QUIZIZZ bảng tính

ATBMHTTT_PTIT_Chương 3 (Mã Hóa)
Tổng số câu hỏi: 39
Thời gian làm bài: 20phút
Tên người hướng dẫn: Ngọ Văn Trọng

Tên
Lớp học
Ngày

1. Đâu là một phương pháp mã hóa

a) OR
b) AND
c) XOR
d) NOT

2. Một trong các điểm yếu của các hệ mã hóa khóa công khai là

a) Khó cài đặt trên thực tế.
b) Độ an toàn thấp
c) Khó khăn trong quản lý và phân phối khóa.
d) Chi phí tính toán lớn
e) Tốc độ chậm

3. Điểm khác nhau chính giữa hai loại hàm băm MDC và MAC là

a) MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa.
b) MDC có khả năng chống đụng độ cao hơn MAC
c) MAC an toàn hơn MDC
d) MDC an toàn hơn MAC.

4. Kích thước khóa hiệu dụng của hệ mã hóa DES là

a) 128 bít
b) 64 bít
c) 56 bít
d) 48 bít

5. Đâu là một chế độ hoạt động (Modes of Operation) của mã hóa khối?

a) ECC
b) ECB
c) EBC
d) EEC

6. Một trong các ứng dụng phổ biến của các hàm băm 1 chiều là:

a) Mã hóa thẻ tín dụng
b) Mã hóa tên tài khoản
c) Mã hóa mật khẩu
d) Mã hóa địa chỉ

7. Tìm phát biểu đúng về mã hóa khóa bất đổi xứng (Asymmetric key cryptography):

a) Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã
b) Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã.
c) Chỉ sử dụng kỹ thuật mã hóa khối
d) An toàn hơn khóa bí mật.

8. Giải thuật mã hóa AES vận hàng dựa trên một ma trận 4*4, được gọi là:

a) Status
b) States
c) State
d) Stock

9. Các hộp thay thế S-Box trong giải thuật DES có số bít đầu vào và đầu ra tương ứng là:

a) Vào 4 bít, ra 4 bít.
b) Vào 8 bit, ra 6 bít
c) Vào 6 bít, ra 4 bít
d) Vào 6 bít, ra 6 bít

10. Hai thuộc tính cơ bản và quan trọng nhất của một hàm băm là:

a) Nén và dễ tính toán.
b) Nén và một chiều
c) Một chiều và đầu ra cố định
d) Dễ tính toán và đầu ra cố định

11. Trật tự các khâu xử lý trong các vòng lặp chính của giải thuật mã hóa AES

a) SubBytes, MixColumns, ShiftRows, AddRoundKey
b) AddRoundKey, MixColumns, ShiftRows, SubBytes
c) AddRoundKey, MixColumns, SubBytes, ShiftRows
d) SubBytes, ShiftRows, MixColumns, AddRoundKey

12. Số lượng vòng lặp chính thực hiện xáo trộn dữ liệu theo hàm Feistel (F) trong giải thuật DES là:

a) 20
b) 14
c) 16
d) 18

13. Trong hệ mã hóa RSA, quan hệ toán học giữa khóa riêng d và khóa công khai e là:

a) d và e là hai số nguyên tố cùng nhau
b) d và e không có quan hệ với nhau.
c) d là modulo nghịch đảo của e
d) d là modulo của e

14. Số vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã của giải thuật mã hóa AES với khóa 192 bít là:

a) 12
b) 16
c) 14
d) 10

15. Các giải thuật mã hóa khóa đối xứng thông dụng gồm:

a) DES, 3DES, RSA
b) DES, 3DES, AES
c) DES, RSA, RC4
d) DES, AES, PGP

16. Trong quá trình xử lý thông điệp đầu vào tạo chuỗi băm, số lượng vòng xử lý của hàm băm SHA1 là:

a) 60
b) 80
c) 70
d) 90

17. Một trong các điểm yếu của các hệ mã hóa khóa đối xứng là:

a) Độ phức tạp của giải thuật RSA
b) Khó khăn trong cài đặt và triển khai hệ thống.
c) Khó khăn trong quản lý và phân phối khóa.
d) Độ an toàn thấp

18. Độ an toàn của giải thuật RSA dựa trên

a) Tính khó của việc phân tích số nguyên lớn.
b) Chi phí tính toán lớn
c) Khóa có kích thước lớn
d) Độ phức tập của giải thuật RSA

19. Đâu là một ứng dụng của mã hóa.

a) PGP
b) PPG
c) GPP
d) PGG

20. Giải thuật mã hóa AES được thiết kế dựa trên:

a) Mạng hoán vị - vernam
b) Mạng Feistel
c) Mạng XOR-thay thế
d) Mạng hoán vị-XOR
e) Mạng hoán vị-thay thế (SPN)

21. Trong hệ mật mã RSA, quan hệ toán học giữa khóa công khai e và số Phi(n) là:

a) E và Phi(n) không có quan hệ với nhau
b) Phi(n) là modulo của e
c) e và Phi(n) là hai số nguyên tố cùng nhau
d) Phi(n) là modulo nghịch đảo của e

