Trắc nghiệm 54 câu

1. Mã hóa là gì ?
a) tập hợp các phương pháp và phương tiện bảo vệ thông tin khỏi việc truy cập trái phép bằng cách ẩn yếu tố tồn tại các thông tin bí mật.
b) môn khoa học về các phương thức biến đổi (mã hóa) thông tin với mục đích bảo vệ thông tin khỏi người truy cập trái phép
c) môn khoa học (và thực tế ứng dụng nó) về các phương pháp và phương thức giải mã

2. Steganography là gì ?
a) bảo vệ thông tin khỏi truy cập trái phép bằng cách ẩn đi sự tồn tại các thông tin bí mật
b) Ẩn đi nội dung của tin bằng cách mã hoá chúng
c) phạm vi kiến thức ,mà mục đích của nó là tìm kiếm và nghiên cứu các phương pháp bẻ khóa các thuật toán mã hóa ,cũng như là thủ tục bẻ khóa

3. Hệ thống mã hóa Vizhiner thuộc lớp biến đổi nào?
a) hoán vị **b) phép thế** c) Gamma Xoring d) mã hóa khối

4. Mã Sejar thuộc lớp biến đổi nào ? (Ceasar chứ ko phải Sejar)
a) phép thế b) phép hoán vị c) gama xoring

5. Mã thay thế (substitution cipher) là gì ?
a) mật mã luồng mà ở đó Gamma xoring được sử dụng để mã hóa dữ liệu ?
b) mật mã ,mà ở đó thủ tục mã hóa là sự hoán vị các phần tử của văn bản ban đầu hoặc các nhóm của chúng, bản thân các phần tử giữ nguyên không thay đổi
c) mật mã,mà ở đó các ký tự riêng rẽ của văn bản ban đầu hoặc nhóm các ký tự được thay thế bởi các ký tự hoặc nhóm các ký tự khác, trong khi giữ nguyên vị trí của mình so với các nhóm được thay thế khác

6. Mã hoá Gamma Xoring là gì?
a) mật mã luồng mà ở đó bộ cảm biến của các số giả ngẫu nhiên được sử dụng để mã hóa dữ liệu
b) mật mã mà ở đó thủ tục mã hóa là sự hoán vị các phần tử của văn bản ban đầu hoặc nhóm các phần tử ,bản than các phần tử thì không thay đổi
c) mật mã mà ở đó các ký tự riêng rẽ của văn bản ban đầu hoặc nhóm các ký tự được thay thế bởi các ký tự hoặc nhóm các ký tự khác , trong khi giữ vị trí của chúng trong văn bản so với các nhóm bị thay thế khác

7. Những thuật toán nào sau đây là thuật toán đối xứng ?
a) DES b) El-Gamal **c) RC5 d) IDEA**

8. Thuật toán nào sau đây không phải là đối xứng ?
a) DES **b) El-Gamal** c) RC5 d) IDEA

9. Chìa khóa mật trong hệ mã hoá DES có độ dài là bao nhiêu ?

a) 48 bit;
b) 64 bit; - có bạn đã trả lời rồi 56 bit để mã hóa, 8 bit để kiểm tra parity
c) 128 bit; d) 192 bit; e) 256 bit

10. Chìa khóa mật trong hệ mã hóa Rijdael có độ dài bằng bao nhiêu? (aka Advanced Encryption Standard (AES))

Key sizes	128, 192 or 256 bits[1]
Block sizes	128 bits[2]
Structure	Substitution-permutation network
Rounds	10, 12 or 14 (depending on key size)

a) 48 bit; b) 64 bit; **c) 128 bit; d) 192 bit; e) 256 bit.**

11. Thuật toán Rijndael có kiến trúc nào ?
a) mạng Filestel b) mật mã luồng (stream cipher)
c) kiến trúc SQUARE (_http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

12. Thuật toán DES có kiến trúc nào?
a) mạng Filestel b) mã luồng (stream cipher) c) kiến trúc SQUARE

13. Đặc tính đặc biệt của các thuật toán mã hóa khối là :
a) trong quá trình làm việc ,chúng biến đổi khối thông tin ban đầu có độ dài xác định và nhận được khối kết quả với độ dài bất kỳ
b) trong quá trình làm việc ,chúng biến đổi khối thông tin ban đầu với độ dài xác định và nhận được khối kết quả với độ dài tương tự
c) trong quá trình làm việc ,chúng biến đổi khối thông tin ban đầu với độ dài bất kỳ và nhận được khối kết quả với độ dài xác định

