TRƯỜNG ĐẠI HỌC MỞ TP.HCM

KHOA CÔNG NGHỆ THÔNG TIN

ĐỀ THI CUỐI KỲ:

AN TOÀN HỆ THỐNG THÔNG TIN

Thời gian làm bài : 90’

(Giám thị thu lại đề)

Đề thi gồm 06 trang (được sử dụng tài liệu giấy)

ĐỀ 2

Hệ chính quy. Nhóm lớp TK73

Mỗi câu trả lời đúng: 0,25đ

Câu 1. Cho bản mã “AVKRMNVBOT” khóa k= 25. Khi giải mã bản mã trên với khóa k theo hệ mã Caesar ta sẽ thu được bản rõ nào sau đây ?

A) BWLSNOWCPV
B) BWLSNOWCLU
C) BWLSNOWGPU
D) BWLSNOWCPU

Câu 2. Cho bản rõ “OUTEACHER” khóa k= (25,59). Khi mã hóa bản rõ với khóa k theo hệ mã Affine ta sẽ thu được bản mã nào sau đây?

A) TNODHFADQ
B) TNODHFADP
C) TNODHFACQ
D) TNODHFEDQ

Câu 3. Cho bản rõ “KHOAHOCPHOTHONG” khóa k là:

19 3
5 24

Khi mã hóa bản rõ với khóa k theo hệ mã Hill ta sẽ thu được bản mã nào sau đây? Biết hàm mã y=kx

A) DKGSTHFGTGSDTSHG
B) DKGSUHFGTHSDTSHG
C) DKGSTHFGTHSDTSHG
D) DKHSTHFGTHSDTSHG

Câu 4. Cho bản rõ “GOODEVENING” khóa k= 25. Khi mã hóa bản rõ với khóa k theo hệ mã Caesar ta sẽ thu được bản mã nào sau đây?

A) FNNCDUDMHME
B) FNNCDUDMHMF
C) FNNCDUDMHNF
D) FNNCDUDNHMF

Câu 5. Cho bản mã “RJMNXOZPBLYKQ” khóa k là “KEY”. Khi giải mã bản mã trên với khóa k theo hệ mã Vigenere ta sẽ thu được bản rõ nào sau đây?

A) HFODTQPLDBVMG
B) HFODTQPLDBUMG
C) HFODTQPLDBUMH
D) HFODTQPLDBUNG

Câu 6. Cho bản rõ "TRUONGDAIHOCMO" khóa k là "TRUONG". Khi mã hóa bản rõ với khóa k theo hệ mã Vigenere ta sẽ thu được bản mã nào sau đây?

A) MIOCAMWRCVBIEF
B) MIOCAMWRCVBIFF
C) MIOCAMWRCVBJFF
D) MIOCBMWRCVBIFF

Câu 7. Cho bản rõ x = 59, khóa công khai n = 437, e = 37. Khi mã hóa bản rõ x với khóa trên theo hệ mã RSA ta sẽ thu được bản mã nào sau đây?

A) 362
B) 633
C) 363
D) 262

Câu 8. Cho bản mã y = 269, khóa riêng là p =31, q= 29, e =47. Khi giải mã bản mã y theo hệ RSA ta sẽ thu được bản rõ nào sau đây ?

A) 85
B) 58
C) 48
D) 84

Câu 9. Người A chọn các thông số p =31, q =19, e = 41. Hỏi cặp khóa riêng của A là gì?

A) 41,589
B) 41,461
C) 41,540
D) 461,589

Câu 10. Cho bản mã "AZTIVXFP" khóa k= (19,29). Khi giải mã bản mã với khóa k theo hệ mã Affine ta sẽ thu được bản rõ nào sau đây?

A) TIUDQMWB
B) TIUDQMQC
C) TIUDQMWC
D) TIUDQNWC

Câu 11. Cho bản mã "QGYPRPCM" khóa k là ma trận cấp 2 sau:

8 3
5 3

Khi giải mã bản mã với khóa k theo hệ mã hill ta sẽ thu được bản rõ nào sau đây? Biết hàm mã hóa y=kx

A) MIDASBOY
B) MIDASBAY
C) MIDASBOT
D) MIDASBET

Câu 12. Cho bản rõ "TRUONGDAIHOC" khóa k là:

9 7
3 4

A) OTOOFLBVQGCC
B) OTOOELBVPGCC
C) OTOOFLBVPGOC
D) OTOOFLBVPGCC

Khi mã hóa bản rõ với khóa k theo hệ mã Hill ta sẽ thu được bản mã nào sau đây? Biết hàm mã hóa y=xk

Câu 13. Theo thuật mã Diffie-Hellman, giả sử 2 người A,B chọn 2 số nguyên tố chung là g = 10 , p = 541, với a= 39, b=91 . Chọn khóa công khai của người gửi và người nhận A,B & khóa riêng của người A ?