22. Kích thức khối dữ liệu xử lý của giải thuật mã hóa AES là

a) 64
b) 192
c) 160
d) 128

23. Đâu là một chế độ hoạt động (Modes of Operation) của mã hóa khối

a) CBB
b) CCB
c) CBC
d) BCC

24. Phần xử lý chính của SHA1 làm việc trên một chuỗi được gọi là state là:

a) 180
b) 160
c) 170
d) 150

25. Một hệ mã hóa (cryptosystem) được cấu thành từ hai thành phần chính gồm:

a) Giải thuật mã hóa và ký số
b) Phương pháp mã hóa và chia khối
c) Phương pháp mã hóa và không gian khóa
d) Giải thuật mã hóa và giải mã

26. Số lượng thao tác trong mỗi vòng xử lý của hàm băm MD5 là

a) 18
b) 12
c) 14
d) 16

27. Một trong các ứng dụng phổ biến của các hàm băm là để tạo chuỗi...

a) CheckTotal
b) CheckNum
c) CheckSum
d) CheckError

28. Trong mã hóa dòng (stream cipher), dữ liệu được xử lý theo...

a) Từng chuỗi ký tự
b) Từng Byte
c) Từng bit hoặc từng byte/ ký tự
d) Từng bít

29. Khi sinh cặp khóa RSA, các số nguyên tố p và q nên được chọn với kích thước:

a) Bằng khoảng 1 nửa kích thước của N (Tính theo bit)
b) Q càng lớn càng tốt
c) Không có yêu cầu về kích thước của p và q
d) P càng lớn càng tốt

30. Giải thuật mã hóa DES được thiết kế dựa trên:

a) Mạng hoán vị - vernam
b) Mạng hoán vị-thay thế (SPN)
c) Mạng hoán vị-XOR
d) Mạng XOR-thay thế
e) Mạng Feistel

31. Phần xử lý chính của MD5 làm việc trên một chuỗi được gọi là state là:

a) 96
b) 128
c) 160
d) 192

32. Liệt kê các chế độ hoạt động của mã hóa khối :

a) CCB
b) CBC
c) CFB
d) ECB
e) OFB

33. Các hàm băm (Hash functions) là các thuật toán để tạo các bản tóm tắt của thông điệp được sử dụng để ... tính toàn vẹn của thông điệp

a) Chứng thực và Đảm bảo
b) Nhận dạng và Đảm bảo
c) Tính toán và Công nhận
d) Xác thực và Công nhận

34. Kích thước khóa đầu vào của hệ mã hóa DES là

a) 48 bít
b) 56 bít
c) 64 bít
d) 128 bít

35. Trong hàm F của mô hình Fiestel trong DES gồm bao nhiêu bước :

a) 5
b) 3
c) 2
d) 4

36. Trong hàm F của mô hình Fiestel trong DES có thứ tự các bước như thế nào:

a) Expansion,XOR,Substitution,Permutation
b) Substitution,XOR,Expansion,Permutation
c) Permutation,Substitution,XOR,Expansion
d) XOR,Expansion,Substitution,Permutation

37. Quá trình sinh khóa của DES có quay trái bao nhiêu vòng và mỗi vòng quay trái mấy bit ?

a) 16 vòng , 1 hoặc 3 bit
b) 16 vòng , 2 bit
c) 16 vòng , 1 hoặc 2 bit
d) 16 vòng , 1 bit

38. MD5 và SHA1 : Thông điệp phải chia thành các khối ... bit

a) 256
b) 512
c) 1024
d) 128

39. MD5 làm việc trên state ... bit

a) 160
b) 128
c) 192
d) 96

Phím trả lời

1. c) XOR
2. e) Tốc độ chậm
3. a) MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa.
4. c) 56 bít
5. b) ECB
6. c) Mã hóa mật khẩu
7. b) Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã.
8. c) State
9. c) Vào 6 bít, ra 4 bít
10. a) Nén và dễ tính toán.
11. d) SubBytes, ShiftRows, MixColumns, AddRoundKey
12. c) 16
13. c) d là modulo nghịch đảo của e
14. a) 12
15. b) DES, 3DES, AES
16. b) 80
17. c) Khó khăn trong quản lý và phân phối khóa.
18. a) Tính khó của việc phân tích số nguyên lớn.
19. a) PGP
20. e) Mạng hoán vị-thay thế (SPN)
21. c) e và Phi(n) là hai số nguyên tố cùng nhau
22. d) 128
23. c) CBC
24. b) 160
25. c) Phương pháp mã hóa và không gian khóa
26. d) 16
27. c) CheckSum
28. c) Từng bit hoặc từng byte/ ký tự
29. a) Bằng khoảng 1 nửa kích thước của N (Tính theo bit)
30. e) Mạng Feistel
31. b) 128
32. d) ECB , CBC , CFB , OFB b) c) e)
33. b) Nhận dạng và Đảm bảo
34. c) 64 bít
35. d) 4
36. a) Expansion,XOR,Substitution,Per
37. c) 16 vòng , 1 hoặc 2 bit
38. b) 512
39. b) 128