Câu 1: Tính toàn vẹn dữ liệu trong an toàn thông tin được hiểu như sau:

• Tài sản của hệ thống chỉ được truy cập bởi những người có thẩm quyền.
✔ Tài sản của hệ thống chỉ được thay đổi bởi những người có thẩm quyền.
• Tài sản luôn sẵn sàng được sử dụng bởi những người có thẩm quyền.
• Tài sản được bảo vệ cho tới khi hết giá trị sử dụng hoặc hết ý nghĩa bí mật.

Câu 2: Tính sẵn dùng trong an toàn thông tin được hiểu như sau:

• Tài sản của hệ thống chỉ được truy cập bởi những người có thẩm quyền.
• Tài sản của hệ thống chỉ được thay đổi bởi những người có thẩm quyền.
✔ Tài sản luôn sẵn sàng được sử dụng bởi những người có thẩm quyền.
• Tài sản được bảo vệ cho tới khi hết giá trị sử dụng hoặc hết ý nghĩa bí mật.

Câu 3: Mã hóa là gì?

✔ Là quá trình biến đổi thông tin từ dạng đọc được sang không đọc được.
• Quá trình tấn công hệ mật mã để tìm bản rõ và khóa bí mật.
• Quá trình biến đổi thông tin từ dạng không đọc được sang đọc được.
• Giấu thông tin để không nhìn thấy.

Câu 4: Thám mã là gì?

✔ Quá trình tấn công hệ mật mã để tìm bản rõ và khóa bí mật.
• Quá trình biến đổi thông tin từ dạng đọc được sang dạng không đọc được.
• Quá trình biến đổi thông tin từ dạng không đọc được sang dạng đọc được.
• Giấu thông tin để không nhìn thấy.

Câu 5: AES là thuật toán thuộc nhóm

✔ Mã hóa khóa đối xứng.
• Mã hóa khóa bất đối xứng.
• Thuật toán tạo chữ ký điện tử.
• Hàm băm.

Câu 6: Thuật toán nào không phải là thuật toán mã hóa khóa đối xứng?

• DES
✔ RSA
• AES
• Caesar

Câu 7: Ứng dụng để các bên đã được xác thực không thể phủ nhận việc tham gia vào một giao dịch hợp lệ trong hệ thống được gọi là

• Bảo mật
• Xác thực hóa
• Toàn vẹn

✔ Dịch vụ không thể chối từ

Câu 8: Giả sử trường gioi_tinh trong cơ sở dữ liệu chỉ lưu trữ nam hoặc nữ. Như vậy Entropy của thông báo chứa trường này là ?

• 2
✔ 1
• 0.5
• 1/2

Câu 9: Số bits lớn nhất cần thiết để mã hóa các ký tự của ngôn ngữ được gọi là

• Tốc độ của ngôn ngữ.
✔ Tốc độ tuyệt đối của ngôn ngữ.
• Độ trễ của ngôn ngữ.
• Độ dư thừa của ngôn ngữ.

Câu 10: Tiếng Anh gồm 26 chữ cái, tốc độ tuyệt đối của ngôn ngữ tiếng Anh là

• 0.28
• 1.3
✔ 4.7
• 3.4

Câu 11: Có bao nhiêu kỹ thuật cơ bản để che dấu sự dư thừa thông tin

✔ 2
• 3
• 4
• 5

Câu 12: Trong các số sau, số nào là số nguyên tố: 2, 4, 13, 19, 25, 31

• 2, 4, 13, 19, 31.
• 4, 13, 19, 25, 31.
✔ 2, 13, 19, 31.
• 2, 4, 13, 19.

Câu 13: Khẳng định nào sau đây là sai?

• Số 2 là số nguyên tố bé nhất.
✔ Mọi số nguyên tố đều là số lẻ.
• Hợp số là số tự nhiên lớn hơn 1, có nhiều hơn 2 ước.
• Có 2 số tự nhiên liên tiếp là số nguyên tố.

Câu 14: Chọn phát biểu sai:

• Số nguyên tố nhỏ hơn 10 là 2, 3, 5, 7.

