MẬT MÃ & AN NINH MẠNG

ĐỀ THI HK-211

Câu 1: Chọn phát biểu sai về các phương pháp xác thực

A. Giao thức xác thực dùng mã hoá đối xứng hỗ trợ xác thực hai chiều

B. Phương pháp xác thực dựa trên mật khẩu không an toàn trước tấn công xen giữa

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

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

Câu 2: Giả sử mật 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: $95^{10} \approx 6 \times 10^{19}$ và lấy kết quả gần đúng nhất).

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

Câu 3: Chọn phát biểu sai về công cụ CrypTool?

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

B. Là công cụ hỗ trợ tấn công mạng

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

D. Câu B và C đều đúng

Câu 4: Chọn phát biểu ĐÚNG trong các phát biểu dưới đây?

A. Dịch vụ xác thực cung cấp khả năng xác thực các thực thể giao tiếp

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

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

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

Câu 5: Thuật ngữ nào sau đây liên quan đến cấu hình bức tường lửa?

A. single-homed bastion host B. Tất cả câu trả lời đều đúng

C. dual-homed bastion host D. screened subnet

Câu 6: 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 thực hiện 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 mã hoá dòng

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

Câu 7: **Trong ngôn ngữ lập trình Java, lớp CertStore thuộc gói (Package) nào sau đây?**

A. java.security B. javax.crypto.spec C. java.security.cert D. javax.crypto

Câu 8: **Chọn phát biểu đúng nhất về chữ ký số**

A. Tồn tại 2 thông điệp khác nhau có cùng giá trị chữ ký số

B. Tất cả các câu trả lời đều sai

C. Hàm bầm được sử dụng trong chữ ký số phải được hiện thực trên phần cứng

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

Câu 9: **Các cổng (port) mặc định của giao thức https và http có giá trị lần lượt là:**

A. 80, 443 B. 80, 8080 C. 8080, 80 D. 443, 80

Câu 10: **Loại ứng dụng nào sau đây không thể dùng để che giấu địa chỉ IP của người dùng khi duyệt web?**

A. Bức tường lửa (Firewall) C. Mạng riêng ảo (VPN)

B. Chế độ ẩn danh (Incognito mode) của trình duyệt D. Các câu A và B đều đúng

Câu 11: **Trong chương trình web server Apache, các tập tin cấu hình có phần đuôi mở rộng là:**

A. json B. conf C. cnf D. xml

Câu 12: **Đâu là kỹ thuật giấu tin để chuyển tải các thông điệp một cách bí mật, sao cho ngoại trừ người gửi và người nhận, không ai biết đến sự tồn tại của thông điệp?**

A. Steganography B. Cryptanalysis C. Tất cả trả lời đều đúng D. Cryptography

Câu 13: **Giải thuật băm MD5 sinh ra giá trị băm có độ dài bao nhiêu?**

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

Câu 14: **Hình thức tấn công nào sau đây là tấn công chủ động?**

A. Các câu trả lời đều đúng B. Phân tích lưu lượng

C. Lấy ra nội dung thông điệp D. Phát lại

Câu 15: **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. Smurf C. Social engineering D. Man-in-the-middle

Câu 16: **Thông tin nào sau đây không tồn tại trong các chứng chỉ X.509:**

A. Khoá công khai của thực thể được cấp chứng chỉ B. Chữ ký số của tổ chức CA cấp chứng chỉ

C. Khoá công khai của tổ chức CA cấp chứng chỉ D. Tên của tổ chức CA cấp chứng chỉ

Câu 17: **Hãy cho biết kết quả khi thực hiện mã hoá thông điệp "CRYPTOGRAPHY" sử dụng hệ mã Vignere Cipher với khoá là "HCMUT"**

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

Câu 18: Phát biểu nào sau đây không phải là điểm yếu của bộ lọc gói là:

A. Không hỗ trợ các lược đồ xác thực người dùng.
B. Không phát hiện giả mạo địa chỉ IP.
C. Không xem xét dữ liệu ở tầng cao hơn.
D. Không chấp nhận phân mảnh gói tin.

