

Câu hỏi 1

Đoạn văn câu hỏi

Áp dụng IPSec vào hệ thống VPN, phương thức chứng thực được hỗ trợ sẵn trong dịch vụ RRAS của Windows là:

Select one:

- a. Certified Authentication (CA)
- b. Internet Key Exchange (IKE)
- c. Kerberos
- d. Encapsulating Security Payload (ESP)

Câu hỏi 2

Đoạn văn câu hỏi

Mật mã hoán vị là (chọn nhiều)

Select one or more:

- Mã thay thế đơn biểu
- Mã khối
- Mã thay thế đa biểu
- Mã dòng

Câu hỏi 3

Đoạn văn câu hỏi

Hàm phi Ole của n là

Select one:

- Số các số nguyên nhỏ hơn n
- Số các số nguyên tố nhỏ hơn n
- Số các số nguyên tố cùng nhau với n
- Số các số nguyên tố cùng nhau với n và nhỏ hơn n

Câu hỏi 4

Đoạn văn câu hỏi

Mật mã dịch vòng mã từng khối bao nhiêu ký tự ?

Select one:

- 1 ký tự
- 26 ký tự
- m ký tự

2 kí tự

Câu hỏi 5

Đoạn văn câu hỏi

Quyền truy cập nào cho phép ta lưu giữ một tập tin?

Select one:

- Ghi
- Backup
- Sao chép
- Đọc

Câu hỏi 6

Đoạn văn câu hỏi

Chữ ký số được sử dụng cho mục đích gì?

Select one:

- a. Để bảo mật tài liệu sao cho người ngoài không đọc được
- b. Thu hồi một chứng chỉ
- c. Cung cấp chứng chỉ
- d. Để kiểm tra định danh người gửi

Câu hỏi 7

Đoạn văn câu hỏi

Virus không thể ẩn mình vào đâu ?

Select one:

- A. Process
- B. CMOS
- C. DLL
- D. BIOS

Câu hỏi 8

Đoạn văn câu hỏi

Trojan là một phương thức tấn công kiểu:

Select one:

- A. Can thiệp trực tiếp vào máy nạn nhân để lấy các thông tin quan trọng
- B. Đánh cắp dữ liệu của nạn nhân truyền trên mạng
- C. Tấn công làm tê liệt hệ thống mạng của nạn nhân
- D. Điều khiển máy tính nạn nhân từ xa thông qua phần mềm cài sẵn trong máy nạn nhân

Câu hỏi 9

Đoạn văn câu hỏi

Cho bản mã “SAGNK” khóa k= 6. Khi giải mã bản mã với khóa k theo hệ mã **dịch vòng** ta sẽ thu được bản rõ nào sau đây?

Select one:

- muahé
- muaha
- muaxu
- muica

Câu hỏi 10

Đoạn văn câu hỏi

Mục nào không là tấn công chủ động

Select one:

- A. Tấn công nghe lén
- B. Tấn công replay
- C. Tấn công từ chối dịch vụ
- D. Tấn công giả mạo (masquerade)

Câu hỏi 11

Đoạn văn câu hỏi

Virus máy tính là gì ? (chọn nhiều)

Select one or more:

- A. phần mềm độc hại , nó là một loại phần mềm hệ thống do các tin tặc hoặc những người thích đùa tạo ra nhằm gây hại cho máy tính
- B. Một chương trình hay đoạn chương trình có khả năng tự nhân bản hay sao chép chính nó từ đối tượng lây nhiễm này sang đối tượng khác
- C. nó sẽ gây ra lỗi thi hành, lệch lạc hay hủy dữ liệu.
- D. Một loại bệnh có thể lây lan cho con người khi truy cập Internet

Câu hỏi 12

Đoạn văn câu hỏi

Chọn câu đúng

Select one:

- Chữ ký số là trường hợp riêng của chữ ký điện tử, được hình thành từ các thuật toán mã công khai
- Chữ ký số với chữ ký điện tử là một

- Chữ ký số là dãy số đặc biệt
- Chữ ký số để ký các văn bản số

Câu hỏi 13

Đoạn văn câu hỏi

Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước kí sau. Người A có khóa $(p,q,e) = (17,3,5)$; Người B có khóa $(p,q,e) = (11,5,13)$. A mã bản tin $m = 10$ gửi cho B. Hỏi A sử dụng khóa nào để mã?

Select one:

- (13,55)
- (5,51)
- 55
- 52

Câu hỏi 14

Đoạn văn câu hỏi

cho bản mã “EC” khóa k là:

83

73

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 $y=kx$

Select one:

- yn
- oy
- cw
- om

Câu hỏi 15

Đoạn văn câu hỏi

Cho bản mã “ECLYR” khóa $k=11$. Khi giải mã bản mã với khóa k theo hệ mã **dịch vòng** ta sẽ thu được bản rõ nào sau đây?