14. ECB (Electronic Code Book), CBC (Cipher Block Chaining), OFB (Output Feed Back), CFB (Cipher Feed Back) là gì?
a) là những chế độ làm việc của thuật toán DES
b) là những chế độ làm việc của thuật toán RSA
c) là những chế độ làm việc của thuật toán Rijndael

15. Cơ sở của độ bền của thuật toán RSA là?
a) sự phân tích các số lớn thành các thừa số nguyên tố (đọc lại vở ghi rất rõ)
b) tính lôgarit tại trường hữu hạn
c) tính nghiệm của các phương trình đại số

16. Cơ sở của độ bền của phương pháp Diff-Hellman là :

a) phân tích các số lớn thành các thừa số nguyên tố
b) hàm nâng lên lũy thừa rời rạc (thuật toán logarit rời rạc)
c) tính nghiệm của các phương trình đại số

17. Thành phần nào của cơ sở hạ tầng của khóa mở (PKI – Public Key Infrastructure) chịu trách nhiệm việc tạo danh sách chứng nhận bị thu hồi ?
a) trung tâm chứng nhận c) người sử dụng cuối cùng
b) trung tâm đăng ký d) cẩm nang tra cứu mạng

18. Cơ sở hạ tầng của khóa mở (Public Key Infrastructure – PKI) được sử dụng để làm gì ?
a) để điều khiển các chìa khóa mật của những thành phần tham gia tương tác
b) để điều khiển các khóa và chứng thực điện tử của những thành phần tham gia tương tác

19 – Giao thức nào được xây dựng để đảm bảo việc bảo mật cho hòm thư điện tử?
a) S/MINE - (Secure/Multipurpose Internet Mail Extensions)
b) SET
c) IPSEC

20. Giao thức nào được xây dựng để đảm bảo cho hệ thống thanh toán điện tử của ngân hàng với việc sử dụng thẻ plastic ?
a) S/MIME
b) SET - Secure Electronic transaction – Thanh toán điện tử an toàn
c) IPSEC

21. Thủ tục phân bố khóa (key) mà không yêu cầu sử dụng kênh bảo mật đối với việc truyền khóa đến người nhận là thủ tục :
a) mã hóa theo thuật toán DES
b) Diff - Hellman (mã công khai)
c) mã hóa Vizhiner

22. Thủ tục phân bố của khóa nào yêu cầu sử dụng kênh bảo mật để truyền khóa tới người nhận ?
a) thủ tục phân bố khóa đối xứng – ví dụ DES
b) thủ tục Diff-Hellman

23. Những tính chất nào là tính chất cần thiết đối với hệ thống không đối xứng bất kỳ ?
a) sự tồn tại kênh đóng để truyền các khóa(key) bí mật
b) không thể đọc thông điệp,chỉ biết khóa mở (khóa mở - public key – biết là đương nhiên, ko đọc được thì mới mật)
c) không thể tính khóa đóng theo khóa mở (tính được còn gọi gì là mật)

24. Thủ tục mã hóa nào sau đây có năng suất hơn ?
a) mã hóa không đối xứng (yêu cầu năng lực tính toán phức tạp)

b)mã hóa đối xứng

25. Hệ thống với khóa mở nào sau đây có năng suất nhất ?
a) hệ thống RSA
b) hệ thống El-Gammal
c) hệ thống trên cơ sở các đường cong êlip

26. Hệ thống với khóa mở nào sau đây được sử dụng chỉ để sinh ra chữ ký số ?
a) RSA b) Diffs-Hellman c) ECC
d) El-Gamal
e) DSS – chỉ để sinh chữ ký số nên chọn thằng này

27. Hệ thống với khóa mở nào sau đây có hiệu suất lớn nhất ?
a) những hệ thống, được xây dựng trên cơ sở phân tích các số lớn thành các thừa số nguyên tố
b) những hệ thống , được xây dựng trên cơ sở tính lôgarit rời rạc trong trường hữu hạn
c) những hệ thống, được xây dựng trên cơ sở các đường cong elip
http://www.tapchibcvt.gov.vn/News/PrintView.aspx?ID=16382

