Câu 1: Tính toàn vẹn dữ liệu trong an toàn thông tin được hiểu như sau:	Đáp án đúng: Tài sản của hệ thống chỉ được thay đổi bởi những người có thẩm quyền.
Câu 2: Tính sẵn dùng trong an toàn thông tin được hiểu như sau:	Đáp án đúng: Tài sản luôn sẵn sàng được sử dụng bởi những người có thẩm quyền.
Câu 3: Mã hóa là gì?	Đáp án đúng: Là quá trình biến đổi thông tin từ dạng đọc được sang không đọc được.
Câu 4: Thám mã là gì?	Đáp án đúng: Quá trình tấn công hệ mật mã để tìm bản rõ và khóa bí mật.
Câu 5: AES là thuật toán thuộc nhóm	Đáp án đúng: Mã hóa khóa đối xứng.
Câu 6: Thuật toán nào không phải là thuật toán mã hóa khóa đối xứng?	Đáp án đúng: RSA
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	Đáp án đúng: 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 ?	Đáp án đúng: 1
Câu 9: Số bits lớn nhất cần thiết để mã hóa các ký tự của ngôn ngữ được gọi là	Đáp án đúng: Tốc độ tuyệt đối của ngôn ngữ.
Câu 10: Tiếng Anh gồm 26 chữ cái, tốc độ tuyệt đối của ngôn ngữ tiếng Anh là	Đáp án đúng: 4.7
Câu 11: Có bao nhiêu kỹ thuật cơ bản để che dấu sự dư thừa thông tin	Đáp án đúng: 2
Câu 12: Trong các số sau, số nào là số nguyên tố: 2, 4, 13, 19, 25, 31	Đáp án đúng: 2, 13, 19, 31.
Câu 13: Khẳng định nào sau đây là sai?	Đáp án đúng: Mọi số nguyên tố đều là số lẻ.

Câu 14: Chọn phát biểu sai:	Đáp án đúng: Số 1 là số nguyên tố bé nhất.
Câu 15: Hệ mã khóa dòng được biết là một:	Đáp án đúng: Hệ mã khóa đối xứng
Câu 16: PKC (Public Key Cryptosystem) được hiểu là:	Đáp án đúng: Hệ mã khóa phi đối xứng
Câu 17: RSA là giải thuật	Đáp án đúng: Mã công khai
Câu 18: Thám mã khi không biết khoá	Đáp án đúng: Bài toán khó
Câu 19: Thuật toán nào sau đây là thuật toán mã hóa theo khối (Block ciphers)	Đáp án đúng: DES
Câu 20: Ứng dụng của mật mã bao gồm:	Đáp án đúng: Bảo mật dữ liệu, xác thực toàn vẹn thông tin, chữ ký số và quản lý khóa.
Câu 21: Theo Shannon, entropy được hiểu là gì:	Đáp án đúng: Đo khối lượng thông tin của thông điệp.
Câu 22: Các cách tăng sự an toàn của bản rõ trong hệ mã là:	Đáp án đúng: Nén bản rõ, che giấu mối quan hệ giữa bản rõ và bản mã, tăng sự phụ thuộc giữ bản mã và bản rổ.
Câu 23: Theo Shannon, để che giấu sự dư thừa thông tin bản rõ:	Đáp án đúng: Bản mã có sự lộn xộn và sự rườm rà
Câu 24: Theo Shannon, hệ mã an toàn tuyệt đối nếu:	Đáp án đúng: Khoá có độ dài tối thiểu là tương đương độ dài thông báo.
Câu 25: Hacker thuộc nhóm đối tượng đe dọa hệ thống nào?	Đáp án đúng: Đối tượng từ bên ngoài hệ thống.
Câu 26: Tính bí mật dùng trong an toàn thông tin được hiểu như sau:	Đáp án đúng: Tài sản của hệ thống chỉ được truy cập bởi những người có thẩm quyền.
Câu 27: DES là thuật toán thuộc nhóm	Đáp án đúng: Mã hóa khóa bí mật.
Câu 28: Entropy trong lý thuyết thông tin dùng để	Đáp án đúng: 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	Đáp án đúng: Tốc độ tuyệt đối của ngôn ngữ.
Câu 30: Mã dịch vòng Caesar thuộc nhóm kỹ thuật che dấu thông tin nào	Đáp án đúng: Kỹ thuật lộn xộn (Confusion)
Câu 31: SKC (Symmetric Key Cryptosystem) được hiểu là:	Đáp án đúng: Hệ mã khóa đối xứng
Câu 32: Đối với mã hóa khóa công khai, khóa nào được sử dụng để mã hóa một thông điệp:	Đáp án đúng: Khóa công khai của người nhận.
Câu 33: Thuật toán nào sau đây là thuật toán mã hóa dòng (Stream ciphers).	Đáp án đúng: 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:	Đáp án đúng: Khoá công khai của Alice.
Câu 35: Các yếu tố không ảnh hưởng đến sự an toàn của một hệ mã mật:	Đáp án đúng: Độ dài bản mã
Câu 36: Kết luận nào sau là đúng cho DES:	Đáp án đúng: Là hệ mã hóa dựa trên mã Lucipher.
Câu 37: AES có mấy khóa chính (khóa chủ):	Đáp án đúng: 3
Câu 38: Số lượng hộp mật (S-box) của giải thuật Des:	Đáp án đúng: 8
Câu 39: Với hệ mã hóa AES có số vòng lặp:	Đáp án đúng: 10, 12, hoặc 14.
Câu 40: Trong hệ mã hóa khóa công khai nhận định nào sau đây là ĐÚNG?	Đáp án đúng: Sử dụng khóa công khai để MÃ HÓA, khóa bí mật để GIẢI MÃ.
Câu 41: Đối với tiêu chuẩn mã hóa dữ liệu DES, mỗi khối gồm bao nhiêu bit	Đáp án đúng: 64
Câu 42: Đối với tiêu chuẩn mã hóa dữ liệu DES, số khóa của không gian khóa k là	Đáp án đúng: 2 56