Select one:

- trung
- trong
- trang
- thong

Câu hỏi 16

Đoạn văn câu hỏi

System Hacking là một phương thức tấn công kiểu:

Select one:

- A. Điều khiển máy tính nạn nhân từ xa
- B. Can thiệp trực tiếp vào máy nạn nhân để lấy các thông tin quan trọng
- C. Tấn công làm tê liệt hệ thống mạng của nạn nhân
- D. Đánh cắp dữ liệu của nạn nhân truyền trên mạng

Câu hỏi 17

Đoạn văn câu hỏi

cho bản rõ “**xinh**” khóa k=9. Khi mã hóa bản rõ với khóa k theo hệ mã dịch vòng ta sẽ thu được bản mã nào sau đây?

Select one:

- a. GRWQ
- b. OHTM
- c. GEVT
- d. GHVO

Câu hỏi 18

Đoạn văn câu hỏi

cho bản mã “IB” khóa k là:

75

54

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 $y=kx$

Select one:

- a. jp
- b. ji
- c. jk
- d. bp

Câu hỏi 19

Đoạn văn câu hỏi

Quá trình tạo khóa của hệ mật RSA như sau :

- Chọn p, q là hai số nguyên tố lớn khác nhau
- Tính $n=p*q$, $f(n)=(p-1)*(q-1)$
- Chọn e sao cho : $1 < e < f(n)$, e và f(n) là 2 số nguyên tố cùng nhau

- Tính $d = e^{-1} \text{mod } f(n)$

Khóa bí mật của hệ mật này là gì ?

Select one:

- A. $f(n), p, q, d$
- B. $f(n), p, q$
- C. p, q, d
- D. d

Câu hỏi 20

Đoạn văn câu hỏi

Cho hoán vị

12345

13452

Khi mã hóa bản rõ “**clock**” theo mã hoán vị ta sẽ thu được bản mã nào sau đây ?

Select one:

- COCKF
- COCKJ
- COCKH
- COCKL

Câu hỏi 21

Đoạn văn câu hỏi

Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước kí sau. Người A có khóa $(p, q, e) = (17, 7, 5)$; Người B có khóa $(p, q, e) = (11, 5, 3)$. A giải mã bản mã $y = 15$ bằng khóa nào?

Select one:

- 77
- 5
- 27
- 17

Câu hỏi 22

Đoạn văn câu hỏi

cho bản mã “MS” khóa k là:

72

33

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 $y = kx$

Select one:

- ag
- se
- sa
- si

Câu hỏi 23

Đoạn văn câu hỏi

Cho hoán vị

12345

52413

Khi mã hóa bản rõ “plain” theo mã hoán vị ta sẽ thu được bản mã nào sau đây ?

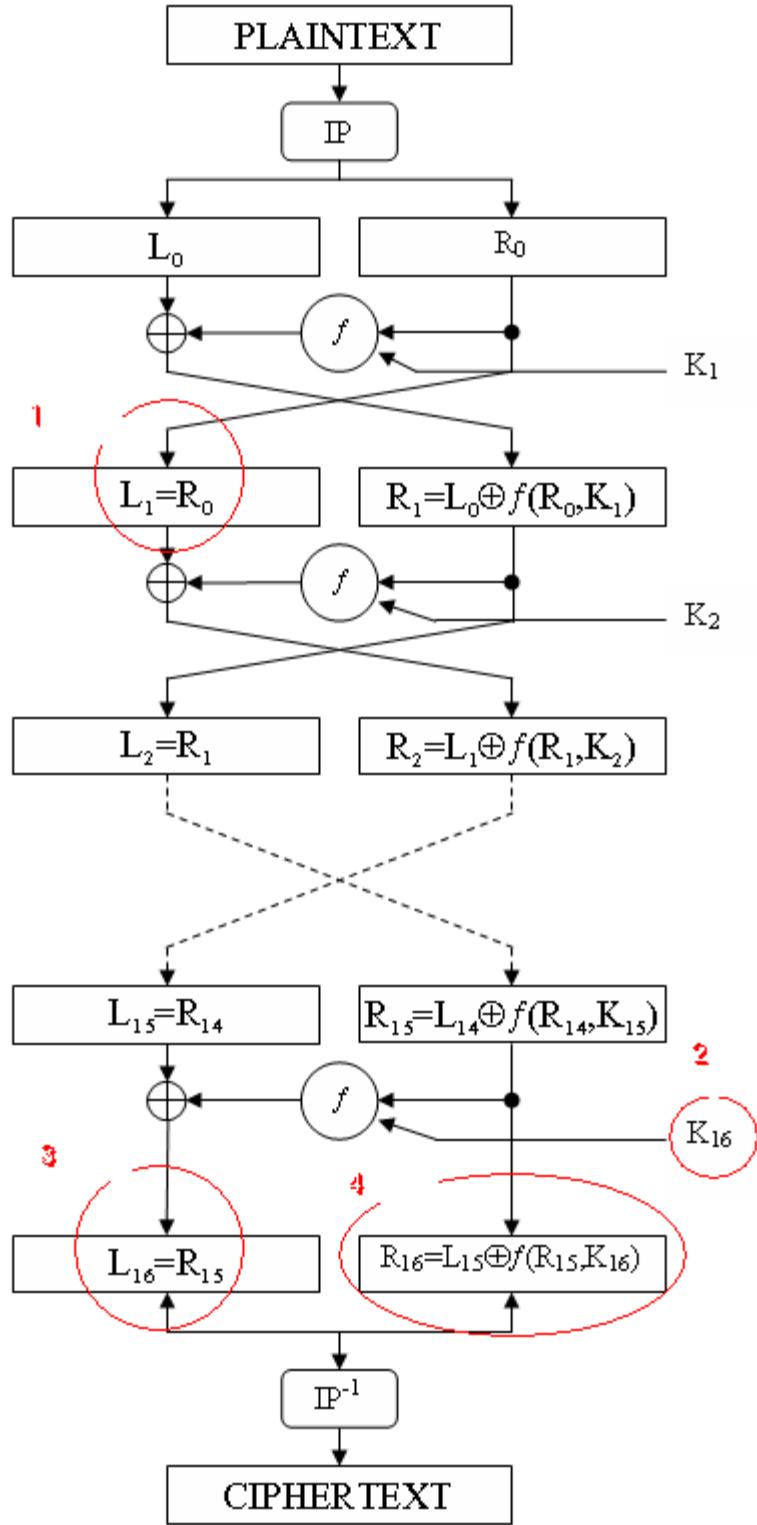
Select one:

