MẬT MÃ & AN NINH MẠNG

ĐỀ THI HK-202

Câu 1: Thông tin nào sau đây không tồn tại trong các chứng chỉ X.509:

A. Tên của tổ chức CA cấp chứng chỉ

B. Chữ ký số của tổ chức CA cấp chứng chỉ

C. Chữ ký số của thực thể được cấp chứng chỉ

D. Khoá công khai của thực thể được cấp chứng chỉ

Câu 2: Trong ngôn ngữ lập trình Java, lớp Signature thuộc gói (Package) nào sau đây?

A. javax.crypto

B. javax.crypto.spec

C. java.security

D. java.security.cert

Câu 3: Đối với hộ mã hóa khóa công khai, khóa nào được sử dụng để xác minh chứ ký số trong một thông điệp:

A. Khóa công khai của người nhận

B. Khóa riêng của người gửi

C. Khóa công khai của người gửi

D. Khóa riêng của người nhận

Câu 4: Thuật ngữ nào sau đây không phải là một loại bức tường lửa (firewall)?

A. Proxy server gateway

B. Cicrui-level gateway

C. Packet filter

D. Application-lever gateway

Câu 5: Kỹ thuật nào sau đây trong chuẩn WPA có tác dụng thay thế cho CRC (Cyclie Redundancy Check) trong WEP?

A. TKIP

B. RC4

C. MIC

D. PSK

Câu 6: Chọn phát biểu đúng nhất về chữ ký số?

A. Hàm băm được sử dụng trong chữ ký số luôn luôn cho ra kết quả có độ dài ngắn hơn thông điệp gốc

B. Hàm băm được sử dụng trong chữ ký số phải được hiện thực trên phần cứng

C. Tất cả các câu trả lời đều sai

X D. Không tồn tại 2 thông điệp khác nhau bất kỳ có cùng giá trị chữ ký số

Câu 7: Phương pháp sử dụng dấu vân tay để xác thực người dùng dựa trên yếu tố nào sau đây?

A. Những gì bạn biết

B. Những gì bạn có

C. Những gì là chính bạn

D. Cả B và C đều đúng

Câu 8: Các cổng (port) mặc định của giao thức http và https có giá trị lần lượt là?

A. 8080, 80

B. 80, 8080

C. 80, 443

D. 443, 80

Câu 9: Đầu là ngành học nghiên cứu các phương thức để thu được ý nghĩa của thông tin đã được mã hóa mà không cần sử dụng khoá?

A. Cryptography

B. Tất cả đều đúng

C. Steganography

D. Cryptanalysis

Câu 10: Hình thức tấn công nào sau đây là tấn công thụ động?

A. Giả mạo.

B. Từ chối dịch vụ

C. Phân tích lưu lượng

D. Phát lại

Câu 11: **Nếu bạn thực hiện một bộ chính sách và thủ tục xác định thông tin công ty là bí mật và sau đó đào tạo nhân viên về các quy trình liên quan, bạn có thể ngăn chặn tấn công nào?**

A. DoS | B. Social engineering | C. Smurf | D. Man-in-the-middle

Câu 12: **Chọn các phát biểu đúng trong các phát biểu sau đây về chế độ mã hoá?**

I. Trong chế độ mã hoá CBC, khối bản rõ được XOR với khối bản mã ở bước trước đó trước khi mã hoá

II. Chế độ mã hoá CTR không yêu cầu sử dụng vector khởi tạo (Initialization Vector)

III. Block cuối cùng trong chế độ mã hoá CBC sử dụng vector khởi tạo

IV. Chế độ mã hoá OFB có thể được sử dụng cho mà hoá dòng

A. (III) | B. (II) và (IV) | C. (I), (II) và (IV) | D. (I), (III) và (V)

Câu 14: **Trong chương trình web server Apache, các tập tin cấu hình có phần đuôi mở rộng là:**