Câu 43: Trong giai đoạn 1 của hàm Feistel. 32 bít đầu vào được mở rộng thành bao nhiêu bit	Đáp án đúng: 48
Câu 44: DES có bao nhiêu khóa yếu (weak keys)	Đáp án đúng: 4
Câu 45: DES có bao nhiêu cặp khóa nửa yếu (semi-weak keys)	Đáp án đúng: 6
Câu 46: Mỗi khối dữ liệu trong tiêu chuẩn AES có kích thước bao nhiêu?	Đáp án đúng: 4x4
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	Đáp án đúng: ShiftRows
Câu 48: Dạng tấn công duy nhất thành công lên AES là	Đáp án đúng: Tấn công bên trên
Câu 49: Phát biểu nào sau đây KHÔNG phải ưu điểm của mã hóa đối xứng	Đáp án đúng: Đảm bảo tính toàn vẹn dữ liệu
Câu 50: Trong sơ đồ sinh khóa của DES từ khóa chính 56 bit sinh	Đáp án đúng: 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	Đáp án đúng: 64, 56 và 16
Câu 52: Trong hộp S-BOX, có bao nhiêu bít đầu vào	Đáp án đúng: 6
Câu 53: Giá trị nào sau đây KHÔNG có trong hộp S-BOX	Đáp án đúng: 20
Câu 54: Trong DES, tại mỗi vòng lặp mỗi khóa con có bao nhiêu bít	Đáp án đúng: 48
Câu 55: Trong hệ mã khối, sử dụng bảng thay thế số liệu (s-box) cho biểu thức tính toán để:	Đáp án đúng: Tăng tốc độ tính toán
Câu 56: Độ dài khóa chính (khóa chủ) của AES:	Đáp án đúng: 128 hoặc 192, hoặc 256 bit

Câu 57: Mệnh đề nào sau đây là SAI:	Đáp án đúng: 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	Đáp án đúng: 8
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	Đáp án đúng: Tấn công bạo lực
Câu 60: Tiêu chuẩn mã hóa AES được NIST chọn để thay thế DES vào năm	Đáp án đúng: 2001
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	Đáp án đúng: SubBytes
Câu 62: Trong các hệ mã hóa sau hệ mã nào không phải hệ mã hóa khóa khối?	Đáp án đúng: DSA
Câu 63: Trong hộp S-BOX, có bao nhiêu bít đầu ra	Đáp án đúng: 4
Câu 64: Có bao nhiêu hộp S-BOX được dùng trong DES	Đáp án đúng: 8
Câu 65: Phát biểu nào sau đây không đúng về DES	Đáp án đúng: DES là thuật toán mã hóa đối xứng dạng dòng.
Câu 66: Sau bước hoán vị khởi tạo (IP), bản rõ 64 được chia thành bao nhiêu phần bằng nhau	Đáp án đúng: 2
Câu 67: Trong 64 bít đầu vào, DES sử dụng bao nhiêu bít để kiểm tra chẵn lẻ	Đáp án đúng: 8
Câu 68: Có bao nhiêu khóa con được sinh ra sau quá trình lặp	Đáp án đúng: 16
Câu 69: Chọn phát biểu SAI trong mã hóa DES	Đáp án đúng: Các khóa con giống nhau