- NLIPA
- NKLJG
- NLIPD
- NIJKB

Câu hỏi 24

Đoạn văn câu hỏi

Cho sơ đồ thể hiện giải thuật mã hóa DES như sau:



Sơ đồ mã DES

Trong sơ đồ có phần chưa chính xác, đó là phần nào trong các điểm được đánh dấu sau:

Select one:

- 3,4
- 1
- 3
- 1,2

Câu hỏi 25

Đoạn văn câu hỏi

Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước kí sau. Người A có khóa $(p,q,e) = (17,3,5)$; Người B có khóa $(p,q,e) = (11,5,13)$. B kí lên bức điện $x=10$ bằng khóa nào sau đây?

Select one:

- 5
- 37
- 13
- 23

Câu hỏi 26

Đoạn văn câu hỏi

Để ngăn tấn công DoS, một quản trị mạng chặn nguồn IP với tường lửa, nhưng tấn công vẫn tiếp diễn. Điều gì có khả năng xảy ra nhất ?

Select one:

- Máy đích bị virus
- Tường lửa chưa hiệu quả
- Sâu DoS đã lây nhiễm cục bộ
- Hệ thống mạng bị lỗi

Câu hỏi 27

Đoạn văn câu hỏi

Một IP flood theo các host phát tán trực tiếp đến một Web server là một ví dụ của loại tấn công gì ?

Select one:

- Trojan Horse
- DDOS
- Tràn IP
- Ipsec

Câu hỏi 28

Đoạn văn câu hỏi

Cho mật mã Affine. $K=(a,b)$ là khóa của hệ mật mã này. Hãy chọn khóa K

Select one:

- (21,13)
- (20,12)
- (13,29)
- (12,20)

Câu hỏi 29

Đoạn văn câu hỏi

Các kỹ thuật an toàn có bao nhiêu mục tiêu cơ bản để được đánh giá là an toàn

Select one:

- a. 4
- b. 6
- c. 5
- d. 3

Câu hỏi 30

Đoạn văn câu hỏi

Mô hình OSI chia ATTT thành bao nhiêu nhóm chức năng?

Select one:

- a. 7
- b. 2
- c. Nhiều
- d. 4

Câu hỏi 31

Đoạn văn câu hỏi

cho bản mã “JT” khóa k là:

98

33

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 $y=kx$

Select one:

- ha
- he
- ho
- tw

Câu hỏi 32

Đoạn văn câu hỏi

Cho hoán vị

12345

52413

Khi mã hóa bản rõ “**plain**” theo mã hoán vị ta sẽ thu được bản mã nào sau đây ?

Select one:

- NLPOJ
- NLIPA
- NLIOJ
- NLOPA

Câu hỏi 33

Đoạn văn câu hỏi

Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước kí sau. Người A có khóa $(p,q,e) = (17,3, 19)$; Người B có khóa $(p,q,e) = (11,5, 3)$. A mã bản tin $m = 10$, sau đó kí thì A kí bằng khóa nào?

Select one:

- 27
- 5
- 3
- 17

Câu hỏi 34

Đoạn văn câu hỏi

Nên cài mức truy cập mặc định là mức nào sau đây để tăng tính an toàn cho dữ liệu?

Select one:

- Full access
- No access
- Read access
- Write access

Câu hỏi 35

Đoạn văn câu hỏi

Cho bản rõ $x = 14$ khóa công khai $n = 33$, $e = 7$. Khi mã hóa bản rõ x với khóa trên theo hệ mã **RSA** ta sẽ thu được bản mã nào sau đây?