A. xml | B. json | C. conf | D. configuration

Câu 15: **Chọn phát biểu đúng nhất về công cụ Cryptool?**

A. Là công cụ hỗ trợ tấn công mạng

B. Là công cụ phục vụ cho việc học tập và nghiên cứu với nhiều thuật toán mã hóa phổ biến

C. Là công cụ có chức năng quét mã đọc (malware)

D. Tất cả các câu trả lời đều đúng

Câu 16: **Sử dụng công cụ fail2ban với hệ điều hành CentOS 7, để xem danh sách các IP đã bị cắm cho dịch vụ SSH, ta có thể dùng lệnh nào sau đây?**

A. fail2ban-client status ssh

B. fail2ban-client status sshd

C. fail2ban-client status

D. Câu B và C đều đúng.

Câu 17: **Tổ chức CA (Certification Authority) có trách nhiệm xác thực thông tin nào sau đây?**

A. Khoá riêng của người đã đăng ký

B. Khoá công khai của người đã đăng ký

C. Hàm băm được sử dụng

D. Khoá sử dụng trong giải thuật DES

Câu 18: **Để cài đặt giao thức HTTPS cho web server Apache, chúng ta cần kích hoạt module nào sau đây:**

A. mod_proxy | B. Tất cả | C. mod tis | D. mod_ssl

Câu 19: **Giả sử mỗi người trong nhóm gồm N người muốn giao tiếp bí mật với (N-1) người còn lại sử dụng hệ thống sử dụng mà hoá đối xứng. Giao tiếp giữa 2 người bất kỳ không bị giải mà bởi những người còn lại trong nhóm. Hãy cho biết số lượng khoá cần thiết cho hệ thống trên là bao nhiêu?**

A. (N-1)2 | B. 2N | C. N(N-1) | D. N(N-1)/2

Câu 20: **Biện pháp nào sau đây là cần thiết để ngăn chặn lây nhiễm virus trên máy tính?**

A. Dọn rác máy tính

B. Cài đặt chương trình phát hiện xâm nhập

C. Cài đặt chương trình bức tường lửa

D. Cài đặt các bản và lỗi cho các app và hệ điều hành

Câu 21: Chọn phát biểu sai về hệ thống mạng riêng ảo (VPN)

A. VPN Server phải được cài đặt trên bức tường lửa hoặc bộ định tuyến biên

B. VPN sử dụng một số giao thức riêng biệt để tạo ra các đường hầm VPN

C. Các thuật toán sử dụng trong VPN phải là các thuật toán nổi tiếng và mã hóa mạnh

D. Các hệ thống VPN bao gồm 2 loại là site-to-site VPN và User VPN

Câu 22: Giao thức nào sau đây là giao thức không an toàn?

A. imaps B. smtp C. https D. sftp

Câu 23: Phần mềm nào sau đây có thể giúp thăm dò mạng máy tính bằng cách quét danh sách địa chỉ IP và Port?

A. Ettercap B. Snort C. Angry IP Scanner D. Cain and Abel

Câu 24: Hãy cho biết kết quả của ($(7^{2020} \bmod 13)$):

A. 9 B. 8 C. 1 D. Tất cả đều sai

Câu 25: Cho biết phát biểu sai về dual signature trong các phát biểu sau:

A. Đối với giao dịch điện từ an toàn, dual signature được dùng để ký trên hai thi liệu gồm thông tin thanh toán (payment information – PO) và thông tin đặt hàng (order information - OI).

B. Đối với giao dịch điện tử an toàn, cual signature được dùng nhằm để ngân hàng không thể biết được hành code của tài liệu đặt hàng.

C. Mục đích của dual signature là để liên kết bài thông điệp dành cho tui nơi nhận khác nhau.

D. Dual signature được dùng để ký trên hai tài liệu nói với nhau và hồi tài liệu này có hash code riêng.

Câu 26: Các nguyên tắc cốt lõi của an toàn thông tin bao gồm?

A. Toàn vẹn, bí mật, sẵn sàng B. Xác thực, sẵn sàng, cấp quyền

C. Xác thực, bí mật, chống thoái thác D. Toàn vẹn, bí mật, xác thực

Câu 27: Có bao nhiêu khoá được sử dụng trong giải thuật Triple DES

A. 2 khóa hoặc 3 khoá B. 3 khoá C. 3 khoá hoặc 4 khoá D. 2 khoá

Câu 28: Chọn phát biểu đúng về các phương pháp xác thực?

