa khóa bất đối xứng (asymmetric key cryptography)
d) Hàm băm mật mã (cryptographic hash function)

2.3 Mật mã hoá khoá bất đối xứng

1. Mã hóa khóa bất đối xứng (asymmetric key cryptography) có đặc điểm gì?
a) Sử dụng cùng một khóa để mã hóa và giải mã
*b) Sử dụng một cặp khóa: khóa công khai (public key) và khóa bí mật (private key)
c) Không sử dụng khóa trong quá trình mã hóa và giải mã
d) Chỉ sử dụng một khóa duy nhất cho mọi người dùng
2. Trong mã hóa khóa bất đối xứng (asymmetric key cryptography), mối quan hệ giữa khóa công khai và khóa bí mật là gì?
a) Hai khóa giống hệt nhau
b) Hai khóa hoàn toàn độc lập, không liên quan đến nhau
*c) Hai khóa có liên quan toán học với nhau, nhưng không thể dễ dàng tính ra khóa bí mật từ khóa công khai
d) Khóa công khai luôn được tạo ra từ khóa bí mật bằng cách đảo ngược các bit
3. Ưu điểm chính của mã hóa khóa bất đối xứng (asymmetric key cryptography) là gì?
a) Tốc độ mã hóa và giải mã nhanh hơn mã hóa khóa đối xứng
*b) Giải quyết vấn đề trao đổi khóa an toàn và cung cấp cơ chế xác thực, chữ ký số
c) Sử dụng ít tài nguyên hệ thống hơn
d) Không cần bảo vệ tính bí mật của bất kỳ khóa nào
4. Nhược điểm chính của mã hóa khóa bất đối xứng (asymmetric key cryptography) là gì?
*a) Tốc độ mã hóa và giải mã chậm hơn nhiều so với mã hóa khóa đối xứng
b) Không thể mã hóa dữ liệu lớn
c) Không thể đảm bảo tính toàn vẹn dữ liệu
d) Khó khăn trong việc trao đổi khóa
5. Thuật toán RSA dựa trên bài toán khó nào trong toán học?
a) Logarithm rời rạc (discrete logarithm)
*b) Phân tích thừa số số nguyên lớn (factoring large integers)
c) Đường cong elliptic (elliptic curve)
d) Bài toán ba-lô (knapsack problem)

6. Trong mã hóa RSA, để đảm bảo tính bảo mật, thông điệp được mã hóa bằng khóa nào và giải mã bằng khóa nào?

a) Mã hóa bằng khóa bí mật, giải mã bằng khóa công khai

*b) Mã hóa bằng khóa công khai của người nhận, giải mã bằng khóa bí mật của người nhận

c) Mã hóa bằng khóa công khai của người gửi, giải mã bằng khóa bí mật của người gửi

d) Mã hóa và giải mã đều sử dụng khóa công khai

7. Trong mã hóa khóa bất đối xứng (asymmetric key cryptography), khóa nào cần được bảo vệ và giữ bí mật?

a) Cả khóa công khai và khóa bí mật

b) Không cần bảo vệ bất kỳ khóa nào

*c) Chỉ khóa bí mật (private key)

d) Chỉ khóa công khai (public key)

8. Chữ ký số (digital signature) được sử dụng để đảm bảo tính chất nào của thông điệp?

a) Chỉ tính bảo mật (confidentiality)

b) Chỉ tính toàn vẹn (integrity)

*c) Tính xác thực nguồn gốc (authentication) và tính không thể chối bỏ (non-repudiation)

d) Chỉ tính sẵn sàng (availability)

9. Hạ tầng khóa công khai (PKI - Public Key Infrastructure) là gì?

a) Một thuật toán mã hóa mới

b) Một phương pháp tạo khóa ngẫu nhiên

*c) Một hệ thống quản lý khóa công khai, bao gồm các thành phần như CA, chứng thư số, và các chính sách

d) Một phương pháp phân phối khóa đối xứng

10. Cơ quan cấp chứng thư số (CA - Certificate Authority) có vai trò gì trong hạ tầng khóa công khai (PKI)?

a) Tạo ra khóa bí mật cho người dùng

b) Mã hóa và giải mã thông điệp thay cho người dùng

*c) Xác thực danh tính người dùng và cấp chứng thư số xác nhận khóa công khai của họ

d) Lưu trữ tất cả các khóa bí mật của người dùng

11. Chứng thư số (digital certificate) chứa những thông tin gì?

a) Khóa bí mật của người dùng
b) Tất cả các thông điệp đã được mã hóa của người dùng
*c) Khóa công khai của người dùng, thông tin định danh và chữ ký số của CA
d) Mật khẩu đăng nhập của người dùng

12. Tại sao mã hóa khóa bất đối xứng (asymmetric key cryptography) thường không được sử dụng để mã hóa trực tiếp các thông điệp lớn?
a) Vì không đủ an toàn cho dữ liệu lớn
b) Vì không thể mã hóa dữ liệu lớn hơn kích thước khóa
*c) Vì tốc độ mã hóa và giải mã chậm, không hiệu quả với dữ liệu lớn
d) Vì dễ bị tấn công hơn với dữ liệu lớn

13. Kích thước khóa RSA thông thường được khuyến nghị sử dụng hiện nay là bao nhiêu để đảm bảo an toàn?
a) 512 bit
b) 768 bit
*c) 2048 bit hoặc lớn hơn
d) 128 bit

14. Trong mã hóa khóa bất đối xứng (asymmetric key cryptography), phương pháp nào thường được sử dụng để mã hóa hiệu quả các thông điệp lớn?
a) Tăng kích thước khóa bất đối xứng
*b) Kết hợp mã hóa đối xứng và bất đối xứng: mã hóa thông điệp bằng khóa đối xứng, sau đó mã hóa khóa đối xứng bằng khóa công khai
c) Chia thông điệp thành nhiều phần nhỏ và mã hóa từng phần riêng biệt
d) Sử dụng nhiều cặp khóa bất đối xứng khác nhau

15. Trong RSA, cặp số nguyên tố lớn được dùng để tạo khóa được ký hiệu là gì?
a) e và d
*b) p và q
c) n và φ(n)
d) a và b

16. Trong RSA, giá trị n trong khóa công khai và khóa bí mật được tính như thế nào?
a) $n = p + q$
b) $n = p - q$
*c) $n = p \times q$
d) $n = p / q$

17. Khóa công khai trong RSA bao gồm những thành phần nào?
a) (p, q)
b) (n, d)

*c) (n, e)

d) (q, d)

18. Điều kiện nào sau đây là đúng khi chọn giá trị e trong RSA?

a) e phải là số nguyên tố nhỏ hơn p

b) e chia hết cho φ(n)

*c) e và φ(n) phải nguyên tố cùng nhau

d) e phải lớn hơn n

19. Giá trị d trong khóa bí mật RSA được tính như thế nào?

a) d = e × φ(n)