Select one:

- 20
- 34
- 25
- 14

Câu hỏi 36

Đoạn văn câu hỏi

Audit (kiểm tra, kiểm toán) trong mô hình AAA (an toàn CSDL) nhằm

Select one:

- Tất cả đều đúng
- Ai đã làm gì
- Cấp quyền ai có thể làm gì
- Xác thực đó là ai

Câu hỏi 37

Đoạn văn câu hỏi

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

Select one:

- a. chữ kí số
- b. khóa bí mật
- c. Khóa công khai
- d. bản mã

Câu hỏi 38

Đoạn văn câu hỏi

Phát biểu nào là sai về Hàm hash

Select one:

- Kết quả phụ thuộc mẫu tin
- Kích thước kết quả có độ dài phụ thuộc vào mẫu tin
- Được tạo từ mẫu tin
- Thường dùng để tạo chữ ký điện tử

Câu hỏi 39

Đoạn văn câu hỏi

Cho bản rõ “**young**” khóa k=15. Khi mã hóa bản rõ với khóa k theo hệ mã dịch vòng ta sẽ thu được bản mã nào sau đây?

Select one:

- a. NERKT
- b. NOTEZ
- c. NDJCV
- d. MNITH

Câu hỏi 40

Đoạn văn câu hỏi

Chọn câu đúng

Select one:

- a. Chữ kí số là dãy số đặc biệt dùng để ký văn bản điện tử
- b. Chữ kí số là trường hợp riêng của chữ kí điện tử, được hình thành từ các thuật toán mã công khai
- c. Chữ kí số với chữ kí điện tử là một
- d. là chữ ký của người dùng internet

Câu hỏi 41

Đoạn văn câu hỏi

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)?

Select one:

- a. Tùy trường hợp mà có tốc độ mã hóa khác nhau
- b. Mã khóa công khai nhanh hơn
- c. Cả 2 có tốc độ bằng nhau
- d. Mã hóa bí mật nhanh hơn

Câu hỏi 42

Đoạn văn câu hỏi

Mô hình OSI chia ATTT thành bao nhiêu mức an toàn hệ thống?

Select one:

- a. 7
- b. Nhiều
- c. 4
- d. 2

Câu hỏi 43

Đoạn văn câu hỏi

Khi kết thúc công việc trên máy tính xách tay và ra ngoài khoảng 1 tiếng vào buổi trưa ta nên làm gì trước khi ra ngoài ?

Select one:

- a. Chắc chắn rằng máy tính xách tay của ta được bảo vệ trên bàn làm việc hay được cất, khóa an toàn
- b. Log out khỏi máy tính xách tay
- c. Nói với đồng nghiệp để mắt đến máy tính xách tay
- d. Shut down và đóng máy lại

Câu hỏi 44

Đoạn văn câu hỏi

Mã hóa feistel, tăng kích thước khóa thì?

Select one:

- Bảo mật hơn, không ảnh hưởng tốc độ xử lý
- Bảo mật hơn đồng thời cũng gây giảm tốc độ xử lý
- Bảo mật hơn, nhưng cần kích thước khối lớn hơn
- Bảo mật hơn đồng thời cũng gây giảm tốc độ mã hóa

Câu hỏi 45

Đoạn văn câu hỏi

Cho bản mã “FBAPN” khóa k= 13. Khi giải mã bản mã với khóa k theo hệ mã **dịch vòng** ta sẽ thu được bản rõ nào sau đây?

Select one:

- sonhj
- sonnu
- sonca
- sondi

Câu hỏi 46

Đoạn văn câu hỏi

Trong mật mã, khóa bí mật dùng để làm gì?

Select one or more:

- a. Giải mã
- b. Mã hóa
- c. Chữ ký công khai
- d. Kiểm tra chữ ký số

Câu hỏi 47

Đoạn văn câu hỏi

Cho bản mã $y = 84$ khóa riêng là $p = 7, q = 13, e = 5$. Khi giải mã bản mã y với khóa trên theo hệ RSA ta sẽ thu được bản rõ nào sau đây ?

Select one:

- 102
- 84
- 28
- 14

Câu hỏi 48

Đoạn văn câu hỏi

Cho bản rõ “center” khóa k=5. Khi mã hóa bản rõ với khóa k theo hệ mã dịch vòng ta sẽ thu được bản mã nào sau đây?

Select one:

- a. VCMHGR
- b. HGRGXV
- c. GRXVCN
- d. XVHGGR

Câu hỏi 49

Đoạn văn câu hỏi

Phần mềm nào trong số đó không phải là phần mềm AntiVirus?

Select one:

- A. Avira
- B. Beast
- C. Panda
- D. Avast

Câu hỏi 50

Đoạn văn câu hỏi

Cho bản mã “YLYR” khóa k= 11. Khi giải mã bản mã với khóa k theo hệ mã **dịch vòng** ta sẽ thu được bản rõ nào sau đây?

Select one:

- A. nenh
- B. ninh
- C. nang
- D. nong

Câu hỏi 51

Đoạn văn câu hỏi

Phương thức nào là hữu ích trong việc tránh phần mềm độc hại cho máy tính cá nhân?

Select one:

- Kerberos
- Firewall
- Phần mềm antivirus
- Xác thực người dùng

Câu hỏi 52

Đoạn văn câu hỏi

Cho bản mã “SW” khóa k là:

72

33

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 $y = kx$

Select one:

- mu
- ma
- sy
- mi

Câu hỏi 53

Đoạn văn câu hỏi

Cho bản gõ “verygood” khóa k = 11. Khi mã hóa bản rõ với khóa k theo hệ mã dịch vòng ta sẽ thu được bản mã nào sau đây?