A. Phương pháp xác thực dựa trên mặt khẩu an toàn trước tấn công xen giữa

B. Trong giao thức xác thực dùng mã hoá khoá công khai, số Nonce được mã hoá sử dụng khóa công khai của bên nhận

C. Giao thức xác thực đúng mã hoá đối xứng chỉ hỗ trợ xác thực 1 chiều

D. Trong giao thức xác thực dựa trên mặt khẩu, để chống tấn công lặp lại ta cần mã hoá mật khẩu trước khi gửi

Câu 29: Trong bộ mã hóa khóa công khai, giả sử A mã hoá thông điệp sử dụng khoá riêng của A và gửi thông đã được mã hóa trên cho B, hãy chọn phát biểu đúng nhất?

A. Nếu B biết thông điệp đến từ A thì B có thể giải mã thông điệp sử dụng khoá công khai của A

B. B không thể giải mã thông điệp ngay cả khi B biết thông điệp đến từ A và khóa công khai của A

C. Không ai có thể giải mã được thông điệp trên vì không biết khoá riêng của A

D. Câu B và C đúng

Câu 30: Loại ứng dụng nào sau đây có thể dùng để che giấu địa chỉ IP của người dùng khi duyệt web?

A. Bức tường lửa (Firewall)

B. Mạng riêng ảo (VPN)

C. Chương trình diệt virus (Antivirus)

D. Chế độ ẩn danh (Incognito mode) của trình duyệt

Câu 31: Trong giải thuật DES, cho bằng thay thế S-Box như bên dưới:

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Hãy cho biết kết quả đầu ra tương ứng với khối chuỗi bắt đầu vào: 100100 khi thực hiện chuyển đổi bằng S-Box này?

A. 1001 B. 0111 C. 1000 D. 0011

Câu 32: Trong ngôn ngữ lập trình Java, lớp KeyGenerator được dùng để làm gì?

A. Tạo một cặp khoa gồm khoá công khai và khoá riêng với một hệ mà khoá công khai đã quy định

B. Tạo số nguyên tố ngẫu nhiên lớn

C. Phân phối khoá giữa 2 thực thế giao tiếp

D. Tạo một khoá bí mật với một hệ mã đối xứng đã quy định

Câu 33: Điều gì là phản ứng thích hợp cho một sự kiện bảo mật trên mạng?

A. Thực hiện các thủ tục an ninh

B. Ngắt kết nối mạng

C. Thực hiện chính sách an ninh

D. Cả đặt bộ định tuyến mới

Câu 34: Giải thuật băm SHA-1 sinh ra giá trị băm có độ dài bao nhiêu?

A. 320 bits B. 160 bits C. 256 bits D. 128 bits

Câu 35: Cho biết cấu hình bức tường lửa nào sau đây có khả năng ngăn chặn các vi phạm an ninh mạng khi bộ lọc gọi trên bộ định tuyến kết nối với Internet bị thương tổn hay đã thỏi hiệp.

A. single-homed bastion host

B. dual-homed bastion host

C. screened subnet

D. Câu B và C đều đúng

Câu 36: Phần mềm nào dưới đây là phần mềm mã nguồn mở được thực hiện để triển khai giao thức SSL/TLS trong thực tế:

A. Cryptool B. OpenSSL C. UFW D. Câu A và B đúng

Câu 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 và chữ ký số trên thông điệp.