A) (541,10,288,253) & (39,288)
B) (541,10,39,253) & (39,288)
C) (541,10,253,333) & (39,288)
D) (541,10, 91,253) & (39,288)

Câu 14. Cho bản mã "GDYDEC" khóa k là ma trận cấp 2 sau:

6 5
3 3

Khi giải mã bản mã với khóa k theo hệ mã Hill ta sẽ thu được bản rõ nào sau đây? Biết hàm mã hóa y=kx

A) BATISE
B) BATISO
C) BATISA
D) BATISU

Câu 15. Cho bản mã "YCQXDELI" khóa k= (59,47). Khi giải mã với khóa k theo hệ mã Affine ta sẽ thu được bản rõ nào sau đây?

A) TBDEQFGN
B) TBDEQFGM
C) TBDEQFHN
D) TBDEQEGN

Câu 16. Cho bản mã "PORZJBNTCNLD" khóa k là:

6 5
3 4

Khi giải mã với khóa k theo hệ mã Hill ta sẽ thu được bản rõ nào sau đây? Biết hàm mã y=kx

A) WNLLPPBRLIJH
B) WNLLPPBRLIJK
C) WNLLPPBRLFJH
D) WNLLPPBQLIJH

Câu 17. Cho bản mã "CDQARFJP" khóa k là ma trận cấp 2 sau:

5 1
9 6

Khi giải mã bản mã với khóa k theo hệ mã hill ta sẽ thu được bản rõ nào sau đây? Biết hàm mã hóa y=xk

A) DNMYZOLS
B) DNNYZOLS
C) DNMYZONS
D) DNMYZOMS

Câu 18. Theo thuật mã Diffie-Hellman, giả sử 2 người A,B chọn 2 số nguyên tố chung là g = 10 , p = 541, với a= 71, b=91 . Chọn khóa công khai của người gửi và người nhận A,B & khóa riêng của người B ?

A) (541,10,282,333) & (71,413)
B) (541,10,71,91) & (91,413)

C) (541,10,282,333) & (91,413)
D) (541,10,91,333) & (71,413)

Câu 19. Theo thuật mã Diffie-Hellman, giả sử Alice & Bob chọn 2 số nguyên tố chung là g = 2, p = 997, với a=91, b=71 . Khóa riêng của Alice là ?

A) 91,377
B) 91,60
C) 91,306
D) 91,997

Câu 20. Theo thuật mã Diffie-Hellman, giả sử Alice & Bob chọn 2 số nguyên tố chung là g = 3, p = 353, với a=79, b=51 . Khóa riêng của Alice & Bob là ?

A) (79,353) & (51,353)
B) (79,87) & (51,87)
C) (79,150) & (87,112)
D) (39,3) & (53,79)

Câu 21. So sánh tốc độ mã và giải mã của hệ mật mã công khai với mật mã bí mật hiện đại (với cùng độ dài bản rõ và độ dài khóa)?

A) Mật mã công khai chậm hơn
B) Mật mã công khai nhanh hơn
C) Tốc độ như nhau
D) Cả 3 câu trên sai

Câu 22. Độ an toàn của hệ mật phụ thuộc vào

A) Không gian khóa đủ lớn để phép vét cạn khóa là không thể thực hiện được
B) Thuật toán, không gian khóa và bản mã
C) Tính bí mật của thuật toán
D) Hàm mã là hàm một chiều

Câu 23. Mật mã là

A) Bao gồm hai quá trình mã hóa và giải mã
B) Quá trình biến đổi thông tin từ dạng đọc được sang dạng không đọc được
C) Ngành khoa học chuyên nghiên cứu các phương pháp truyền tin bí mật
D) Quá trình biến đổi từ dạng không đọc được sang đọc được

Câu 24. Xét trong bảng chữ cái tiếng Anh. Hệ mã Viginere có

A) 312 cách chọn khóa
B) 26! cách chọn khóa
C) 26^m cách chọn khóa
D) m! cách chọn khóa

Câu 25. Cho bản mã y = 269, khóa riêng là p =41, q= 29, e =47. Khi giải mã bản mã y theo hệ RSA ta sẽ thu được bản rõ nào sau đây ?

A) 589
B) 1179
C) 478
D) 85

Câu 26. Mã ms11_080 là?