Select one:

- CVPEIUEM
- GCPEUCRQ
- CRBUOAAG
- GPCJRZZO

Câu hỏi 54

Đoạn văn câu hỏi

Cho bản rõ $x = 7$ khóa công khai $n = 91$, $e = 7$ khi mã hóa bản rõ x với khóa trên theo hệ mã RSA ta sẽ thu được bản mã nào sau đây?

Select one:

- 7

- 95
- 13
- 84

Câu hỏi 55

Đoạn văn câu hỏi

Cho bản rõ $x = 8$ khóa công khai $n = 33$, $e = 7$ khi mã hóa bản rõ x với khóa trên theo hệ mã RSA ta sẽ thu được bản mã nào sau đây?

Select one:

- 2
- 6
- 8
- 4

Câu hỏi 56

Đoạn văn câu hỏi

Cho bản mã “WKRQJ” khóa $k=3$. Khi giải mã bản mã với khóa k theo hệ mã **dịch vòng** ta sẽ thu được bản rõ nào sau đây?

Select one:

- thinh
- thong
- thung
- theng

Câu hỏi 57

Đoạn văn câu hỏi

Cho bản mã “ECLYR” khóa $k=11$. Khi giải mã bản mã với khóa k theo hệ mã **dịch vòng** ta sẽ thu được bản rõ nào sau đây?

Select one:

- thung
- thong
- trong
- trang

Câu hỏi 58

Đoạn văn câu hỏi

Cho bản rõ $x = 15$ khóa công khai $n = 39$, $e = 7$. Khi mã hóa bản rõ x với khóa trên theo hệ mã **RSA** ta sẽ thu được bản mã nào sau đây?

Select one:

- 32
- 24
- 14
- 65

Câu hỏi 59

Đoạn văn câu hỏi

Để tìm bản rõ người thám mã sử dụng

Select one:

- a. sử dụng khóa
- b. sử dụng phần mềm, công cụ hack
- c. sử dụng phương pháp bài toán ngược
- d. kết hợp nhiều cách thức khác nhau

Câu hỏi 60

Đoạn văn câu hỏi

Chứng nhận chứa (certificate) chứa thông tin?

Select one:

- Thuật toán tạo chữ ký
- Chữ ký
- Thông tin thuật toán mã hóa
- Tất cả đều đúng

Câu hỏi 61

Đoạn văn câu hỏi

Cho bản mã “XL” khóa k là:

192

71

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 $y = kx$

Select one:

- hi
- vu
- ha
- hk

Câu hỏi 62

Đoạn văn câu hỏi

Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước kí sau. Người A có khóa $(p,q,e) = (17,3,5)$; Người B có khóa $(p,q,e) = (11,5,13)$. A mã bản tin $m = 10$ sau đó kí thì A kí bằng khóa nào?

Select one:

- 3
- 11
- 5
- 13

Câu hỏi 63

Đoạn văn câu hỏi

CIH là gì?

Select one:

- a. Là một chủng virut máy tính
- b. Là trojan giúp hacker phân tích dữ liệu
- c. Khóa học an toàn mạng máy tính
- d. Tên gọi khác của virus chernobyl

Câu hỏi 64

Đoạn văn câu hỏi

Phát biểu nào sau đây là sai về hàm hash

Select one:

- Được tạo từ mẫu tin
- Thường dùng để tạo chữ ký điện tử
- Kích thước kết quả có độ dài phụ thuộc vào mẫu tin
- Kết quả phụ thuộc mẫu tin

Câu hỏi 65

Đoạn văn câu hỏi

Cho bản mã “UNOPOVJ” khóa k= 7. Khi giải mã bản mã với khóa k theo hệ mã **dịch vòng** ta sẽ thu được bản rõ nào sau đây?

Select one:

- nghihoc
- nghingo
- nghinle
- nghilam

Câu hỏi 66

Đoạn văn câu hỏi

Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước kí sau. Người A có khóa $(p,q,e) = (19, 7, 5)$; Người B có khóa $(p,q,e) = (13, 17, 11)$. A mã bản tin $m = 15$ gửi cho B thì A sử dụng khóa nào?

Select one:

- (19, 133)
- (11, 221)
- (11, 133)
- 19, 221

Câu hỏi 67

Đoạn văn câu hỏi

Trong các nguy cơ mất an toàn thông tin thì giả mạo thông tin là dạng

Select one:

- thông tin được gửi từ nguồn bị chặn tại một điểm trên đường đi vẫn đến được đích với đầy đủ thông tin nhưng thông tin đã bị lộ
- thông tin được gửi từ nguồn bị chặn tại một điểm trên đường đi vẫn đến được đích với thông tin sai lệch
- thông tin được gửi từ nguồn giả tạo
- thông tin được gửi từ nguồn bị chặn tại một điểm trên đường đi và không đến được đích

Câu hỏi 68

Đoạn văn câu hỏi

Một trong hai cách tiếp cận tấn công mã đối xứng

Select one:

- Tấn công tìm bản gõ
- Brute force Attack
- Birthdy paradox
- Tấn công tìm khóa

Câu hỏi 69

Đoạn văn câu hỏi

Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, A thực hiện theo quy trình mã trước kí sau rồi gửi cho B. A có khóa $(p,q,e)=(17,3,5)$; Người B có khóa $(p,q,e)=(11,5,13)$. B nhận được chữ kí s và bản mã từ A gửi đến là $(s,y)=(40,10)$. Hỏi bản rõ mà B tìm được là gì?