B. Thông điệp

C. Tóm tắt thông điệp

D. Chữ ký số trên thông điệp.

Câu 38: **Giả sử một khẩu được giới hạn sử dụng là 95 ký tự ASCII có thể in được và mật khẩu có chiều dài là 10 ký tự. Giả sử một chương trình bẻ gãy mật khẩu với tỷ lệ mã hóa là 6400000 mã hóa/giây. Hãy cho biết cần bao lâu để kiểm tra tất cả các mật khẩu có thể có? (Cho biết: $95^{10} >> 6 \times 10^{10}$ và lấy kết quả gần đúng nhất).**

A. 100 ngàn năm. B. 400 ngàn năm. C. 300 ngàn năm. D. 200 ngàn năm.

Câu 39: **Chọn phát biểu SAI trong các phát biểu dưới đây?**

A. Khi có sự thay đổi về mặt công nghệ thì các chính sách an toàn thông tin của tổ chức cần phải được xem xét lại

B. Trong an toàn thông tin, việc hiện thực các giải pháp công nghệ đơn lẻ là không thể cung cấp đủ sự an toàn

C. Dịch vụ xác thực chỉ cung cấp khả năng xác thực các thức thế giao tiếp

D. Thông điệp trước khi thực hiện mã hoá (thông điệp gốc) được gọi là plaintext

Câu 40: **Hãy cho biết ước số chung lớn nhất (GCD) của 8376238 và 1981252 là bao nhiêu (sử dụng thuật toán Euclidean)**

A. 26 B. 33 C. 13 D. 57

Câu 41: **Các trạng thái của cổng (port) được xác định bởi chương trình NMAP có thể là?**

A. Open, half-open, closed B. Active, closed, unused

C. Open, filtered, unfiltered D. Active, inactive, standby

Câu 42: **Trong hệ mã RSA, một người sử dụng 2 số nguyên tố p=13 và q=17 để sinh ra 1 cặp khoá riêng và khoá công khai. Nếu khoá công khai có giá trị là 35, thì khoá riêng tương ứng của người này có giá trị là bao nhiêu?**

A. 19 B. 7 C. 23 D. 11

Câu 43: **Dùng công cụ hydra thực hiện tấn công vét cạn mặt khẩu trên dịch vụ SSH của máy chủ Linux, với người dùng có tên đăng nhập là root, địa chỉ IP của máy chủ là 192.168.1.105, danh sách mật khẩu được cho trong tập tin rockyou.txt, câu lệnh nào sau đây là đúng?**

A. hydra -l root -P rockyou.txt 192.168.1.105 -t 4 ssh

B. hydra -u root -p rockyou.txt -h 192.168.1.105 ssh

C. hydra-u root -p rockyou.txt 192.168.1.105 ssh

D. hydra-l root -p rockyou.txt 192.168.1.105 ssh

Câu 44: **Trong PGP, để gởi các E-mail người dùng cần có một bộ khóa, cho biết đó là bộ khoá gì?**

A. Bộ khóa bí mật B. Tất cả đều sai C. Bộ khóa công khai D. Bộ khóa riêng

Câu 45: **Bức tượng lửa (firewall) có thể giúp chống lại tấn công nào sau đây?**

A. Shoulder surfing B. Denial of Service C. Phishing D. Dumpster

Câu 46: **Hãy cho biết kết quả khi thực hiện mã hoá thông điệp "CRYPTOGRAPHY" sử dụng hệ mà Vignere Cipher với khoá là "HCMUT**

A. JTKJMXJEVJPZ B. JTKJMVIEVIOA C. JTKJMXIDUIOA D. JTKJMVIDUIOA

Câu 47: Đối với việc khởi tạo một IDS, sau khi đã xác định mục tiêu ta phải làm gì tiếp theo?

A. Chọn thành phần, hệ thống để theo dõi

B. Chọn đáp ứng thích hợp

C. Hiện thực chính sách

D. Xét các ngưỡng

Câu 48: Trong giao dịch điện tử an toàn (SET), người mua hàng mã hoá thông tin thì (credit card) của mình sử dụng khoá nào sau đây?

A. Khoá riêng của khách hàng

B. Khoa riêng của ngân hàng

C. Khoa công khai của ngân hàng

D. Khối công khai của người bán hàng

Câu 50: Điểm yếu của bộ lọc gọi là:

A. Không hỗ trợ các lược đổ xác thực người dùng.

B. Không phát hiện giả mạo địa chỉ IP

C. Tất cả các câu trả lời đều đúng.

D. Không xem xét dữ liệu ở tầng cao hơn.