A) Mã lỗi khai thác qua giao thức http, tạo backdoor qua lỗi phần mềm VLC.
B) Mã lỗi của phần mềm Acrobat Reader, thực hiện tấn công máy chủ
C) Loại mã của phương pháp mã hóa công khai
D) Mã lỗi cho phép khai thác mã từ xa, nâng cấp, chiếm quyền hệ thống.

Câu 27. Mã khóa công khai

A) B và C đúng
B) Có thể dùng khóa công khai để mã hóa
C) Dùng 1 khóa để mã hóa và 1 khóa để giải mã
D) A và B đều sai

Câu 28. Mật mã hoán vị mã từng khối

A) 1 kí tự
B) m kí tự
C) 2 kí tự
D) 26 kí tự

Câu 29. So sánh độ an toàn của các hệ mật mã công khai với mật mã bí mật hiện đại (với cùng độ dài bản rõ và độ dài khóa) ?

A) Cả hai có độ an toàn như nhau
B) Mật mã công khai an toàn hơn
C) Mật mã có khóa dài hơn thì an toàn hơn
D) Mật mã bí mật an toàn hơn

Câu 30. Câu lệnh "nmap -n -PN -sT -sU -p remote_host" được dùng khi:

A) Thực hiện quét từng port TCP,UDP
B) Thực hiện quét nhanh hệ điều hành
C) Thực hiện quét nhanh bỏ qua phân giải DNS
D) Thực hiện quét TCP không ACK

Câu 31. Hacker khai thác lỗ hổng nào để nâng cấp đặc quyền trên Windows XP, Windows 7

A) Ms08_067, Ms16_032
B) Ms10_067, Ms18_054
C) Ms10_067, Ms08_054
D) Ms02_067, Ms03_016

Câu 32. Trong mật mã, khóa công khai dùng để làm gì?

A) Kí,giải mã
B) Mã hóa, kiểm tra chữ kí
C) Chứng thực SSL/TSL
D) Giải mã

Câu 33. Chọn câu đúng

A) Chữ kí số với chữ kí điện tử là một
B) Chữ kí số là dãy số đặc biệt
C) Chữ kí số là trường hợp riêng của chữ kí điện tử, hình thành từ các thuật toán mã công khai
D) Cả 3 câu đều sai

Câu 34. Trong sơ đồ kí số thành phần nào đặc trưng xác nhận cho một người?

A) Khóa công khai
B) Bức điện tín
C) Bản mã
D) Khóa bí mật

Câu 35. Cho bản mã "MIOCAMWACSBIFF" khóa k là "MONARCHY". Khi giải mã bản mã trên với khóa k theo hệ mã Playfair ta sẽ thu được bản rõ nào sau đây?

A) AEMHNRZNHUABIVIV
B) AEMHNRZNHUACIVIV
C) AEMHMRXNBLABIVIV
D) AEMHNRXNBLABIVIU

Câu 36. Phát biểu nào sau đây là sai ? Công cụ NMAP có thể :

A) Quét và phát hiện máy chủ
B) Liệt kê các cổng được mở tre n một host
C) Kiểm tra thông tin hệ điều hành máy chủ
D) Quét & khai thác lỗi hệ điều hành máy chủ.

Câu 37. Metasploit Framework là

A) Môi trường khai thác, tấn công các lỗ hổng website
B) Môi trường dùng để kiểm tra , tấn công và khai thác lỗi
C) Môi trường dùng để dò quét thu thập thông tin, lập trình thực hiện khai thác lỗi
D) Môi trường để thực hiện các cuộc tấn công mạng

Câu 38. SQLmap là một công cụ

A) Tìm kiếm và khai thác lỗ hổng lỗ hổng hệ điều hành,máy chủ web, mạng wifi
B) Nâng cấp đặc quyền hệ thống, phá hủy dữ liệu
C) Tìm kiếm và khai thác lỗ hổng SQL injection
D) Tấn công dò tìm mật khẩu các hệ mã hóa công khai và đối xứng

Câu 39. Armitage là một công cụ

A) Tìm các lỗ hổng, khai thác lỗ hổng cơ sở dữ liệu
B) Thu thập thông tin mục tiêu. Tìm các lỗ hổng, khai thác lỗ hổng
C) Sử dụng với chức năng tương tự như công cụ Havij
D) Tìm kiếm, khai thác mã lỗi ms_1080. Tấn công DDoS mục tiêu

Câu 40. Lỗ hổng nào dưới đây hacker thực hiện tấn công chiếm quyền máy chủ Windows 2008

A) MS09_050_smb2
B) MS08_050_smb2
C) MS02_030_mtext
D) MS02_030_negotiate

---------- oOo ----------