Select one:

- a. 51
- b. 10
- c. 55
- d. 40

Câu hỏi 70

Đoạn văn câu hỏi

Loại file nào có thể phát tán virus?

Select one:

- a. .exe
- b. .xyz
- c. .com
- d. virus có thể phát tán ở bất cứ file nào

Câu hỏi 71

Đoạn văn câu hỏi

Cho bản rõ “mahoa” khóa $k=7$. Khi mã hóa bản rõ với khóa k theo hệ dịch vòng ta sẽ thu được bản mã nào sau đây?

Select one:

- a. GEVOIT
- b. VOHTM
- c. MHVOT
- d. THOVH

Câu hỏi 72

Đoạn văn câu hỏi

Cách nào sau đây là tốt nhất để chống lại điểm yếu bảo mật trong HĐH?

Select one:

- Cập nhật bản vá lỗi
- Cài phần mềm diệt virus
- Sao lưu hệ thống
- Cài lại HDH

Câu hỏi 73

Đoạn văn câu hỏi

Cho hoán vị

12345

31425

Khi mã hóa bǎn rõ “**justs**” theo mã hoán vị ta sẽ thu được bǎn mã nào sau đây?

Select one:

- GSHDG
- GJHJH
- GTHDD
- SJTUS

Câu hỏi 74

Đoạn văn câu hỏi

Phương thức nào cho phép ta kết nối đến một mạng LAN của công ty qua internet thông qua một kênh được mã hóa an toàn?

Select one:

- SSL
- SSH
- VPN
- IPSec

Câu hỏi 75

Đoạn văn câu hỏi

Trong mật mã, khóa công khai dùng để làm gì? (chọn nhiều)

Select one:

- Giải mã
- Mã hóa
- Kí



Kiểm tra chữ kí

Câu hỏi 76

Đoạn văn câu hỏi

Phát biểu nào sau đây là đúng với **Bitlocker Drive Encryption**?

Select one:

- Là chương trình của hệ điều hành Windows cho phép mã hóa bit dữ liệu trên máy tính
- Là phần mềm mã hóa công khai
- Là chương trình của hệ điều hành Windows cho phép mã hóa dữ liệu trên máy tính
- Tất cả các ý trên

Câu hỏi 77

Đoạn văn câu hỏi

Cho hệ mật mã Elgamal.

Chọn p là số nguyên tố lớn sao cho bài toán logarit rời rạc không thể giải được

Chọn a là phần tử sinh của \mathbb{Z}_p

Chọn a sao cho $1 < a < p-1$

Tính $b = a^k \text{ mod } p$

Để mã bản rõ x ($\in \mathbb{Z}_p$) người ta chọn một số bí mật k

y_1, y_2 là bản mã của x được tính như sau:

$$y_1 = a^k \text{ mod } p$$

$$y_2 = x \cdot b^k \text{ mod } p$$

Hỏi khóa công khai của hệ mật mã Elgamal là gì?

Select one:

- a, b, p
- k, a, b, p
- k, a
- k, a, b

Câu hỏi 78

Đoạn văn câu hỏi

Phá mã là:

Select one:

- Qúa trình giải mã
- Qúa trình thu thập thông tin để giải mã
- Qúa trình tấn công hệ mật mã để tìm bản rõ hoặc khóa bí mật
- Qúa trình biến đổi thông tin từ dạng không đọc được sang dạng đọc được

Câu hỏi 79

Đoạn văn câu hỏi

Các mật khẩu nào sau đây là khó phá nhất đối với một hacker?

Select one:

- pass@word83
- password@83
- password83@
- pas@sword83

Câu hỏi 80

Đoạn văn câu hỏi

Cho quá trình tạo khóa của hệ mật RSA như sau:

- chọn p, q là hai số nguyên tố lớn khác nhau
- tính $n=p^*q$, $f(n)=(p-1)^*(q-1)$
- chọn e sao cho: $1 < e < f(n)$, e và f(n) là 2 số nguyên tố cùng nhau
- tính $d=e^{-1} \text{mod } f(n)$

Khóa bí mật của hệ này là gì?

Select one:

- $f(n), p, q$
- $f(n), p, q, d$
- p, q, d
- d

Câu hỏi 81

Đoạn văn câu hỏi

Phá hoại thu động mang đặc trưng gì

Select one:

- Chặn bắt và phân tích dòng số liệu
- Chặn bắt hoặc giám sát thông tin
- Chặn bắt và khám phá nội dung thông tin
- Chặn bắt và thay đổi thông tin

Câu hỏi 82

Đoạn văn câu hỏi

Xét trong bảng chữ cái tiếng anh . Mã hoán vị có

Select one:

- $m!$ cách chọn khóa
- 26^m cách chọn khóa
- 312 cách chọn khóa
- $26!$ cách chọn khóa

Câu hỏi 83

Đoạn văn câu hỏi

Cho bản mã “AZ” khóa k là:

83

53

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

Select one:

- vo
- jc
- va
- ve

Câu hỏi 84

Đoạn văn câu hỏi

mật mã dịch vòng là

Select one:

- mã thay thế đa biểu
- mã thay thế đơn biểu
- mã công khai
- mã bí mật

Câu hỏi 85

Đoạn văn câu hỏi

Sniffing là một phương thức tấn công kiểu?