*b) d là nghịch đảo modular của e theo modulo φ(n)

c) d = n − e

d) d = p × q − e

20. Trong RSA, phép mã hóa được thực hiện như thế nào để đảm bảo tính bảo mật cho bản rõ m?

a) C = m × e mod n

*b) C = m^e mod n

c) C = e^m mod n

d) C = (m + e) mod n

21. Cho hai số nguyên tố p = 17 và q =11, giá trị n trong RSA bằng bao nhiêu?

a) 187

*b) 187

c) 28

d) 204

2.4 Quản lý và phân phối khoá

1. Trong hệ thống mật mã (cryptosystem), khóa phiên (session key) có đặc điểm gì?

a) Được sử dụng lâu dài và ít khi thay đổi

*b) Là khóa tạm thời, được sử dụng trong một phiên giao dịch và bị xóa bỏ sau khi sử dụng

c) Được sử dụng để mã hóa khóa chủ

d) Được phân phối thủ công giữa các bên tham gia

2. Trong hệ thống mật mã (cryptosystem), khóa chủ (master key) có đặc điểm gì?

*a) Được sử dụng lâu dài và dùng để mã hóa khóa phiên

b) Là khóa tạm thời, được sử dụng trong một phiên giao dịch

c) Được thay đổi tự động sau mỗi phiên giao dịch

d) Chỉ được sử dụng trong mã hóa khóa bất đối xứng (asymmetric key cryptography)

3. Trung tâm phân phối khóa (KDC - Key Distribution Center) có vai trò gì trong hệ thống mật mã (cryptosystem)?

a) Tạo ra các khóa công khai cho mọi người dùng

b) Lưu trữ tất cả các bản mã (ciphertext) đã được mã hóa

*c) Là bên thứ ba đáng tin cậy, giúp phân phối khóa phiên giữa các bên tham gia

d) Giải mã các thông điệp khi người dùng quên khóa

4. Tại sao cần thay đổi khóa phiên (session key) thường xuyên?

a) Để tiết kiệm tài nguyên hệ thống

b) Để tăng tốc độ mã hóa và giải mã

*c) Để tránh các tấn công thám mã (cryptanalysis) do sử dụng khóa quá lâu

d) Để giảm kích thước của khóa

5. Trong phân phối khóa đối xứng (symmetric key distribution), phương pháp phân phối không tập trung có nghĩa là gì?

a) Tất cả các khóa được lưu trữ tại một máy chủ trung tâm

*b) Mỗi người dùng phải trao đổi khóa chủ một cách thủ công với tất cả người dùng khác

c) Không cần sử dụng khóa để mã hóa thông tin

d) Chỉ có một khóa duy nhất được sử dụng trong toàn hệ thống

6. Giá trị Nonce trong phân phối khóa có đặc điểm gì?

a) Là một khóa bí mật được sử dụng nhiều lần

b) Là một giải thuật mã hóa (encryption algorithm) đặc biệt

*c) Là một số được sử dụng một lần, thường là số ngẫu nhiên hoặc số đếm

d) Là một loại mã hóa không sử dụng khóa

7. Chứng thư số khóa công khai (digital certificate) bao gồm những thông tin gì?

a) Chỉ có khóa bí mật (private key) của người dùng

b) Chỉ có danh tính của cơ quan cấp chứng thư

*c) Khóa công khai (public key), danh tính của chủ sở hữu và chữ ký số (digital signature) của cơ quan cấp chứng thư

d) Toàn bộ lịch sử giao dịch của người dùng

8. Ưu điểm chính của phương pháp thông báo công khai trong phân phối khóa công khai (public key distribution) là gì?

*a) Đơn giản và thuận tiện

b) Bảo mật cao nhất

c) Không thể bị giả mạo

d) Không cần bên thứ ba đáng tin cậy

9. Trong phân phối khóa tập trung qua KDC, quy trình cơ bản diễn ra như thế nào?

a) Người dùng tự tạo khóa phiên và gửi cho nhau

*b) Người dùng A gửi yêu cầu đến KDC, KDC tạo khóa phiên (session key) và gửi cho cả A và B

c) KDC tự động gửi khóa phiên cho tất cả người dùng định kỳ

d) Người dùng A và B trao đổi khóa công khai (public key) với nhau qua KDC

10. Thời gian sống của khóa phiên (session key) trong giao thức hướng kết nối (TCP) thường được xác định như thế nào?

a) Cố định là 24 giờ

b) Cố định là 1 giờ

*c) Mỗi kết nối yêu cầu một khóa phiên mới

d) Thay đổi sau một số lượng byte cố định

11. Trong phương pháp thư mục khóa công khai (public key directory), làm thế nào để đảm bảo tính xác thực của khóa?

a) Không cần xác thực vì khóa công khai luôn an toàn

b) Mỗi người dùng tự xác thực khóa của mình

*c) Người dùng đăng ký khóa với bên thẩm quyền quản lý danh mục thông qua kênh được chứng thực an toàn

d) Sử dụng mã hóa khóa đối xứng (symmetric key cryptography) để bảo vệ khóa công khai

12. Tại sao việc sử dụng mã hóa khóa bất đối xứng (asymmetric key cryptography) để phân phối khóa đối xứng (symmetric key) lại hiệu quả?

a) Vì mã hóa khóa bất đối xứng luôn nhanh hơn mã hóa khóa đối xứng

b) Vì không cần sử dụng khóa phiên

*c) Vì kết hợp được ưu điểm của cả hai: tốc độ của mã hóa khóa đối xứng và khả năng phân phối khóa an toàn của mã hóa khóa bất đối xứng

d) Vì giảm được kích thước của khóa

13. Trong phân phối khóa công khai qua trung tâm thẩm quyền, làm thế nào để A xác thực rằng thông điệp nhận được thực sự đến từ B?

a) A tin tưởng trung tâm thẩm quyền mà không cần xác thực
b) A kiểm tra chữ ký số (digital signature) của trung tâm thẩm quyền
*c) A gửi một nonce (N1) cho B và B phải trả lại đúng nonce đó
d) A và B phải gặp nhau trực tiếp để xác thực

14. Vấn đề chính trong phân phối khóa công khai (public key distribution) là gì?
a) Khóa công khai quá dài nên khó phân phối
b) Khóa công khai dễ bị đánh cắp
*c) Làm sao đảm bảo khóa công khai thực sự thuộc về người mà nó tuyên bố thuộc về
d) Khóa công khai không thể được sử dụng để mã hóa dữ liệu

15. Trong hệ thống chứng thư số khóa công khai, vai trò của cơ quan cấp chứng thư (CA - Certificate Authority) là gì?
a) Tạo ra khóa bí mật (private key) cho người dùng
b) Lưu trữ tất cả các khóa bí mật
*c) Xác thực danh tính người dùng và ký số chứng thư chứa khóa công khai (public key) của họ
d) Mã hóa và giải mã thông điệp thay cho người dùng

16. Khi sử dụng phương pháp phân phối khóa tập trung qua KDC, vấn đề nghẽn cổ chai (bottleneck) có thể xảy ra như thế nào?
a) KDC tạo ra quá nhiều khóa phiên không cần thiết
b) Khóa phiên quá dài làm chậm quá trình truyền
*c) Tất cả các yêu cầu phân phối khóa đều phải thông qua KDC, có thể gây quá tải khi số lượng người dùng lớn
d) Khóa chủ quá ngắn dễ bị tấn công vét cạn (brute force attack)

17. Trong quy trình phân phối khóa qua KDC, giả sử A muốn thiết lập kết nối an toàn với B, khi KDC nhận được yêu cầu từ A, KDC sẽ trả về những thông tin gì?
a) Chỉ khóa phiên Ks được mã hóa bằng khóa chủ của A
b) Khóa phiên Ks được mã hóa bằng khóa chủ của B
*c) Khóa phiên Ks được mã hóa bằng khóa chủ của A và một bản tin chứa khóa phiên Ks và định danh của A được mã hóa bằng khóa chủ của B
d) Khóa phiên Ks ở dạng bản rõ (plaintext) và định danh của A và B