• 2 là số nguyên tố chẵn duy nhất.
• Số 0 không là số nguyên tố cũng không là hợp số.
✔ Số 1 là số nguyên tố bé nhất.

Câu 15: Hệ mã khóa dòng được biết là một:

✔ Hệ mã khóa đối xứng
• Hệ mã khóa phi đối xứng
• Hệ mã khóa công khai
• Hệ mã khóa cổ điển

Câu 16: PKC (Public Key Cryptosystem) được hiểu là:

• Hệ mã khóa đối xứng
✔ Hệ mã khóa phi đối xứng
• Hệ mã khóa dòng
• Hệ mã khóa cổ điển

Câu 17: RSA là giải thuật

✔ Mã công khai
• Là tên của một tổ chức quốc tế về mã hóa
• Mã khóa riêng
• Hàm băm

Câu 18: Thám mã khi không biết khoá

• Bài toán dễ
✔ Bài toán khó
• Phụ thuộc vào khoá
• Phụ thuộc vào giải thuật

Câu 19: Thuật toán nào sau đây là thuật toán mã hóa theo khối (Block ciphers)

✔ DES
• RC4
• A5/1
• A5/2

Câu 20: Ứng dụng của mật mã bao gồm:

• Mã hóa, toàn vẹn thông tin, sinh chữ ký số, thỏa thuận khóa.
✔ Bảo mật dữ liệu, xác thực toàn vẹn thông tin, chữ ký số và quản lý khóa.
• Bảo mật dữ liệu, xác thực thông tin, xác nhận chữ ký số, phân phối khóa băm, chữ ký điện tử.
• Mã hóa dữ liệu, tạo hàm ký số, quản lý khóa.

Câu 21: Theo Shannon, entropy được hiểu là gì:

✔ Đo khối lượng thông tin của thông điệp.
• Đo độ an toàn thông báo.
• Đo độ dài bản mã của thông báo.
• Kết hợp các đáp án trên.

Câu 22: Các cách tăng sự an toàn của bản rõ trong hệ mã là:

• Nén bản rõ.
• Che giấu mối quan hệ giữa bản rõ và bản mã.
• Tăng sự phụ thuộc giữ bản mã và bản rõ.
✔ Nén bản rõ, che giấu mối quan hệ giữa bản rõ và bản mã, tăng sự phụ thuộc giữ bản mã và bản rõ.

Câu 23: Theo Shannon, để che giấu sự dư thừa thông tin bản rõ:

• Giải thuật mã hóa phức tạp
• Khóa độ dài lớn
• Kết hợp các đáp án trên
✔ Bản mã có sự lộn xộn và sự rườm rà

Câu 24: Theo Shannon, hệ mã an toàn tuyệt đối nếu:

• Giải thuật mã hóa phức tạp.
• Khóa thay đổi liên tục.
✔ Khoá có độ dài tối thiểu là tương đương độ dài thông báo.
• Kết hợp các đáp án trên.

Câu 25: Hacker thuộc nhóm đối tượng đe dọa hệ thống nào?

• Đối tượng từ bên trong hệ thống.
✔ Đối tượng từ bên ngoài hệ thống.
• Các phần mềm chạy trên hệ thống.
• Không thuộc các nhóm đối tượng đe dọa hệ thống.

Câu 26: Tính bí mật dùng trong an toàn thông tin được hiểu như sau:

✔ Tài sản của hệ thống chỉ được truy cập bởi những người có thẩm quyền.
• Tài sản của hệ thống chỉ được thay đổi bởi những người có thẩm quyền.
• Tài sản luôn sẵn sàng được sử dụng bởi những người có thẩm quyền.
• Tài sản được bảo vệ cho tới khi hết giá trị sử dụng hoặc hết ý nghĩa bí mật.

Câu 27: DES là thuật toán thuộc nhóm

✔ Mã hóa khóa bí mật.
• Mã hóa khóa công khai.
• Thuật toán tạo chữ ký điện tử.

• Hàm băm.