Select one:

- Điều khiển máy tính nạn nhân từ xa
- Can thiệp trực tiếp vào máy của nạn nhân để lấy các thông tin quan trọng
- Tấn công làm tê liệt hệ thống mạng của nạn nhân
- Đánh cắp dữ liệu của nạn nhân truyền trên mạng

Câu hỏi 86

Đoạn văn câu hỏi

Độ an toàn của hệ mật phụ thuộc vào

Select one:

- Không gian khóa đủ lớn để phép vét cạn khóa là không thể thực hiện được
- Tính bí mật của khóa
- Thuật toán, không gian khóa và bản mã
- Tính bí mật của thuật toán

Câu hỏi 87

Đoạn văn câu hỏi

Cho bản mã “FB” khóa k là:

72

33

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

Select one:

- bk
- nw
- bh

bj

Câu hỏi 88

Đoạn văn câu hỏi

Cho bản rõ $x=8$ khóa công khai là $n = 33$, $e = 7$. Khi mã hóa bản rõ x với khóa trên theo hệ mã RSA ta sẽ thu được bản mã nào sau đây?

Select one:

- 8
- 6
- 4
- 2

Câu hỏi 89

Đoạn văn câu hỏi

RSA là giải thuật

Select one:

- Mã khóa riêng
- Mã khóa công khai
- Tổ chức quản lý mã hóa
- Mã hóa khóa bí mật

Câu hỏi 90

Đoạn văn câu hỏi

Mã hóa feistel, tăng kích thước khóa lớn mới mục đích chính

Select one:

- Chống lại dạng brute-force
- Tăng kích thước khối
- Tăng thời gian giải mã
- Chống lại các hình thức tấn công hệ mật

Câu hỏi 91

Đoạn văn câu hỏi

Mã Ceaser của “party” là

Select one:

- sduwb

- tduwb
- sduzb
- seuwb

Câu hỏi 92

Đoạn văn câu hỏi

Cho bản rõ “member” khóa k=22. Khi mã hóa bản rõ với khóa k theo hệ mã dịch vòng ta sẽ thu được bản mã nào sau đây?

Select one:

- JDJKGGE
- DQQJNF
- IAIKAN
- JEAJDWM

Câu hỏi 93

Đoạn văn câu hỏi

Vì sao cần bảo vệ thông tin máy tính

Select one:

- Luôn có nguy cơ gây mất an toàn thông tin khi sử dụng máy tính
- Vì đối với người sử dụng, thông tin là tài sản quan trọng trong máy tính
- Sự mất an toàn thông tin ở quy mô lớn hoặc ở tầm quốc gia có thể đưa đến những hậu quả vô cùng to lớn
- Tất cả các đáp án

Câu hỏi 94

Đoạn văn câu hỏi

Điều kiện của a để các bản mã tiếng anh có thể giải mã trong hệ mã affine là gì?

Select one:

- a, b thuộc Z 26 , a + b = 26
- gcd(a, 26) = 1
- a, b thuộc 26
- a thuộc Z26 và a là nguyên tố cùng nhau với 26

Câu hỏi 95

Đoạn văn câu hỏi

Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước trước kí sau. Người A có khóa $(p,q,e)=(19,7,5)$; người B có khóa $(p,q,e)=(13,17,11)$. A mã bản tin $m=15$ gửi cho B thì A sử dụng khóa nào?

Select one:

- (19, 221)
- (19, 133)
- (11, 133)
- (11, 221)

Câu hỏi 96

Đoạn văn câu hỏi

Để thực hiện cuộc tấn công Trojan-Backdoor. Hacker sẽ thực hiện

Select one:

- Trojan server được cài trên máy nạn nhân. Hacker thực hiện bằng Trojan Client
- Hacker dùng Trojan Client, tấn công vào máy nạn nhân qua các port nhận được từ kỹ thuật scanning
- Hacker dùng Trojan server, tấn công vào máy nạn nhân qua các port nhận được từ kỹ thuật scanning
- Trojan Client được cài trên máy nạn nhân. Hacker điều khiển bằng Trojan server

Câu hỏi 97

Đoạn văn câu hỏi

Trong khoảng thời gian nguồn điện cung cấp cho hệ thống máy tính chập chờn không ổn định, có thể bị ngắt bất cứ lúc nào, thiết bị nào có thể hỗ trợ cấp nguồn giúp bảo vệ an toàn thông tin?

Select one:

- Thanh nguồn điện
- Ổn áp
- UPS
- Dự phòng nguồn điện của máy phát điện

Câu hỏi 98

Đoạn văn câu hỏi

Cho hoán vị

12345

52143

Khi mã hóa bản rõ “kalvi” theo mã hoán vị ta sẽ thu được bản mã nào sau đây?