Câu 19: Trong ngôn ngữ lập trình Java, lớp KeyPairGenerator được dùng để làm gì?

A. Phân phối khoá giữa 2 thực thể giao tiếp

B. Tạo số nguyên tố ngẫu nhiên lớn

C. Tạo một cặp khoá gồm khoá công khai và khoá riêng với một hệ mã khoá công khai đã quy định

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

Câu 20: Loại chương trình độc hại có khả năng tự sao chép và lây nhiễm sang các máy tính khác trong mạng máy tính được gọi là gì?

A. Tất cả đều đúng.
B. Worm
C. Virus
D. Spyware

Câu 21: Đối với việc khởi tạo một IDS, sau khi đã chọn thành phần, hệ thống để theo dõi ta phải làm gì tiếp theo?

A. Hiện thực chính sách
B. Xác định mục tiêu
C. Chọn đáp ứng thích hợp
D. Xét các ngưỡng

Câu 22: Chọn phát biểu đúng về hệ thống mạng riêng ảo (VPN):

A. Các câu trả lời đều đúng

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 23: Cho biết cấu hình bức tưởng lửa nào sau dãy khi 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

Câu 24: Hãy cho biết ước số chung lớn nhất (GCD) của 5376238 và 1981252 là bao nhiêu (sử dụng thuật toán Euclidean)

A. 26
B. 32
C. 14
D. 56

Câu 25: Nguyên tắc nào sau đây không phải là nguyên tắc cốt lõi của an toàn thông tin?

A. Sẵn sàng
B. Toàn vẹn
C. Xác thực
D. Bí mật

Câu 26: Phương pháp sử dụng OTP (One Time Password) để xác thực người dùng dựa trên yếu tố nào?

A. Những gì bạn biết
B. Những gì bạn có
C. Những gì là chính bạn
D. Cả A và B đều đúng

Câu 27: Giao thức nào sau đây là giao thức an toàn?

A. smtp
B. ftp
C. imap
D. https

Câu 28: **Trong hệ mã hoá khoá công khai, giả sử A mã hoá thông điệp sử dụng khoá riêng của A và gởi thông điệp đã được mã hoá trên cho B, hãy chọn phát biểu SAI:**

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 khoá công khai của A

C. Ai cũng có thể giải mã được thông điệp trên nếu biết khoá công khai của A

D. Câu A và C đều đúng

Câu 29: **Chuẩn bảo mật cho mạng cục bộ không dây nào dưới đây mà người khác dễ dàng bẻ khoá hoặc giả mạo nhằm sử dụng không hợp pháp mạng cục bộ không dây?**

A. WPA B. WEP C. Tất cả đều đúng D. WPA2

Câu 30: **Trong PGP, để đọc được các E-mail đã được mã hóa khi gởi người dùng cần có một bộ khóa, cho biết đó là bộ khóa gì?**

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

Câu 31: **Hãy cho biết kết quả của ($(7^{2021}$ mod 13):**

A. 11 B. 8 C. 9 D. Tất cả đều sai

Câu 32: **Trong giải thuật DES, cho bảng 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: 101000 khi thực hiện chuyển đổi bằng S-Box này?

A. 1100 B. 1001 C. 0111 D. 0011

Câu 33: **Các trạng thái của cổng (port) được xác định bởi chương trình NMAP không thể là?**

A. Unfiltered B. Filtered C. Open D. Active

Câu 34: **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 mã hoá đối xứng. Giao tiếp giữa 2 người bất kỳ không bị giải mã 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 35: **Tổ chức CA (Certification Authority) sử dụng khóa nào sau đây để tạo chứng chỉ khóa công khai?**

A. Khoá riêng của người đã đăng ký. B. Khoá công khai của CA

C. Khoá công khai của người đã đăng ký D. Khoá riêng của CA

Câu 36: **Biện pháp nào sau đây là không cần thiết để ngăn chặn lây nhiễm virus trên máy tính?**