18. Phân tích tại sao phương pháp thông báo công khai trong phân phối khóa công khai dễ bị tấn công Man-in-the-Middle:
a) Vì khóa công khai quá ngắn nên dễ bị phá giải
b) Vì người dùng thường quên khóa công khai của mình

*c) Vì kẻ tấn công có thể chặn thông báo gốc và thay thế bằng khóa công khai của chính họ, làm cho người nhận tin rằng đó là khóa công khai của người gửi thực sự

d) Vì khóa công khai không thể được sử dụng để mã hóa dữ liệu lớn

2.5 Một số giao thức đảm bảo an toàn thông tin dựa trên mật mã hoá

1. IPsec (Internet Protocol Security) hoạt động ở lớp nào trong mô hình TCP/IP?
   a) Lớp ứng dụng (Application Layer)
   b) Lớp giao vận (Transport Layer)
   *c) Lớp mạng (Network Layer)
   d) Lớp liên kết dữ liệu (Data Link Layer)
2. SSL/TLS (Secure Socket Layer/Transport Layer Security) hoạt động ở lớp nào trong mô hình TCP/IP?
   a) Lớp ứng dụng (Application Layer)
   *b) Lớp giao vận (Transport Layer)
   c) Lớp mạng (Network Layer)
   d) Lớp liên kết dữ liệu (Data Link Layer)
3. PGP (Pretty Good Privacy) được sử dụng chủ yếu để bảo vệ loại dữ liệu nào?
   a) Dữ liệu truyền qua giao thức HTTP
   *b) Thư điện tử (Email)
   c) Dữ liệu truyền qua mạng riêng ảo (VPN)
   d) Dữ liệu truyền qua giao thức FTP
4. Trong IPsec, ESP (Encapsulation Security Payload) cung cấp những dịch vụ an toàn nào?
   a) Chỉ tính xác thực
   b) Chỉ tính bảo mật
   *c) Cả tính bảo mật và tính xác thực
   d) Chỉ tính toàn vẹn dữ liệu
5. Trong IPsec, AH (Authentication Header) cung cấp những dịch vụ an toàn nào?
   *a) Tính xác thực và tính toàn vẹn dữ liệu
   b) Tính bảo mật và tính xác thực
   c) Chỉ tính bảo mật
   d) Chỉ tính không từ chối
6. Thuật toán mã hóa nào thường được sử dụng trong ESP của IPsec?
   a) RSA và DSA

b) MD5 và SHA-1

*c) DES, 3DES hoặc AES

d) Diffie-Hellman

7. Trong IPsec, khi sử dụng kết hợp cả AH và ESP trong chế độ vận chuyển (Transport mode), thứ tự xử lý gói tin nào là chính xác?

a) Áp dụng AH trước, sau đó áp dụng ESP

*b) Áp dụng ESP trước, sau đó áp dụng AH

c) Áp dụng AH và ESP đồng thời

d) Không thể kết hợp AH và ESP trong chế độ vận chuyển

8. PGP sử dụng kết hợp những kỹ thuật mật mã học (cryptography) nào?

a) Chỉ mã hóa khóa đối xứng (symmetric key cryptography)

b) Chỉ mã hóa khóa bất đối xứng (asymmetric key cryptography)

*c) Mã hóa khóa đối xứng, mã hóa khóa bất đối xứng, hàm băm (hash function) và chữ ký số (digital signature)

d) Chỉ hàm băm và chữ ký số

9. Trong IPsec, chế độ vận chuyển (Transport mode) có đặc điểm gì?

a) Các gateway thực hiện quá trình xử lý mật mã

*b) Các máy chủ nguồn và đích trực tiếp thực hiện tất cả các thao tác mã hóa

c) Chỉ bảo vệ phần payload của gói tin

d) Chỉ sử dụng giao thức AH, không sử dụng ESP

10. Trong IPsec, chế độ đường hầm (Tunnel mode) có đặc điểm gì?

a) Các máy chủ nguồn và đích trực tiếp thực hiện tất cả các thao tác mã hóa

*b) Các gateway thực hiện quá trình xử lý mật mã, không phải các máy chủ nguồn và đích

c) Chỉ bảo vệ phần header của gói tin

d) Chỉ sử dụng giao thức ESP, không sử dụng AH

11. Trong SSL/TLS, Record Protocol có chức năng gì?

a) Thiết lập phiên làm việc và trao đổi khóa

b) Thông báo lỗi và cảnh báo

*c) Phân mảnh, nén, mã hóa và xác thực dữ liệu

d) Cập nhật trạng thái mật mã của kết nối

12. Trong SSL/TLS, Handshake Protocol có chức năng gì?

*a) Xác thực các bên tham gia và thỏa thuận thuật toán, khóa mã hóa

b) Phân mảnh và nén dữ liệu

c) Truyền đạt cảnh báo cho đối tượng kết nối

d) Mã hóa và giải mã dữ liệu

13. Trong PGP, để đảm bảo tính bí mật của email, quy trình mã hóa diễn ra như thế nào?

a) Mã hóa email bằng khóa bí mật (private key) của người gửi

b) Mã hóa email bằng khóa bí mật của người nhận

*c) Tạo khóa phiên (session key) ngẫu nhiên, mã hóa email bằng khóa phiên, sau đó mã hóa khóa phiên bằng khóa công khai (public key) của người nhận

d) Mã hóa email bằng khóa công khai của người gửi

14. Trong PGP, để đảm bảo tính xác thực của email, quy trình ký số diễn ra như thế nào?

a) Ký email bằng khóa công khai (public key) của người gửi

*b) Tạo giá trị băm (hash value) của email, sau đó mã hóa giá trị băm bằng khóa bí mật (private key) của người gửi

c) Ký email bằng khóa bí mật của người nhận

d) Tạo giá trị băm của email, sau đó mã hóa giá trị băm bằng khóa công khai của người nhận

15. Trong SSL/TLS, MAC (Message Authentication Code) được sử dụng để làm gì?

a) Mã hóa dữ liệu

*b) Đảm bảo tính toàn vẹn của dữ liệu

c) Xác thực danh tính của máy chủ

d) Trao đổi khóa bí mật

16. So sánh IPsec và SSL/TLS, nhận xét nào sau đây là chính xác?

a) IPsec và SSL/TLS đều hoạt động ở lớp giao vận và cung cấp các dịch vụ an toàn giống nhau

b) IPsec cung cấp tính bảo mật tốt hơn SSL/TLS trong mọi trường hợp

c) SSL/TLS dễ triển khai hơn IPsec nhưng không hỗ trợ xác thực hai chiều

*d) IPsec hoạt động ở lớp mạng nên trong suốt với ứng dụng, trong khi SSL/TLS hoạt động ở lớp giao vận và yêu cầu ứng dụng phải hỗ trợ