28. Những hệ thống với khóa mở nào sau đây được sử dụng để mã hóa thông tin ?
a) RSA
b) Diff-Hellman - thằng này dùng để trao đổi khóa
c) El-Gamal – thằng này chữ ký số
d) DSS – thằng này chữ ký số

29 . Thuật toán RSA thuộc dạng nào của thuật toán mã hóa (xét trên phương diện độ chắc chắn khi bị bẻ khóa) ?

a) hiển nhiên chắc chắn – hệ mật hoàn hảo
b) chắc chắn được chứng thực – độ phức tạp tính toán
c) chắc chắn giả định

30. Thuật toán Vernam (sổ ghi chép 1 lần) thuộc dạng nào của thuật toán mã hóa (xét trên phương diện độ chắc chắn khi bị bẻ khóa)?
a) hiển nhiên chắc chắn
b) chắc chắn được chứng thực
c) chắc chắn giả định (thuyết)

31. Điều gì quyết định độ tin cậy của thuật toán DES?
a) phân tích các số lớn thành các thừa số nguyên tố;
b) kích thước của khóa;
c) tính nghiệm của các phương trình đại số.

32. Cơ sở của độ chắc chắn của phương pháp El-Gamal là :
a) Sự phân tích các số lớn thành các thừa số nguyên tố
b) Tính lôgarít trong trường hữu hạn – cùng loại với Diffie-Hellman, Knapsach

c) Tính nghiệm của các phương trình đại số

33. Phương pháp nào sau đây không thể được sử dụng để mã hóa hay giải mã thông tin?
a) phương pháp BlowFich
b) phương pháp El-Gammal
c) phương pháp Diff-Hellman

34. Message digest – là …
a) kết quả của việc mã hóa;
b) kết quả của hàm hash ;
c) kết quả của việc giải mã

35. Thủ tục chứng thực (authentication) dữ liệu là gì ?
a) thủ tục kiểm tra tính toàn vẹn của dữ liệu
b) thủ tục kiểm tra tính đúng đắn của dữ liệu và các chủ thể tương tác thông tin
c) thủ tục đảm bảo việc bảo vệ dữ liệu khỏi việc truy cập trái phép

36. Chữ ký điện tử (số) là :
a) các đặc tính của mật mã, được sử dụng để biến đổi mã hóa thông tin
b) họ tên người gửi được ghi ở dạng điện tử và kết nối với thông tin
c) biến đổi mã hóa văn bản được gắn vào văn bản cho phép người nhận khác kiểm tra tác giả và tính đích thực của thông tin

37. Kết quả của phép tính hàm hash theo thuật toán MD5 bằng bao nhiêu ?
a) 64 bit **b) 128 bit** c) 160 bit d) 256 bit

38. Hàm hash là gì ?
a) là sự biến đổi, nhận giá trị nào đó có độ dài bất kỳ từ dữ liệu có độ dài cố định
b) là sự biến đổi, nhận giá trị nào đó có độ dài cố định từ dữ liệu có độ dài bất kỳ
c) là sự biến đổi, nhận các giá trị khác có độ dài bất kỳ từ dữ liệu có độ dài bất kỳ

39. Hàm hash 1 phía là gì ?
a) hàm hash, khó tính theo hướng thuận và dễ tính theo hướng ngược
b) hàm hash , dễ tính theo hướng thuận và hướng ngược
c) hàm hash, về mặt tính toán là hàm không thuận nghịch -
kythuatmatma.com/lythuyet/congkhai/1002_ham1chieu.php

40. Kết quả của phép tính hàm hash theo thuật toán SHA-1 là?
a) 64 bit b) 128 bit **c) 160 bit** d) 256 bit

Input: Đầu vào message có độ dài < 2^{64}, chia thành các block có size 512 bit
Output: 1 digest có độ dài 160 bit
Bảo mật:

- Ko tính ra được thông điệp với 1 digest đã cho
- Ko có 2 message tạo ra cùng 1 digest