A. Cài đặt các bản vá lỗi cho các app và hệ điều hành C. Cài đặt chương trình bức tường lửa

B. Cài đặt chương trình phát hiện xâm nhập D. Dọn rác máy tính

Câu 37: **Phần mềm nào có thể được dùng để triển khai một hệ thống phát hiện thêm nhập bất hợp pháp?**

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

Câu 38: **Đối với hệ mã hóa khóa công khai, khóa nào được sử dụng để tạo chữ ký số cho một thông điệp:**

A. Khóa riêng của người gửi B. Khóa riêng của người nhận

C. Khóa công khai của người nhận D. Khóa công khai của người gửi

Câu 39: **Khi cần truyền một thông điệp và chỉ dùng dịch vụ bí mật 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. Chữ ký số trên thông điệp.

C. Thông điệp D. Tóm tắt thông điệp

Câu 40: **Với công cụ fail2ban trên hệ điều hành CentOS 7, để xóa bỏ một địa chi a.b.c.d đã bị cấm kết nối từ xa trên dịch vụ SSH ta có thể dùng lệnh nào sau đây?**

A. fail2ban-client set ssh unbanip a.b.c.d B. fail2ban-client set ssh unban a.b.c.d

C. fail2ban-client set sshd unbanip a.b.c.d D. fail2ban-client set sshd unban a.b.c.d

Câu 41: **Để cài đặt giao thức HTTPS cho web server Apache, chúng ta cần kích hoạt module nào sau đây:**

A. mod_proxy B. mod_ssl C. mod_tls D. Câu B và C đều đúng

Câu 42: **Trong giao dịch điện tử an toàn (SET), người mua hàng mã hoá thông tin thanh toán sử dụng khoá nào sau đây?**

A. Khoá riêng của khách hàng B. Khoá riêng của ngân hàng

C. Khóa phiên phát sinh ngẫu nhiên D. Khoá công khai của ngân hàng

Câu 43: **Cho biết phát biểu đúng về dual signature trong các phát biểu sau:**

A. Tất cả các câu trả lời đều đúng

B. Dual signature được dùng để ký trên hai tài liệu nối với nhau và mỗi tài liệu này có hash code riêng.

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

D. 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).

Câu 44: **Bức tường lửa (firewall) không thể giúp chống lại tấn công nào sau đây?**

A. Phishing B. Shoulder surfing C. Tất cả đều đúng D. Dumpster diving

Câu 45: **Phần mềm nào dưới đây là không phải là phần mềm mã nguồn mở được hiện thực để triển khai giao thức SSL/TLS trong thực tế:**

A. OpenSSL B. MbedTLS C. WolfSSL D. Cryptool

Câu 46: **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 11, thì khoá riêng tương ứng của người này có giá trị là bao nhiêu?**

A. 7 B. 19 C. 35 D. 23

Câu 47: Thuật toán mã hóa được sử dụng trong chuẩn WPA2 là gì?

A. 3-DES B. RC4 C. AES D. RC4 with TKI(P/MIC)

Câu 48: Dùng công cụ hydra thực hiện tấn công vết cạn mật khẩu trên dịch vụ Remote Desktop của máy chủ Microsoft Windows, với người dùng có tên đăng nhập là admin, 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 - admin -P rockyou.txt rdp://192.168.1.105 -t 4

B. hydra-l admin -p rockyou.txt 192.168.1.105 rdp

C. hydra -u admin -p rockyou.txt rdp://192.168.1.105

D. Các câu trả lời đều đúng

Câu 49: Điều gì là phản ứng không thích hợp cho một sự kiện bảo mật trên mạng?

A. Cài đặt lại bức tường lửa B. Thực hiện các thủ tục an ninh

C. Ngắt kết nối mạng D. Các cầu A và C đều đúng.

Câu 50: Có bao nhiêu khoá được sử dụng trong giải thuật DES

A. 1 khoá B. 3 khoá C. 2 khoá hoặc 3 khoá D. 2 khoá