Câu 28: Entropy trong lý thuyết thông tin dùng để

• Mã hóa thông tin.
• Giải mã thông tin.
• Chứa khóa thông tin.
✔ Đo khả năng chứa thông tin.

Câu 29: Nếu có L ký tự trong một ngôn ngữ. Công thức R = log 2 L dùng để tính

• Tốc độ của ngôn ngữ.
✔ Tốc độ tuyệt đối của ngôn ngữ.
• Độ trễ của ngôn ngữ.
• Độ dư thừa của ngôn ngữ.

Câu 30: Mã dịch vòng Caesar thuộc nhóm kỹ thuật che dấu thông tin nào

✔ Kỹ thuật lộn xộn (Confusion)
• Kỹ thuật rườm rà (Diffusion)
• Kỹ thuật hoán vị
• Kỹ thuật đổi chỗ (Swap)

Câu 31: SKC (Symmetric Key Cryptosystem) được hiểu là:

✔ Hệ mã khóa đối xứng
• Hệ mã khóa phi đối xứng
• Hệ mã khóa dòng
• Hệ mã khóa cổ điển

Câu 32: Đối với mã hóa khóa công khai, khóa nào được sử dụng để mã hóa một thông điệp:

✔ Khóa công khai của người nhận.
• Khóa riêng của người nhận.
• Khóa công khai của người gửi.
• Khóa riêng của người gửi.

Câu 33: Thuật toán nào sau đây là thuật toán mã hóa dòng (Stream ciphers).

• DES,
• 3DES
• RC5
✔ RC4

Câu 34: Nếu Bob muốn gửi một tin nhắn an toàn cho Alice bằng cách sử dụng một thuật toán mã hóa bất đối xứng, thì anh ta sử dụng khóa nào để mã hóa thông điệp:

✔ Khoá công khai của Alice.
• Khoá bí mật của Alice.
• Khoá bí mật của Bob.
• Khoá công khai của Bob.

Câu 35: Các yếu tố không ảnh hưởng đến sự an toàn của một hệ mã mật:

• Bí mật của khóa
• Giải thuật mã hóa và giải mã
✔ Độ dài bản mã
• Độ phức tạp tính toán của hệ mã

Câu 36: Kết luận nào sau là đúng cho DES:

• Là hệ mã hóa có độ phức tạp thấp.
• Là hệ mã hóa PKC.
• Là hệ mã hóa có không gian khóa nhỏ.
✔ Là hệ mã hóa dựa trên mã Lucipher.

Câu 37: AES có mấy khóa chính (khóa chủ):

• 2
✔ 3
• 4
• 5

Câu 38: Số lượng hộp mật (S-box) của giải thuật Des:

• 6
✔ 8
• 10
• 12

Câu 39: Với hệ mã hóa AES có số vòng lặp:

• 8, 12, hoặc 14.
• 8, 16, hoặc 32.
• 10, 16, hoặc 32.
✔ 10, 12, hoặc 14.

Câu 40: Trong hệ mã hóa khóa công khai nhận định nào sau đây là ĐÚNG?

• Sử dụng khóa mật để MÃ HÓA, sử dụng khóa công khai để GIẢI MÃ.
✔ Sử dụng khóa công khai để MÃ HÓA, khóa bí mật để GIẢI MÃ.
• Sử dụng hai khóa do người gửi sinh ra.
• Sử dụng một khóa mật chung cho cả hai hệ mã.

Câu 41: Đối với tiêu chuẩn mã hóa dữ liệu DES, mỗi khối gồm bao nhiêu bit

• 16
• 32
✔ 64
• 128

Câu 42: Đối với tiêu chuẩn mã hóa dữ liệu DES, số khóa của không gian khóa k là

• 2 64
✔ 2 56
• 2 32
• 2 16

Câu 43: Trong giai đoạn 1 của hàm Feistel. 32 bít đầu vào được mở rộng thành bao nhiêu bit

• 32
✔ 48
• 64
• 128

Câu 44: DES có bao nhiêu khóa yếu (weak keys)

• 16
• 8
✔ 4
• 2

Câu 45: DES có bao nhiêu cặp khóa nửa yếu (semi-weak keys)

✔ 6
• 8
• 4
• 2

Câu 46: Mỗi khối dữ liệu trong tiêu chuẩn AES có kích thước bao nhiêu?