41. Mã nào sau đây là mã không đối xứng?
a) DES (Data Encryption Standart)
b) RSA (Rivest-Shamir-Alderman)
c) El Gamal
42. Những mã nào sau đây là đối xứng?
a) DES (Data Encryption Standart)
c) chuẩn 28147-89 – hay là GOST (block cipher)
b) RSA (Rivest-Shamir-Alderman) d) El Gamal

43. Những thuật toán nào được sử dụng để tính toán digest thông tin ?
a) DES
b) MD5 V c) SHA-1 - xem câu 34
d) RSA

44. Những thuật toán nào sau đây không được sử dụng để tính toán digest thông tin?
a) DES b) MD5 c) SHA-1 **d) RSA**

45. Khi nào thì cần đưa tường lửa vào trong thành phần trang thiết bị của cơ quan
a) khi liên kết nguồn tính toán của cơ quan vào mạng nội bộ
b) khi mua hệ thống phòng chống virus
c) khi thường xuyên kết nối thẳng từ mạng nội bộ ra mạng internet

46. Những nguy cơ nào yêu cầu đưa tường lửa vào thành phần trang thiết bị cuả cơ quan
a) những nguy cơ xâm nhập trái phép vào mạng nội bộ từ mạng bên ngoài
b) những nguy cơ truy cập trái phép vào mạng bên ngoài từ mạng bên trong
c) những nguy cơ xuất hiện lỗi của người sử dụng ,người điều phối và người quản lý

47. Tường lửa thực hiện những chức năng nào sau đây ?
a) chức năng lọc những luồng thông tin đi qua
b) chức năng trung gian khi thực hiện các tương tác giữa các mạng
c) (hàm) chức năng biến đổi mã hóa các luồng thông tin

48. Những biến đổi mã hóa nào sau đây được sử dụng để mã hóa thông tin khi xây dựng " phong bì điện tử "?
a) các thuật toán mã hóa đối xứng
b) các thuật toán mã hóa không đối xứng

49. Việc bảo vệ thông tin trong quá trình truyền theo kênh liên kết mở được xây dựng trên cơ sở thực hiện :
a) (hàm) các chức năng bảo vệ mã hóa của dữ liệu được truyền
b) (hàm) các chức năng bảo vệ việc kết nối mạng nội bộ hoặc các máy tính cá nhân tới kênh công cộng khỏi các tác động trái phép từ môi trường bên ngoài

50. Mạng riêng ảo (VPN) thực hiện những bài toán nào sau đây ?
a) bảo vệ những mạng nội bộ và các máy tính cá nhân có kết nối tới kênh công cộng khỏi các tác động trái phép từ môi trường bên ngoài
b) bảo vệ thông tin trong quá trình truyền theo các kênh liên lạc mở

51. "Chương trình cài vào " là gì ?
a) là chương trình được xây dựng để tự động thực hiện các tác động trái phép
b) là chương trình dùng để bảo vệ bằng mã hóa dữ liệu khỏi sự truy cập trái phép

52. "Chương trình cài vào " được cài vào bởi các công cụ phần cứng như thế nào?
a) bởi các chương trình bị lây nhiễm dạng bất kỳ theo công nghệ virus
b) bằng cách lây nhiễm của các chương trình chứa trong các công cụ phần cứng, ví dụ các chương trình của vi mạch BIOS …

53. Giải mã là :
a) tập hợp các phương pháp và môi trường để khôi phục lại các thông tin đã bị mã hóa trở lại dạng ban đầu mà không cần khóa cần thiết.
b) khôi phục các thông tin đã bị mã hóa lại dạng ban đầu với sự giúp đỡ của khóa tương ứng.

54. Phân tích mã là:
a) Tập hợp các phương pháp và công cụ để thực hiện việc giải mã thông tin mà không cần có chìa khóa cần thiết
b) khôi phục thông tin lại mẫu ban đầu với sự giúp đỡ của khóa tương ứng

55. Lọc các luồng thông tin bởi tường lửa là :
a) lọc lượng thông tin cho thông tin qua tường bảo vệ có chọn lọc kèm theo thực hiện 1 vài sự biến đổi.
b) lọc lượng thông tin (có trong dữ liệu) là biến đổi mã hóa dữ liệu đi qua tường lửa.