Câu 70: AES-192 có độ dài khóa là	Đáp án đúng: 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	Đáp án đúng: AddRoundKey()
Câu 72: Trong AES, hàm gì thực hiện dịch vòng 3 hàng cuối của mảng trạng thái với số lần dịch khác nhau	Đáp án đúng: ShiftRows()
Câu 73: Trong AES, hàm gì làm việc trên các cột của mảng trạng thái.	Đáp án đúng: MixColumns()
Câu 74: Giải thuật AES quá trình lặp gồm có bao nhiêu bước chính	Đáp án đúng: 4
Câu 75: Quá trình lặp để giải mã AES gồm bao nhiêu bước chính	Đáp án đúng: 4
Câu 76: Đối với AES, nếu khóa có độ dài 192 bít, giải thuật lặp bao nhiêu lần	Đáp án đúng: 12
Câu 77: Đối với AES, nếu khóa có độ dài 256 bít, giải thuật lặp bao nhiêu lần	Đáp án đúng: 14
Câu 78: Bản chất của hàm AddRoundKey() trong AES là dùng phép tính nào	Đáp án đúng: XOR
Câu 79: So với hệ mã khối, hệ mã mật khóa công khai có đặc tính gì:	Đáp án đúng: Có tốc độ tính toán chậm.
Câu 80: Hoạt động của RSA gồm có bao nhiêu bước	Đáp án đúng: 4
Câu 81: Hệ mật mã dựa trên bài Logarit rời rạc là	Đáp án đúng: Hệ mật mã ElGamal
Câu 82: Hệ mật mã dựa cấu trúc đại số của các đường cong trên những trường hữu hạn là	Đáp án đúng: Hệ mật mã đường cong Elliptic
Câu 83: Kích thước của MD5 là	Đáp án đúng: 128

Câu 84: SHA-1 trả lại kết quả dài bao nhiêu bit	Đáp án đúng: 160
Câu 85: Chữ ký số được xây dựng dựa trên	Đáp án đúng: Công nghệ mã hóa công khai hoặc bất đối xứng.
Câu 86: Hàm băm có độ dài biến thiên là	Đáp án đúng: HAVAL
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	Đáp án đúng: Chứng thư điện tử
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	Đáp án đúng: Tính nhận biết
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	Đáp án đúng: Tính bảo mật
Câu 90: Chuẩn mã hóa AES có kích thước dữ liệu đầu vào là?	Đáp án đúng: 128
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	Đáp án đúng: SubBytes()
Câu 92: Trong AES, hàm gì thực hiện hoán vị vòng một DoubleWord thành một DoubleWord	Đáp án đúng: RotWord()
Câu 93: Đối với AES, nếu khóa có độ dài 128 bít, giải thuật lặp bao nhiêu lần	Đáp án đúng: 10
Câu 94: Hàm ShiftRow trong AES thực hiện không dịch hàng bao nhiêu của mảng trạng thái?	Đáp án đúng: 1
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	Đáp án đúng: RSA

Câu 96: Chọn phát biểu đúng về ưu điểm của RSA	Đáp án đúng: Mã RSA có độ bảo mật cao.
Câu 97: Phát biểu nào sau đây SAI về hàm băm	Đáp án đúng: Nếu hai giá trị băm khác nhau thì chắc chắn hai khối dữ liệu tạo ra chúng là giống nhau.
Câu 98: Chọn phát biểu sai về hàm băm tốt	Đáp án đúng: Tính toán chậm.
Câu 99: Phát biểu nào sau đây là SAI về chữ ký số	Đáp án đúng: Dựa trên công nghệ khóa đối xứng.