• 2x2
✔ 4x4
• 3x3
• 5x5

Câu 47: Trong thuật toán AES, Quá trình đổi chỗ, các hàng trong khối được dịch vòng là bước nào trong các bước sau đây

• AddRoundKey
• SubBytes

✔ ShiftRows
• MixColumns

Câu 48: Dạng tấn công duy nhất thành công lên AES là

• Tấn công bạo lực
✔ Tấn công bên trên
• Tấn công bên dưới
• Tấn công tổng hợp

Câu 49: Phát biểu nào sau đây KHÔNG phải ưu điểm của mã hóa đối xứng

• Tốc độ lập mã
• Độ bảo mật khá cao
✔ Đảm bảo tính toàn vẹn dữ liệu
• Dễ cài đặt và hoạt động hiệu quả

Câu 50: Trong sơ đồ sinh khóa của DES từ khóa chính 56 bit sinh

• 8 khóa con mỗi khóa 48 bit, mỗi khóa dùng cho 1 vòng.
• 16 khóa con mỗi khóa 32 bit, mỗi khóa dùng cho 1 vòng.
• 12 khóa con mỗi khóa 32 bit, mỗi khóa dùng cho 1 vòng.
✔ 16 khóa con mỗi khóa 48 bit, mỗi khóa dùng cho 1 vòng.

Câu 51: Mã DES có khối dữ liệu, khóa (bit) và số vòng tương ứng như sau

• 128, 56 và 16
• 64, 64 và 16
✔ 64, 56 và 16
• 64, 56 và 12

Câu 52: Trong hộp S-BOX, có bao nhiêu bít đầu vào

• 2
• 4
✔ 6
• 8

Câu 53: Giá trị nào sau đây KHÔNG có trong hộp S-BOX

• 5
• 10
• 15
✔ 20

Câu 54: Trong DES, tại mỗi vòng lặp mỗi khóa con có bao nhiêu bít

• 16

• 24
• 32
✔ 48

Câu 55: Trong hệ mã khối, sử dụng bảng thay thế số liệu (s-box) cho biểu thức tính toán để:

✔ Tăng tốc độ tính toán
• Giải mã khó
• Tạo thuận tiện cho lập trình
• Kết hợp các đặc điểm trên

Câu 56: Độ dài khóa chính (khóa chủ) của AES:

✔ 128 hoặc 192, hoặc 256 bit
• 64 hoặc 128, hoặc 256 bit
• 64 hoặc 192, hoặc 256 bit
• 128 hoặc 256, hoặc 512 bit

Câu 57: Mệnh đề nào sau đây là SAI:

• DES có các khóa con độ dài 48 bit
• DES có 4 khóa yếu
• DES có 6 cặp khóa nửa yếu
✔ DES có các khóa con độ dài 32 bit

Câu 58: Đối với tiêu chuẩn mã hóa dữ liệu DES, mỗi khối dành bao nhiêu bit để kiểm tra lỗi

• 32
• 16
✔ 8
• 4

Câu 59: Phương pháp tấn công bằng cách thử lần lượt tất cả các khóa có thể cho đến khi tìm ra khóa đúng được gọi là

✔ Tấn công bạo lực
• Tấn công phá mã vi sai
• Tấn công phá mã tuyến tính
• Tấn công phá mã Davies

Câu 60: Tiêu chuẩn mã hóa AES được NIST chọn để thay thế DES vào năm

• 2000
✔ 2001
• 2002
• 2003

Câu 61: Trong thuật toán AES, Quá trình thực hiện phép thế (phi tuyến) trong đó mỗi byte sẽ được thế bằng một byte khác theo bảng tra là bước nào trong các bước sau đây

• AddRoundKey
✔ SubBytes
• ShiftRows
• MixColumns

Câu 62: Trong các hệ mã hóa sau hệ mã nào không phải hệ mã hóa khóa khối?