17. Trong PGP, khi kết hợp cả tính bảo mật và tính xác thực cho một email, quy trình xử lý nào sau đây là chính xác?

a) Tạo giá trị băm (hash value) của email, mã hóa giá trị băm bằng khóa bí mật (private key) của người gửi, mã hóa email bằng khóa công khai (public key) của người nhận

b) Mã hóa email bằng khóa phiên (session key), mã hóa khóa phiên bằng khóa công khai của người nhận, ký email đã mã hóa bằng khóa bí mật của người gửi

*c) Tạo giá trị băm của email, mã hóa giá trị băm bằng khóa bí mật của người gửi (tạo chữ ký số), nén email và chữ ký, mã hóa kết quả bằng khóa phiên, mã hóa khóa phiên bằng khóa công khai của người nhận

d) Mã hóa email bằng khóa bí mật của người gửi, mã hóa kết quả bằng khóa công khai của người nhận

Chương 3

2.1 Tổng quan về mật mã hoá

1. Theo từ điển Free Online Dictionary of Computing, mật mã học (cryptography) là gì?

a) Một quá trình giải mã thông điệp đã bị mã hóa

b) Một quá trình chuyển đổi dữ liệu có kích thước thay đổi về dữ liệu có kích thước cố định

*c) Việc mã hóa dữ liệu mà chỉ có thể được giải mã bởi một số người chỉ định

d) Một quá trình tạo ra các khóa mã hóa

2. Mã hóa khóa đối xứng (symmetric key cryptography) và mã hóa khóa bất đối xứng (asymmetric key cryptography) là gì?

a) Hai phương pháp giải mã khác nhau

*b) Hai loại mã hóa sử dụng các loại khóa khác nhau

c) Hai phương pháp tạo hàm băm

d) Hai phương pháp thám mã

3. Các thành phần cơ bản của một hệ thống mật mã (cryptosystem) bao gồm:

a) Bản rõ (plaintext), bản mã (ciphertext), không gian khóa (key space)

b) Giải thuật mã hóa, giải thuật giải mã, hàm băm

c) Khóa mã hóa, khóa giải mã, thám mã

*d) Bản rõ, bản mã, giải thuật mã hóa, giải thuật giải mã, khóa mã hóa và khóa giải mã

4. Mối quan hệ giữa mật mã học và toán học là gì?

a) Mật mã học phát triển độc lập với toán học

*b) Mật mã học là con đẻ của toán học và phát triển đi liền với sự phát triển của toán học

c) Toán học là ứng dụng của mật mã học

d) Mật mã học và toán học không có mối liên hệ với nhau

5. Bản rõ (plaintext) trong hệ thống mật mã là gì?

*a) Thông điệp gốc trước khi được mã hóa
b) Thông điệp sau khi đã được mã hóa
c) Khóa dùng để mã hóa thông điệp
d) Giải thuật dùng để mã hóa thông điệp

6. Bản mã (ciphertext) trong hệ thống mật mã là gì?
a) Thông điệp gốc trước khi được mã hóa
*b) Thông điệp sau khi đã được mã hóa
c) Khóa dùng để mã hóa thông điệp
d) Giải thuật dùng để mã hóa thông điệp

7. Khóa mã hóa (encryption key) trong hệ thống mật mã có tác dụng gì?
a) Giải mã bản mã thành bản rõ
*b) Mã hóa bản rõ thành bản mã
c) Tạo ra hàm băm
d) Phân tích và phá vỡ mã

8. Không gian khóa (key space) trong hệ thống mật mã là gì?
a) Kích thước của khóa mã hóa
b) Số lượng bit trong khóa
*c) Tập hợp tất cả các khóa có thể có
d) Vị trí lưu trữ khóa mã hóa

9. Hàm băm (hash function) trong an toàn thông tin là gì?
a) Một giải thuật mã hóa dữ liệu
b) Một giải thuật giải mã dữ liệu
*c) Một ánh xạ chuyển các dữ liệu có kích thước thay đổi về dữ liệu có kích thước cố định
d) Một phương pháp phân phối khóa mã hóa

10. Thám mã (cryptanalysis) là gì?
a) Quá trình tạo ra các khóa mã hóa mới
b) Quá trình mã hóa thông điệp
*c) Quá trình giải mã thông điệp đã bị mã hóa mà không cần có trước thông tin về giải thuật mã hóa và khóa mã
d) Quá trình tạo ra các giải thuật mã hóa mới

11. Mối quan hệ giữa không gian khóa và độ an toàn của hệ thống mật mã là gì?
a) Không gian khóa càng nhỏ, hệ thống mật mã càng an toàn
b) Không gian khóa không ảnh hưởng đến độ an toàn của hệ thống mật mã
*c) Không gian khóa càng lớn, hệ thống mật mã càng an toàn
d) Không gian khóa và độ an toàn của hệ thống mật mã không có mối liên hệ

12. Trong mã hóa khóa đối xứng (symmetric key cryptography), đặc điểm của khóa là gì?

*a) Khóa mã hóa và khóa giải mã giống nhau

b) Khóa mã hóa và khóa giải mã hoàn toàn khác nhau

c) Chỉ sử dụng một khóa duy nhất cho mọi người dùng

d) Không sử dụng khóa trong quá trình mã hóa

13. Trong mã hóa khóa bất đối xứng (asymmetric key cryptography), đặc điểm của khóa là gì?

a) Khóa mã hóa và khóa giải mã giống nhau

*b) Khóa mã hóa và khóa giải mã khác nhau và không thể dễ dàng suy ra từ nhau

c) Chỉ sử dụng một khóa duy nhất cho mọi người dùng

d) Không sử dụng khóa trong quá trình mã hóa

14. Ứng dụng chính của mã hóa khóa đối xứng (symmetric key cryptography) là gì?

a) Chỉ dùng để xác thực người dùng

b) Chỉ dùng để tạo chữ ký số

*c) Mã hóa dữ liệu với tốc độ nhanh và hiệu quả

d) Chỉ dùng để phân phối khóa

15. Ứng dụng chính của mã hóa khóa bất đối xứng (asymmetric key cryptography) là gì?

a) Chỉ dùng để mã hóa dữ liệu với tốc độ cao

*b) Xác thực, chữ ký số và trao đổi khóa an toàn

c) Chỉ dùng để tạo hàm băm

d) Chỉ dùng để thám mã

16. Vai trò của giải thuật mã hóa (encryption algorithm) trong hệ thống mật mã là gì?

a) Tạo ra khóa mã hóa

b) Phân phối khóa mã hóa

*c) Chuyển đổi bản rõ thành bản mã bằng cách sử dụng khóa mật mã

d) Phân tích và phá vỡ mã

17. Tại sao việc tăng kích thước khóa làm tăng độ an toàn của hệ thống mật mã?

a) Vì nó làm tăng tốc độ mã hóa

b) Vì nó làm giảm kích thước của bản mã

*c) Vì nó mở rộng không gian khóa, khiến việc tấn công vét cạn (brute force) trở nên khó khăn hơn

d) Vì nó làm giảm độ phức tạp của giải thuật mã hóa

18. Sự phát triển của mật mã học hiện đại có mối liên hệ như thế nào với toán học?
a) Mật mã học hiện đại phát triển độc lập với toán học
b) Mật mã học hiện đại chỉ dựa vào lý thuyết thông tin
c) Mật mã học hiện đại chỉ dựa vào lý thuyết độ phức tạp tính toán
*d) Mật mã học hiện đại dựa trên các bài toán khó trong toán học như phân tích thừa số số nguyên lớn và logarithm rời rạc

