Câu 1 Mã hóa Vigenere sẽ an toàn tuyệt đối nếu

1. Độ dài khóa tương đương độ dài văn bản
2. Độ dài khóa lớn
3. Có cửa bẫy
4. Kết hợp từ các đáp án trên //Giáo trình trang 30

Câu 2 Giải thuật Lehman có thể được áp dụng cho

1. Giải mã hệ RSA
2. Giải mã hệ El – gamal
3. Giải mã hệ mã Merkle – Hellman
4. Giải mã hệ mã ECC

Câu 3 Định lý phần dư Trung hoa dùng cho

1. Giải hệ mã RSA //Giáo trình trang 82
2. Giải hệ mã El- Gamal
3. Giải hệ mã DES
4. Giải hệ mã AES

Câu 4 Giải thuật lũy thừa nhanh được áp dụng cho

1. Hệ mã khóa công khai
2. Hệ mã khóa bí mật
3. Hệ chữ ký số
4. Hệ mã khóa công khai và chữ ký số

Câu 5 Mã Morse là

1. Mã hóa đối xứng
2. Mã hóa công khai
3. Mã hóa không sử dụng khóa
4. Một loại mã hóa nén dữ liệu

Câu 6 Theo Kirchoff thì độ an toàn của hệ mã phụ thuộc

// Theo luật Kirchoff (1835 - 1903) (một nguyên tắc cơ bản trong mã hoá) thì: toàn bộ cơ chế mã/giải mã trừ khoá là không bí mật đối với kẻ địch .

1. Khóa
2. Giải thuật mã hóa
3. Giải thuật giải mã
4. Kết hợp các đáp án trên

Câu 7 Toàn vẹn thông tin được hiểu là

1. Che giấu dữ liệu
2. Dữ liệu không sửa đổi
3. Mã hóa dữ liệu
4. Thông tin được mã hóa đối xứng

Câu 8 Các yếu tố không ảnh hưởng đến sự an toàn của một hệ mã mật

a. Phương pháp mã hóa và giải mã

b. Độ bí mật của khóa c. Độ dài bản mã d. Độ phức tạp tính toán của hệ mã

Câu 9 Mã vạch là

1. Mã hóa tượng hình
2. Mã hóa khóa đối xứng
3. Mã khối
4. Mã hoán vị

Câu 10 Ứng dụng của mật mã bao gồm

1. Bảo mật dữ liệu, xác thực toàn vẹn thông tin, chữ ký số và quản lý khóa
2. Mã hóa, toàn vẹn thông tin, sinh chữ ký số, thỏa thuận khóa
3. Bảo mật dữ liệu, xác thực thông tin, xác nhận chữ ký số, phân phối khóa
4. Mã hóa dữ liệu, tạo hàm băm, chữ ký số, quản lý khóa

Câu 11 SKC được hiểu là

1. Hệ mã khóa đối xứng
2. Hệ mã khóa dùng chung
3. Hệ mã khóa bí mật
4. Một trong những hệ mã trên

Câu 12 Theo Shannon, dư thừa từ mã khiến

1. Thông tin có thể bị giải mã
2. Bản mã độ dài lớn
3. Thuật toán không tối ưu
4. Giải mã chậm

Câu 13 *Giải thuật Lehman*

1. Đoán số là nguyên tố
2. Xác định số là nguyên tố
3. Ứng dụng các hệ mã PKC
4. Ứng dụng các hệ mã SKC

Câu 14 *Hệ mật mã có*

1. 5 bộ khác nhau
2. 4 bộ khác nhau
3. 6 bộ khác nhau
4. 3 bộ khác nhau

Câu 15 *Số nghịch đảo của số nguyên a theo đồng dư N*

1. Chỉ tồn tại theo điều kiện
2. Luôn tồn tại với mọi điều kiện
3. Là số thực
4. Là số chẵn

Câu 17 Hãy mã hóa thông điệp P = GT với khóa a=3;b=5 của hệ mã Affine //a\*x+b(x là vị trí của chữ cần mã hóa trong bảng chữ cái) =>XK

1. AN b. XK c. GA d. AJ

Câu 12 Hãy mã hóa thông điệp AB theo hệ mã Hill với khóa K = (5-10;6-13) //C=P\*K=(0;1)\* (5-10;6-13)=(6;13)=>GN

1. VN b. GN c. VD d. KT

Câu 18 Hãy tính khóa đảo trong hệ mã Hill biết khóa K = [24][13];[21][17]// Giáo trình trang 31

a. [19][1];[13][10] b. [19][13];[1][10] c. [19][10];[13][1] d. Không tính được khóa đảo.

Câu 19 Hãy mã hóa thông điệp = THITIN với hệ mã Vigenere có khóa K =TDC

1. MKKMLP
2. MKKMLX
3. MKMKLX
4. MKLKLP

Câu 20 Trong giải thuật mã khối, sử dụng bảng thế số liệu thay cho biểu thức tính toán

1. Tạo thuận tiện cho lập trình
2. Giải mã khó
3. Tăng tốc độ tính toán
4. Kết hợp các đặc điểm trên

Câu 21 Các hộp mật của giải thuật Des

1. Nhận chuỗi bít vào độ dài 48 và sinh chuỗi 32 bít ra
2. Nhận chuỗi bít vào độ dài 32 và sinh chuỗi 32 bít ra
3. Nhận chuỗi bít vào độ dài 48 và sinh chuỗi 40 bít ra
4. Nhận chuỗi bít vào độ dài 32 và sinh chuỗi 40 bít ra

Câu 23 Phát biểu nào sau là đúng cho mã hóa Affine

1. Không thay đổi tần suất bản rõ
2. Độ an toàn cao
3. Là một loại mã hóa khối
4. Là trường hợp riêng của mã hóa Vigenere

Câu 24 Khóa chủ của Aes có số lượng tùy chọn

1. 3
2. 4
3. 2
4. 1

Câu 25 Độ dài khóa của Aes

1. 128, 192, 256 bit //Giáo trình trang 57
2. 64, 128, 192 bit
3. 64, 128, 192, 256 bit
4. 128, 192, 256, 512 bit

Câu 26 Hệ mã RSA với n= 221, e=31 hãy cho biết khóa mật // thấy 17\*13=221 nên p q là 17 vs 13. Sử dụng excel theo công thức d\*e=1mod(PhiN)

1. (16, 12, 31)
2. (17, 13, 13)
3. (17, 13, 31)
4. (16, 12, 13)

Câu 27 Hệ mã RSA với n= 145, e = 9 hãy cho biết kết quả mã hóa bản rõ 15

1. 55
2. 20
3. 15
4. 25

Câu 28 Sử dụng chữ ký số lên đại diện nội dung số

1. Tăng tính bảo mật của nội dung số
2. Khiến chữ ký số giống chữ ký tay
3. Tạo và xác nhận chữ ký nhanh chóng
4. Tăng tính bảo mật của chữ ký số trên nội dung số

Câu 29 *Hệ thống phân phối khóa Blom trường hợp đơn giản chỉ an toàn cho nhóm có tối đa*

1. 3 thành viên
2. 4 thành viên
3. 2 thành viên
4. Không giới hạn thành viên

Câu 20 *Chứng chỉ khóa công khai có mô tả*

1. Khóa, giải thuật băm và xác nhận chữ ký
2. Khóa, giải thuật mã hóa và giải mã văn bản
3. Khóa và giải thuật xác nhận chữ ký
4. Khóa và giải thuật mã hóa văn bản