QUIZIZZ

NAME : _____

CLASS : _____

CSATTT-C4
29 Questions

DATE : _____

1. Đâu là một phương pháp mã hóa

A AND

B NOT

C OR

D XOR

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

A Độ an toàn thấp

B Khó khăn trong quản lý và phân phối khóa.

C Khó cài đặt trên thực tế.

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 MAC an toàn hơn MDC

B MDC có khả năng chống đụng độ cao hơn MAC

C MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa.

D MDC an toàn hơn MAC.

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

A 64 bít

B 48 bít

C 128 bít

D 56 bít

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

A EBC

B EEC

C ECC

D ECB

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

A Mã hóa tên tài khoản

B Mã hóa mật khẩu

C Mã hóa thẻ tín dụng

D Mã hóa địa chỉ

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

A An toàn hơn khóa bí mật.

B Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã

C Chỉ sử dụng kỹ thuật mã hóa khối

D Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã.

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 8 bit, ra 6 bít

B Vào 6 bít, ra 4 bít

C Vào 6 bít, ra 6 bít

D Vào 4 bít, ra 4 bít.

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

A Một chiều và đầu ra cố định

B Dễ tính toán và đầ
u ra cố định

C Nén và một chiều

D Nén và dễ tính toán.

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

A AddRoundKey, MixColumns, ShiftRows, SubBytes

B SubBytes, MixColumns, ShiftRows, AddRoundKey

C SubBytes, ShiftRows, MixColumns, AddRoundKey

D AddRoundKey, MixColumns, SubBytes, ShiftRows

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

A 16
B 18
C 20
D 14

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

A d là modulo nghịch đảo của e
B d và e là hai số nguyên tố cùng nhau
C d là modulo của e
D d và e không có quan hệ với nhau.

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 14
C 16
D 10

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

A DES, 3DES, RSA
B DES, AES, PGP
C DES, 3DES, AES
D DES, RSA, RC4

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

A 70
B 90
C 80
D 60

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

A Khó khăn trong cài đặt và triển khai hệ thống.
B Độ an toàn thấp
C Khó khăn trong quản lý và phân phối khóa.
D Độ phức tạp của giải thuật RSA

18. Độ an toàn của giải thuật RSA dựa trên

A Khóa có kích thước lớn
B Chi phí tính toán lớn
C Tính khó của việc phân tích số nguyên lớn.
D Độ phức tập của giải thuật RSA

19. Đâu là một ứng dụng của mã hóa.

A PGP
B PPG
C PGG
D GPP

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

A Mạng hoán vị-XOR
B Mạng XOR-thay thế
C Mạng hoán vị-thay thế (SPN)
D Mạng hoán vị - vernam
E Mạng Feistel

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) là hai số nguyên tố cùng nhau
B Phi(n) là modulo của e
C Phi(n) là modulo nghịch đảo của e
D E và Phi(n) không có quan hệ với nhau

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

A 128
B 160
C 64
D 192

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

A CBC
B CCB
C CBB
D BCC

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

A 160
B 150
C 170
D 180

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

A Phương pháp mã hóa và chia khối

B Giải thuật mã hóa và ký số

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 16

B 18

C 12

D 14

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

A checkError

B CheckNum

C CheckSum

D CheckTotal

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

A Từng bit hoặc từng byte/ ký tự

B Từng chuỗi ký tự

C Từng bít

D Từng Byte

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

A Q càng lớn càng tốt

B Bằng khoảng 1 nửa kích thước của N (Tính theo bit)

C P càng lớn càng tốt

D Không có yêu cầu về kích thước của p và q

Answer Key

1. d	2. e	3. c	4. d
5. d	6. b	7. d	8. c
9. b	10. d	11. c	12. a
13. a	14. a	15. c	16. c
17. c	18. c	19. a	20. c
21. a	22. a	23. a	24. a
25. c	26. a	27. c	28. a
29. b			