2.2 Mật mã hoá khoá đối xứng
1. Mã hóa khóa đối xứng (symmetric key cryptography) có đặc điểm gì?
a) Sử dụng hai khóa khác nhau để mã hóa và giải mã
*b) Sử dụng cùng một khóa để mã hóa và giải mã
c) Không sử dụng khóa trong quá trình mã hóa và giải mã
d) Chỉ sử dụng khóa công khai (public key)
2. Ưu điểm chính của mã hóa khóa đối xứng (symmetric key cryptography) là gì?
a) Dễ dàng trong việc quản lý khóa
b) Không cần bảo vệ tính bí mật của khóa
*c) Tốc độ mã hóa và giải mã nhanh, hiệu quả với dữ liệu lớn
d) Không cần trao đổi khóa trước khi truyền thông
3. Nhược điểm chính của mã hóa khóa đối xứng (symmetric key cryptography) là gì?
*a) Khó khăn trong việc trao đổi khóa an toàn giữa các bên
b) Tốc độ mã hóa và giải mã chậm
c) Không thể mã hóa dữ liệu lớn
d) Không thể đảm bảo tính toàn vẹn dữ liệu
4. Mã hóa khối (block cipher) là gì?
a) Phương pháp mã hóa từng bit một của bản rõ
*b) Phương pháp mã hóa chia bản rõ thành các khối có kích thước cố định và mã hóa từng khối
c) Phương pháp mã hóa không sử dụng khóa
d) Phương pháp mã hóa chỉ áp dụng cho dữ liệu văn bản
5. Mã hóa dòng (stream cipher) là gì?
*a) Phương pháp mã hóa từng bit hoặc từng byte một của bản rõ
b) Phương pháp mã hóa chia bản rõ thành các khối có kích thước cố định
c) Phương pháp mã hóa không sử dụng khóa

d) Phương pháp mã hóa chỉ áp dụng cho dữ liệu nhị phân

6. Thuật toán DES (Data Encryption Standard) có kích thước khóa (không tính các bit kiểm tra) là bao nhiêu?

a) 128 bit

b) 192 bit

*c) 56 bit

d) 64 bit

7. Thuật toán AES (Advanced Encryption Standard) hỗ trợ kích thước khóa nào?

a) Chỉ 56 bit

b) Chỉ 64 bit

c) Chỉ 128 bit

*d) 128 bit, 192 bit và 256 bit

8. Chế độ ECB (Electronic Codebook) trong mã hóa khối có đặc điểm gì?

a) Mỗi khối được mã hóa phụ thuộc vào khối trước đó

*b) Mỗi khối được mã hóa độc lập với các khối khác

c) Sử dụng một vector khởi tạo (IV) để mã hóa khối đầu tiên

d) Chuyển đổi mã hóa khối thành mã hóa dòng

9. Chế độ CBC (Cipher Block Chaining) trong mã hóa khối có đặc điểm gì?

*a) Mỗi khối bản rõ được XOR với khối bản mã trước đó trước khi mã hóa

b) Mỗi khối được mã hóa độc lập với các khối khác

c) Tạo ra một dòng khóa để XOR với bản rõ

d) Chỉ mã hóa sự khác biệt giữa các khối liên tiếp

10. Chế độ CTR (Counter) trong mã hóa khối có đặc điểm gì?

a) Mỗi khối bản rõ được XOR với khối bản mã trước đó trước khi mã hóa

b) Mỗi khối được mã hóa độc lập với các khối khác

*c) Mã hóa một bộ đếm và XOR kết quả với bản rõ để tạo bản mã

d) Chỉ mã hóa sự khác biệt giữa các khối liên tiếp

11. Tại sao chế độ ECB (Electronic Codebook) không được khuyến nghị sử dụng cho dữ liệu lớn?

a) Vì tốc độ mã hóa quá chậm

b) Vì tiêu tốn quá nhiều tài nguyên hệ thống

*c) Vì các khối bản rõ giống nhau sẽ tạo ra các khối bản mã giống nhau, làm lộ mẫu dữ liệu

d) Vì không thể giải mã chính xác

12. Thuật toán 3DES (Triple DES) là gì?

a) Một thuật toán mã hóa hoàn toàn mới, không liên quan đến DES

*b) Một biến thể của DES, áp dụng thuật toán DES ba lần cho mỗi khối dữ liệu

c) Một thuật toán mã hóa sử dụng ba khóa khác nhau đồng thời

d) Một thuật toán mã hóa có tốc độ gấp ba lần DES

13. Trong AES (Advanced Encryption Standard), số vòng lặp (rounds) phụ thuộc vào yếu tố nào?

a) Kích thước của bản rõ

*b) Kích thước của khóa

c) Chế độ mã hóa được sử dụng

d) Loại dữ liệu được mã hóa

14. Chế độ OFB (Output Feedback) trong mã hóa khối có đặc điểm gì?

a) Mỗi khối bản rõ được XOR với khối bản mã trước đó trước khi mã hóa

b) Mỗi khối được mã hóa độc lập với các khối khác

*c) Tạo ra một dòng khóa bằng cách mã hóa liên tiếp đầu ra của bước trước đó, sau đó XOR với bản rõ

d) Chỉ mã hóa sự khác biệt giữa các khối liên tiếp

15. Tại sao AES (Advanced Encryption Standard) được chọn để thay thế DES (Data Encryption Standard)?

a) Vì AES dễ triển khai hơn

b) Vì AES sử dụng ít tài nguyên hệ thống hơn

*c) Vì DES có kích thước khóa nhỏ (56 bit) dễ bị tấn công vét cạn (brute force)

d) Vì DES không thể mã hóa dữ liệu nhị phân

16. Trong mã hóa khối, padding là gì?

*a) Kỹ thuật thêm dữ liệu vào khối cuối cùng để đạt đủ kích thước khối yêu cầu

b) Kỹ thuật giảm kích thước của khối để tăng tốc độ mã hóa

c) Kỹ thuật tạo ra khóa mã hóa từ mật khẩu người dùng

d) Kỹ thuật nén dữ liệu trước khi mã hóa

17. Kích thước khối (block size) của thuật toán AES là bao nhiêu?

a) 64 bit

*b) 128 bit

c) 192 bit

d) 256 bit

18. Ưu điểm của mã hóa dòng (stream cipher) so với mã hóa khối (block cipher) là gì?

a) Luôn an toàn hơn trong mọi trường hợp

b) Không cần sử dụng khóa mã hóa
*c) Thích hợp cho dữ liệu thời gian thực và có độ trễ thấp
d) Không thể bị phân tích mật mã học

20. Thuật toán RC4 là một ví dụ của loại mã hóa nào?
a) Mã hóa khối (block cipher)
*b) Mã hóa dòng (stream cipher)
c) Mã hóa khóa bất đối xứng (asymmetric key cryptography)
d) Hàm băm mật mã (cryptographic hash function)