• Trapdoor
• DES
• AES
✔ DSA

Câu 63: Trong hộp S-BOX, có bao nhiêu bít đầu ra

• 2
✔ 4
• 6
• 8

Câu 64: Có bao nhiêu hộp S-BOX được dùng trong DES

• 2
• 4
• 6
✔ 8

Câu 65: Phát biểu nào sau đây không đúng về DES

✔ DES là thuật toán mã hóa đối xứng dạng dòng.
• Đầu vào của DES là 64 bít.
• Thuật toán DES thực hiện 16 vòng lặp.
• Đầu vào của DES là 64 bít.

Câu 66: Sau bước hoán vị khởi tạo (IP), bản rõ 64 được chia thành bao nhiêu phần bằng nhau

✔ 2
• 4
• 8
• 16

Câu 67: Trong 64 bít đầu vào, DES sử dụng bao nhiêu bít để kiểm tra chẵn lẻ

• 2

• 4
• 6
✔ 8

Câu 68: Có bao nhiêu khóa con được sinh ra sau quá trình lặp

• 2
• 8
✔ 16
• 32

Câu 69: Chọn phát biểu SAI trong mã hóa DES

✔ Các khóa con giống nhau
• DES có 16 khóa con
• Mỗi khóa con có 48 bít
• Đầu ra của DES có 64 bít

Câu 70: AES-192 có độ dài khóa là

• 32
• 64
• 128
✔ 192

Câu 71: Hàm biến đổi được sử dụng trong thuật toán mã hóa và giải mã trong đó thực hiện phép toán XOR bit giữa một trạng thái trung gian (State) và một khóa của vòng lặp (Round Key) là

✔ AddRoundKey()
• MixColumns()
• ShiftRows()
• SubBytes()

Câu 72: Trong AES, hàm gì thực hiện dịch vòng 3 hàng cuối của mảng trạng thái với số lần dịch khác nhau

• AddRoundKey()
• MixColumns()
✔ ShiftRows()
• SubBytes()

Câu 73: Trong AES, hàm gì làm việc trên các cột của mảng trạng thái.

• AddRoundKey()
✔ MixColumns()
• ShiftRows()
• SubBytes()

Câu 74: Giải thuật AES quá trình lặp gồm có bao nhiêu bước chính

• 3
✔ 4
• 5
• 6

Câu 75: Quá trình lặp để giải mã AES gồm bao nhiêu bước chính

• 3
✔ 4
• 5
• 6

Câu 76: Đối với AES, nếu khóa có độ dài 192 bít, giải thuật lặp bao nhiêu lần

• 10
✔ 12
• 14
• 16

Câu 77: Đối với AES, nếu khóa có độ dài 256 bít, giải thuật lặp bao nhiêu lần

• 10
• 12
✔ 14
• 16

Câu 78: Bản chất của hàm AddRoundKey() trong AES là dùng phép tính nào

• AND
• OR
• NOT
✔ XOR

Câu 79: So với hệ mã khối, hệ mã mật khóa công khai có đặc tính gì:

• Có khóa được công khai nên nội dung thông điệp dễ dàng bị giải mã.
• Giải thuật mã hóa công khai nên không an toàn.
• Không gian khóa nhỏ dễ bị thám mã.
✔ Có tốc độ tính toán chậm.

Câu 80: Hoạt động của RSA gồm có bao nhiêu bước

• 3
✔ 4
• 5

• 6

Câu 81: Hệ mật mã dựa trên bài Logarit rời rạc là

✔ Hệ mật mã ElGamal
• Hệ mật mã đường cong Elliptic
• Hệ mật mã Merkle-Hellman
• Hệ mật mã RSA

Câu 82: Hệ mật mã dựa cấu trúc đại số của các đường cong trên những trường hữu hạn là

• Hệ mật mã ElGamal
✔ Hệ mật mã đường cong Elliptic
• Hệ mật mã Merkle-Hellman
• Hệ mật mã RSA

Câu 83: Kích thước của MD5 là

• 64
✔ 128
• 256
• 512

Câu 84: SHA-1 trả lại kết quả dài bao nhiêu bit

✔ 160
• 128
• 256
• 512

Câu 85: Chữ ký số được xây dựng dựa trên

• Công nghệ mã hóa khóa bất đối xứng.
• Công nghệ mã hóa khóa đối xứng.
✔ Công nghệ mã hóa công khai hoặc bất đối xứng.
• Công nghệ mã hóa đối xứng hoặc công khai.