2.3 Mật mã hoá khoá bất đối xứng
1. Mã hóa khóa bất đối xứng (asymmetric key cryptography) có đặc điểm gì?
a) Sử dụng cùng một khóa để mã hóa và giải mã
*b) Sử dụng một cặp khóa: khóa công khai (public key) và khóa bí mật (private key)
c) Không sử dụng khóa trong quá trình mã hóa và giải mã
d) Chỉ sử dụng một khóa duy nhất cho mọi người dùng
2. Trong mã hóa khóa bất đối xứng (asymmetric key cryptography), mối quan hệ giữa khóa công khai và khóa bí mật là gì?
a) Hai khóa giống hệt nhau
b) Hai khóa hoàn toàn độc lập, không liên quan đến nhau
*c) Hai khóa có liên quan toán học với nhau, nhưng không thể dễ dàng tính ra khóa bí mật từ khóa công khai
d) Khóa công khai luôn được tạo ra từ khóa bí mật bằng cách đảo ngược các bit
3. Ưu điểm chính của mã hóa khóa bất đối xứng (asymmetric key cryptography) là gì?
a) Tốc độ mã hóa và giải mã nhanh hơn mã hóa khóa đối xứng
*b) Giải quyết vấn đề trao đổi khóa an toàn và cung cấp cơ chế xác thực, chữ ký số
c) Sử dụng ít tài nguyên hệ thống hơn
d) Không cần bảo vệ tính bí mật của bất kỳ khóa nào
4. Nhược điểm chính của mã hóa khóa bất đối xứng (asymmetric key cryptography) là gì?
*a) Tốc độ mã hóa và giải mã chậm hơn nhiều so với mã hóa khóa đối xứng
b) Không thể mã hóa dữ liệu lớn
c) Không thể đảm bảo tính toàn vẹn dữ liệu

d) Khó khăn trong việc trao đổi khóa

5. Thuật toán RSA dựa trên bài toán khó nào trong toán học?

a) Logarithm rời rạc (discrete logarithm)

*b) Phân tích thừa số số nguyên lớn (factoring large integers)

c) Đường cong elliptic (elliptic curve)

d) Bài toán ba-lô (knapsack problem)

6. Trong mã hóa RSA, để đảm bảo tính bảo mật, thông điệp được mã hóa bằng khóa nào và giải mã bằng khóa nào?

a) Mã hóa bằng khóa bí mật, giải mã bằng khóa công khai

*b) Mã hóa bằng khóa công khai của người nhận, giải mã bằng khóa bí mật của người nhận

c) Mã hóa bằng khóa công khai của người gửi, giải mã bằng khóa bí mật của người gửi

d) Mã hóa và giải mã đều sử dụng khóa công khai

7. Trong mã hóa khóa bất đối xứng (asymmetric key cryptography), khóa nào cần được bảo vệ và giữ bí mật?

a) Cả khóa công khai và khóa bí mật

b) Không cần bảo vệ bất kỳ khóa nào

*c) Chỉ khóa bí mật (private key)

d) Chỉ khóa công khai (public key)

8. Chữ ký số (digital signature) được sử dụng để đảm bảo tính chất nào của thông điệp?

a) Chỉ tính bảo mật (confidentiality)

b) Chỉ tính toàn vẹn (integrity)

*c) Tính xác thực nguồn gốc (authentication) và tính không thể chối bỏ (non-repudiation)

d) Chỉ tính sẵn sàng (availability)

9. Hạ tầng khóa công khai (PKI - Public Key Infrastructure) là gì?

a) Một thuật toán mã hóa mới

b) Một phương pháp tạo khóa ngẫu nhiên

*c) Một hệ thống quản lý khóa công khai, bao gồm các thành phần như CA, chứng thư số, và các chính sách

d) Một phương pháp phân phối khóa đối xứng

10. Cơ quan cấp chứng thư số (CA - Certificate Authority) có vai trò gì trong hạ tầng khóa công khai (PKI)?

a) Tạo ra khóa bí mật cho người dùng

b) Mã hóa và giải mã thông điệp thay cho người dùng

*c) Xác thực danh tính người dùng và cấp chứng thư số xác nhận khóa công khai của họ

d) Lưu trữ tất cả các khóa bí mật của người dùng

11. Chứng thư số (digital certificate) chứa những thông tin gì?

a) Khóa bí mật của người dùng

b) Tất cả các thông điệp đã được mã hóa của người dùng

*c) Khóa công khai của người dùng, thông tin định danh và chữ ký số của CA

d) Mật khẩu đăng nhập của người dùng

12. Tại sao mã hóa khóa bất đối xứng (asymmetric key cryptography) thường không được sử dụng để mã hóa trực tiếp các thông điệp lớn?

a) Vì không đủ an toàn cho dữ liệu lớn

b) Vì không thể mã hóa dữ liệu lớn hơn kích thước khóa

*c) Vì tốc độ mã hóa và giải mã chậm, không hiệu quả với dữ liệu lớn

d) Vì dễ bị tấn công hơn với dữ liệu lớn

13. Kích thước khóa RSA thông thường được khuyến nghị sử dụng hiện nay là bao nhiêu để đảm bảo an toàn?

a) 512 bit

b) 768 bit

*c) 2048 bit hoặc lớn hơn

d) 128 bit

14. Trong mã hóa khóa bất đối xứng (asymmetric key cryptography), phương pháp nào thường được sử dụng để mã hóa hiệu quả các thông điệp lớn?

a) Tăng kích thước khóa bất đối xứng

*b) Kết hợp mã hóa đối xứng và bất đối xứng: mã hóa thông điệp bằng khóa đối xứng, sau đó mã hóa khóa đối xứng bằng khóa công khai

c) Chia thông điệp thành nhiều phần nhỏ và mã hóa từng phần riêng biệt

d) Sử dụng nhiều cặp khóa bất đối xứng khác nhau

15. Trong RSA, cặp số nguyên tố lớn được dùng để tạo khóa được ký hiệu là gì?

a) e và d

*b) p và q

c) n và φ(n)

d) a và b

16. Trong RSA, giá trị n trong khóa công khai và khóa bí mật được tính như thế nào?

a) n = p + q

b) n = p − q

*c) n = p × q

d) n = p / q

17. Khóa công khai trong RSA bao gồm những thành phần nào?

a) (p, q)

b) (n, d)

*c) (n, e)

d) (q, d)

18. Điều kiện nào sau đây là đúng khi chọn giá trị e trong RSA?

a) e phải là số nguyên tố nhỏ hơn p

b) e chia hết cho φ(n)

*c) e và φ(n) phải nguyên tố cùng nhau

d) e phải lớn hơn n

19. Giá trị d trong khóa bí mật RSA được tính như thế nào?

a) d = e × φ(n)

*b) d là nghịch đảo modular của e theo modulo φ(n)

c) d = n − e

d) d = p × q − e

20. Trong RSA, phép mã hóa được thực hiện như thế nào để đảm bảo tính bảo mật cho bản rõ m?

a) C = m × e mod n

*b) C = m^e mod n

c) C = e^m mod n

d) C = (m + e) mod n

21. Cho hai số nguyên tố p = 17 và q =11, giá trị n trong RSA bằng bao nhiêu?

a) 187

*b) 187

c) 28

d) 204

2.4 Quản lý và phân phối khoá

1. Trong hệ thống mật mã (cryptosystem), khóa phiên (session key) có đặc điểm gì?

a) Được sử dụng lâu dài và ít khi thay đổi

*b) Là khóa tạm thời, được sử dụng trong một phiên giao dịch và bị xóa bỏ sau khi sử dụng

c) Được sử dụng để mã hóa khóa chủ

d) Được phân phối thủ công giữa các bên tham gia

2. Trong hệ thống mật mã (cryptosystem), khóa chủ (master key) có đặc điểm gì?

*a) Được sử dụng lâu dài và dùng để mã hóa khóa phiên

b) Là khóa tạm thời, được sử dụng trong một phiên giao dịch

c) Được thay đổi tự động sau mỗi phiên giao dịch

d) Chỉ được sử dụng trong mã hóa khóa bất đối xứng (asymmetric key cryptography)

3. Trung tâm phân phối khóa (KDC - Key Distribution Center) có vai trò gì trong hệ thống mật mã (cryptosystem)?

a) Tạo ra các khóa công khai cho mọi người dùng

b) Lưu trữ tất cả các bản mã (ciphertext) đã được mã hóa

*c) Là bên thứ ba đáng tin cậy, giúp phân phối khóa phiên giữa các bên tham gia

d) Giải mã các thông điệp khi người dùng quên khóa

4. Tại sao cần thay đổi khóa phiên (session key) thường xuyên?

a) Để tiết kiệm tài nguyên hệ thống

b) Để tăng tốc độ mã hóa và giải mã

*c) Để tránh các tấn công thám mã (cryptanalysis) do sử dụng khóa quá lâu

d) Để giảm kích thước của khóa

5. Trong phân phối khóa đối xứng (symmetric key distribution), phương pháp phân phối không tập trung có nghĩa là gì?

a) Tất cả các khóa được lưu trữ tại một máy chủ trung tâm

*b) Mỗi người dùng phải trao đổi khóa chủ một cách thủ công với tất cả người dùng khác

c) Không cần sử dụng khóa để mã hóa thông tin

d) Chỉ có một khóa duy nhất được sử dụng trong toàn hệ thống

6. Giá trị Nonce trong phân phối khóa có đặc điểm gì?

a) Là một khóa bí mật được sử dụng nhiều lần

b) Là một giải thuật mã hóa (encryption algorithm) đặc biệt

*c) Là một số được sử dụng một lần, thường là số ngẫu nhiên hoặc số đếm

d) Là một loại mã hóa không sử dụng khóa

7. Chứng thư số khóa công khai (digital certificate) bao gồm những thông tin gì?

a) Chỉ có khóa bí mật (private key) của người dùng
b) Chỉ có danh tính của cơ quan cấp chứng thư
*c) Khóa công khai (public key), danh tính của chủ sở hữu và chữ ký số (digital signature) của cơ quan cấp chứng thư
d) Toàn bộ lịch sử giao dịch của người dùng

8. Ưu điểm chính của phương pháp thông báo công khai trong phân phối khóa công khai (public key distribution) là gì?
*a) Đơn giản và thuận tiện
b) Bảo mật cao nhất
c) Không thể bị giả mạo
d) Không cần bên thứ ba đáng tin cậy

9. Trong phân phối khóa tập trung qua KDC, quy trình cơ bản diễn ra như thế nào?
a) Người dùng tự tạo khóa phiên và gửi cho nhau
*b) Người dùng A gửi yêu cầu đến KDC, KDC tạo khóa phiên (session key) và gửi cho cả A và B
c) KDC tự động gửi khóa phiên cho tất cả người dùng định kỳ
d) Người dùng A và B trao đổi khóa công khai (public key) với nhau qua KDC

10. Thời gian sống của khóa phiên (session key) trong giao thức hướng kết nối (TCP) thường được xác định như thế nào?
a) Cố định là 24 giờ
b) Cố định là 1 giờ
*c) Mỗi kết nối yêu cầu một khóa phiên mới
d) Thay đổi sau một số lượng byte cố định

11. Trong phương pháp thư mục khóa công khai (public key directory), làm thế nào để đảm bảo tính xác thực của khóa?
a) Không cần xác thực vì khóa công khai luôn an toàn
b) Mỗi người dùng tự xác thực khóa của mình
*c) Người dùng đăng ký khóa với bên thẩm quyền quản lý danh mục thông qua kênh được chứng thực an toàn
d) Sử dụng mã hóa khóa đối xứng (symmetric key cryptography) để bảo vệ khóa công khai

12. Tại sao việc sử dụng mã hóa khóa bất đối xứng (asymmetric key cryptography) để phân phối khóa đối xứng (symmetric key) lại hiệu quả?
a) Vì mã hóa khóa bất đối xứng luôn nhanh hơn mã hóa khóa đối xứng
b) Vì không cần sử dụng khóa phiên

*c) Vì kết hợp được ưu điểm của cả hai: tốc độ của mã hóa khóa đối xứng và khả năng phân phối khóa an toàn của mã hóa khóa bất đối xứng

d) Vì giảm được kích thước của khóa

13. Trong phân phối khóa công khai qua trung tâm thẩm quyền, làm thế nào để A xác thực rằng thông điệp nhận được thực sự đến từ B?

a) A tin tưởng trung tâm thẩm quyền mà không cần xác thực

b) A kiểm tra chữ ký số (digital signature) của trung tâm thẩm quyền

*c) A gửi một nonce (N1) cho B và B phải trả lại đúng nonce đó

d) A và B phải gặp nhau trực tiếp để xác thực

14. Vấn đề chính trong phân phối khóa công khai (public key distribution) là gì?

a) Khóa công khai quá dài nên khó phân phối

b) Khóa công khai dễ bị đánh cắp

*c) Làm sao đảm bảo khóa công khai thực sự thuộc về người mà nó tuyên bố thuộc về

d) Khóa công khai không thể được sử dụng để mã hóa dữ liệu

15. Trong hệ thống chứng thư số khóa công khai, vai trò của cơ quan cấp chứng thư (CA - Certificate Authority) là gì?

a) Tạo ra khóa bí mật (private key) cho người dùng

b) Lưu trữ tất cả các khóa bí mật

*c) Xác thực danh tính người dùng và ký số chứng thư chứa khóa công khai (public key) của họ

d) Mã hóa và giải mã thông điệp thay cho người dùng

16. Khi sử dụng phương pháp phân phối khóa tập trung qua KDC, vấn đề nghẽn cổ chai (bottleneck) có thể xảy ra như thế nào?

a) KDC tạo ra quá nhiều khóa phiên không cần thiết

b) Khóa phiên quá dài làm chậm quá trình truyền

*c) Tất cả các yêu cầu phân phối khóa đều phải thông qua KDC, có thể gây quá tải khi số lượng người dùng lớn

d) Khóa chủ quá ngắn dễ bị tấn công vét cạn (brute force attack)

17. Trong quy trình phân phối khóa qua KDC, giả sử A muốn thiết lập kết nối an toàn với B, khi KDC nhận được yêu cầu từ A, KDC sẽ trả về những thông tin gì?

a) Chỉ khóa phiên Ks được mã hóa bằng khóa chủ của A

b) Khóa phiên Ks được mã hóa bằng khóa chủ của B

*c) Khóa phiên Ks được mã hóa bằng khóa chủ của A và một bản tin chứa khóa phiên Ks và định danh của A được mã hóa bằng khóa chủ của B

d) Khóa phiên Ks ở dạng bản rõ (plaintext) và định danh của A và B

18. Phân tích tại sao phương pháp thông báo công khai trong phân phối khóa công khai dễ bị tấn công Man-in-the-Middle:

a) Vì khóa công khai quá ngắn nên dễ bị phá giải

b) Vì người dùng thường quên khóa công khai của mình

*c) Vì kẻ tấn công có thể chặn thông báo gốc và thay thế bằng khóa công khai của chính họ, làm cho người nhận tin rằng đó là khóa công khai của người gửi thực sự

d) Vì khóa công khai không thể được sử dụng để mã hóa dữ liệu lớn

2.5 Một số giao thức đảm bảo an toàn thông tin dựa trên mật mã hoá

1. IPsec (Internet Protocol Security) hoạt động ở lớp nào trong mô hình TCP/IP?

a) Lớp ứng dụng (Application Layer)

b) Lớp giao vận (Transport Layer)