Câu 86: Hàm băm có độ dài biến thiên là

• SHA1
• MD5
✔ HAVAL
• RIPEMD

Câu 87: Dịch vụ chứng thực chữ ký điện tử phát hành nhằm xác nhận cơ quan, tổ chức, cá nhân được chứng thực là người ký chữ ký điện tử gọi là

✔ Chứng thư điện tử
• Chữ ký điện tử
• Chữ ký số
• Công chứng

Câu 88: Giả sử An gửi một bức thư cho Bình, khi nhận được thư, Bình nhận ra được đúng là thư do An gửi, không phải là do một kẻ thứ ba giả mạo. Đây là nguyên lý gì của bảo mật thông tin

✔ Tính nhận biết
• Tính không chối bỏ
• Tính bảo mật
• Tính toàn vẹn thông tin

Câu 89: Giả sử An gửi một bức thư cho Bình, khi nhận được thư, Lá thư dù lọt vào tay kẻ khác ngoài Bình thì kẻ đó cũng không hiểu được nội dung thư. Đây là nguyên lý gì của bảo mật thông tin

• Tính nhận biết
• Tính không chối bỏ
✔ Tính bảo mật
• Tính toàn vẹn thông tin

Câu 90: Chuẩn mã hóa AES có kích thước dữ liệu đầu vào là?

• 32
• 64
✔ 128
• 256

Câu 91: Trong AES, hàm gì thực hiện phép thay thế các byte của mảng trạng thái bằng cách sử dụng một bảng thế S-BOX

• AddRoundKey()
• MixColumns()
• ShiftRows()
✔ SubBytes()

Câu 92: Trong AES, hàm gì thực hiện hoán vị vòng một DoubleWord thành một DoubleWord

✔ RotWord()
• SubWord()
• Rcon()
• SubByte()

Câu 93: Đối với AES, nếu khóa có độ dài 128 bít, giải thuật lặp bao nhiêu lần

✔ 10

• 12
• 14
• 16

Câu 94: Hàm ShiftRow trong AES thực hiện không dịch hàng bao nhiêu của mảng trạng thái?

✔ 1
• 2
• 3
• 4

Câu 95: Hệ mã nào được xây dựng dựa trên tính khó giải của bài toán phân tích một số thành thừa số nguyên tố

• DES
• ASE
✔ RSA
• 3DES

Câu 96: Chọn phát biểu đúng về ưu điểm của RSA

✔ Mã RSA có độ bảo mật cao.
• Mã RSA có tính tin cậy.
• RSA thực hiện một dãy phép tính lũy thừa modulo khá lớn.
• Tốc độ lập mã và giải mã rất chậm.

Câu 97: Phát biểu nào sau đây SAI về hàm băm

✔ Nếu hai giá trị băm khác nhau thì chắc chắn hai khối dữ liệu tạo ra chúng là giống nhau.
• Ứng với mỗi khối dữ liệu một giá trị băm duy nhất.
• Hàm băm được đánh giá là tốt nếu số đụng độ xảy ra rất nhỏ.
• Là một giải thuật toán học (một ánh xạ một - một (một chiều)).

Câu 98: Chọn phát biểu sai về hàm băm tốt

• Xử lý được các loại khóa có kiểu dữ liệu khác nhau.
✔ Tính toán chậm.
• Ít xảy ra đụng độ.
• Các khóa được phân bố đều trong bảng.

Câu 99: Phát biểu nào sau đây là SAI về chữ ký số

• Là lớp con của chữ ký điện tử.
✔ Dựa trên công nghệ khóa đối xứng.
• Khóa bí mật dùng để tạo chữ ký số.
• Khóa công khai dùng để thẩm định CKS.