*c) Lớp mạng (Network Layer)

d) Lớp liên kết dữ liệu (Data Link Layer)

2. SSL/TLS (Secure Socket Layer/Transport Layer Security) hoạt động ở lớp nào trong mô hình TCP/IP?

a) Lớp ứng dụng (Application Layer)

*b) Lớp giao vận (Transport Layer)

c) Lớp mạng (Network Layer)

d) Lớp liên kết dữ liệu (Data Link Layer)

3. PGP (Pretty Good Privacy) được sử dụng chủ yếu để bảo vệ loại dữ liệu nào?

a) Dữ liệu truyền qua giao thức HTTP

*b) Thư điện tử (Email)

c) Dữ liệu truyền qua mạng riêng ảo (VPN)

d) Dữ liệu truyền qua giao thức FTP

4. Trong IPsec, ESP (Encapsulation Security Payload) cung cấp những dịch vụ an toàn nào?

a) Chỉ tính xác thực

b) Chỉ tính bảo mật

*c) Cả tính bảo mật và tính xác thực

d) Chỉ tính toàn vẹn dữ liệu

5. Trong IPsec, AH (Authentication Header) cung cấp những dịch vụ an toàn nào?

*a) Tính xác thực và tính toàn vẹn dữ liệu

b) Tính bảo mật và tính xác thực

c) Chỉ tính bảo mật
d) Chỉ tính không từ chối

6. Thuật toán mã hóa nào thường được sử dụng trong ESP của IPsec?
a) RSA và DSA
b) MD5 và SHA-1
*c) DES, 3DES hoặc AES
d) Diffie-Hellman

7. Trong IPsec, khi sử dụng kết hợp cả AH và ESP trong chế độ vận chuyển (Transport mode), thứ tự xử lý gói tin nào là chính xác?
a) Áp dụng AH trước, sau đó áp dụng ESP
*b) Áp dụng ESP trước, sau đó áp dụng AH
c) Áp dụng AH và ESP đồng thời
d) Không thể kết hợp AH và ESP trong chế độ vận chuyển

8. PGP sử dụng kết hợp những kỹ thuật mật mã học (cryptography) nào?
a) Chỉ mã hóa khóa đối xứng (symmetric key cryptography)
b) Chỉ mã hóa khóa bất đối xứng (asymmetric key cryptography)
*c) Mã hóa khóa đối xứng, mã hóa khóa bất đối xứng, hàm băm (hash function) và chữ ký số (digital signature)
d) Chỉ hàm băm và chữ ký số

9. Trong IPsec, chế độ vận chuyển (Transport mode) có đặc điểm gì?
a) Các gateway thực hiện quá trình xử lý mật mã
*b) Các máy chủ nguồn và đích trực tiếp thực hiện tất cả các thao tác mã hóa
c) Chỉ bảo vệ phần payload của gói tin
d) Chỉ sử dụng giao thức AH, không sử dụng ESP

10. Trong IPsec, chế độ đường hầm (Tunnel mode) có đặc điểm gì?
a) Các máy chủ nguồn và đích trực tiếp thực hiện tất cả các thao tác mã hóa
*b) Các gateway thực hiện quá trình xử lý mật mã, không phải các máy chủ nguồn và đích
c) Chỉ bảo vệ phần header của gói tin
d) Chỉ sử dụng giao thức ESP, không sử dụng AH

11. Trong SSL/TLS, Record Protocol có chức năng gì?
a) Thiết lập phiên làm việc và trao đổi khóa
b) Thông báo lỗi và cảnh báo
*c) Phân mảnh, nén, mã hóa và xác thực dữ liệu
d) Cập nhật trạng thái mật mã của kết nối

12. Trong SSL/TLS, Handshake Protocol có chức năng gì?
*a) Xác thực các bên tham gia và thỏa thuận thuật toán, khóa mã hóa

b) Phân mảnh và nén dữ liệu
c) Truyền đạt cảnh báo cho đối tượng kết nối
d) Mã hóa và giải mã dữ liệu

13. Trong PGP, để đảm bảo tính bí mật của email, quy trình mã hóa diễn ra như thế nào?
a) Mã hóa email bằng khóa bí mật (private key) của người gửi
b) Mã hóa email bằng khóa bí mật của người nhận
*c) Tạo khóa phiên (session key) ngẫu nhiên, mã hóa email bằng khóa phiên, sau đó mã hóa khóa phiên bằng khóa công khai (public key) của người nhận
d) Mã hóa email bằng khóa công khai của người gửi

14. Trong PGP, để đảm bảo tính xác thực của email, quy trình ký số diễn ra như thế nào?
a) Ký email bằng khóa công khai (public key) của người gửi
*b) Tạo giá trị băm (hash value) của email, sau đó mã hóa giá trị băm bằng khóa bí mật (private key) của người gửi
c) Ký email bằng khóa bí mật của người nhận
d) Tạo giá trị băm của email, sau đó mã hóa giá trị băm bằng khóa công khai của người nhận

15. Trong SSL/TLS, MAC (Message Authentication Code) được sử dụng để làm gì?
a) Mã hóa dữ liệu
*b) Đảm bảo tính toàn vẹn của dữ liệu
c) Xác thực danh tính của máy chủ
d) Trao đổi khóa bí mật

16. So sánh IPsec và SSL/TLS, nhận xét nào sau đây là chính xác?
a) IPsec và SSL/TLS đều hoạt động ở lớp giao vận và cung cấp các dịch vụ an toàn giống nhau
b) IPsec cung cấp tính bảo mật tốt hơn SSL/TLS trong mọi trường hợp
c) SSL/TLS dễ triển khai hơn IPsec nhưng không hỗ trợ xác thực hai chiều
*d) IPsec hoạt động ở lớp mạng nên trong suốt với ứng dụng, trong khi SSL/TLS hoạt động ở lớp giao vận và yêu cầu ứng dụng phải hỗ trợ

17. Trong PGP, khi kết hợp cả tính bảo mật và tính xác thực cho một email, quy trình xử lý nào sau đây là chính xác?
a) Tạo giá trị băm (hash value) của email, mã hóa giá trị băm bằng khóa bí mật (private key) của người gửi, mã hóa email bằng khóa công khai (public key) của người nhận

b) Mã hóa email bằng khóa phiên (session key), mã hóa khóa phiên bằng khóa công khai của người nhận, ký email đã mã hóa bằng khóa bí mật của người gửi

*c) Tạo giá trị băm của email, mã hóa giá trị băm bằng khóa bí mật của người gửi (tạo chữ ký số), nén email và chữ ký, mã hóa kết quả bằng khóa phiên, mã hóa khóa phiên bằng khóa công khai của người nhận

d) Mã hóa email bằng khóa bí mật của người gửi, mã hóa kết quả bằng khóa công khai của người nhận