Select one:

- FJHFK
- HJYHF
- IAKVL
- FHJKH

Câu hỏi 99

Đoạn văn câu hỏi

Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước kí sau. Người A có khóa $(p,q,e)=(19,7,5)$; người B có khóa $(p,q,e)=(13,17,13)$. Giải mã bản rõ gửi cho B thì bản rõ A chọn phải nhỏ hơn giá trị nào?

Select one:

- 192
- 221
- 133
- 108

Câu hỏi 100

Đoạn văn câu hỏi

Cho bản rõ “verygood” khóa $k=12$. Khi mã hóa bản rõ với khóa k theo hệ mã dịch vòng ta sẽ thu được bản mã nào sau đây?

Select one:

- EDJKGGE
- SHRTFFK
- HQDKSAAP
- HEDRASSP

Câu hỏi 101

Đoạn văn câu hỏi

Hãy chọn phát biểu đúng trong các phát biểu sau

Select one:

- Phần mềm diệt virus tốt là có thể diệt tất cả các virus
- Tại một thời điểm một phần mềm quét virus chỉ diệt được một số loại virus nhất định
- Máy tính không kết nối internet thì không bị nhiễm virus
- Một phần mềm quét virus chỉ diệt được duy nhất một loại virus

Câu hỏi 102

Đoạn văn câu hỏi

Giai đoạn đầu của hacking là gì?

Select one:

- Gaining truy cập
- Trinh sát
- Duy trì truy cập
- Dò tìm (Scanning)

Câu hỏi 103

Đoạn văn câu hỏi

Độ an toàn của hệ mật mã Elgamal dựa vào độ khó của bài toán

Select one:

- Phân tích số nguyên lớn thành tích các thừa số nguyên tố
- Knapsack
- Logarit rời rạc
- Phân tích số

Câu hỏi 104

Đoạn văn câu hỏi

Phòng chống tấn công Tấn công từ chối dịch vụ phân tán (DDOS)

Select one:

- Chỉ có thể dùng tường lửa
- Cách hiệu quả duy nhất là lưu trữ và phục hồi (backup và restore)
- Hiện nay đã có cách phòng chống hiệu quả
- Có thể hạn chế trong bằng cách lập trình

Câu hỏi 105

Đoạn văn câu hỏi

Thuật toán chia Euclid mở rộng dùng để

Select one:

- Tính nhanh một lũy thừa với số lớn
- Tính phần tử nghịch đảo của phép nhân và tìm ước chung lớn nhất
- Kiểm tra nhanh một số nguyên tố lớn
- Tính phần tử nghịch đảo của phép nhân

Câu hỏi 106

Đoạn văn câu hỏi

Loại virus nào có thể lây nhiễm vào các tệp dữ liệu

Select one:

- Mailware
- Toolkit
- File virus
- Macro virus

Câu hỏi 107

Đoạn văn câu hỏi

Cho bản mã $y = 20$ khóa riêng là $p = 3$, $q = 11$, $e = 7$. Khi giải mã bản mã y với khóa trên theo hệ RSA ta sẽ thu được bản rõ nào sau đây?

Select one:

- 35
- 14
- 20
- 10

Câu hỏi 108

Đoạn văn câu hỏi

Cho bản mã “MS” khóa k là:

7 2

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 $y = kx$

Select one:

- sa
- se
- ag
- si

Câu hỏi 109

Đoạn văn câu hỏi

“An ninh mạng” là gì?

Select one:

- Là sự kiểm tra hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân
- Là sự kiểm tra hoạt động trên không gian mạng không thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển làm sai lệch, gián đoạn ngưng trệ, tê liệt hoặc các phá hoại hệ thống thông tin quan trọng về an ninh quốc gia ...
- Là sự phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng
- Là sự đảm bảo hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân

Câu hỏi 110

Đoạn văn câu hỏi

Chính sách tài khoản nào nên được thiết lập để ngăn chặn các cuộc tấn công ác ý vào tài khoản của user?

Select one:

- Disable tài khoản không dùng đến
- Giới hạn số lần logon
- Hạn chế thời gian
- Ngày hết hạn tài khoản

Câu hỏi 111

Đoạn văn câu hỏi

Thám mã là

Select one:

- Quá trình biến đổi thông tin từ dạng không đọc được sang dạng đọc được
- Quá trình tấn công hệ mật mã để tìm bản rõ và khóa bí mật
- Quá trình dò tìm khóa bí mật để đọc thông tin
- Quá trình dò tìm thông tin

Câu hỏi 112

Đoạn văn câu hỏi

Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước kí sau. Người A có khóa $(p,q,e) = (17,3,5)$; Người B có khóa $(p,q,e) = (11,5,13)$. B mã hóa thông tin gửi cho A thì B sử dụng khóa nào?

Select one:

- 55
- 37
- (5, 51)
- (55, 13)

Câu hỏi 113

Đoạn văn câu hỏi

Cho bản mã “VG” ” khóa k là:

93

83

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

Select one:

- bg
- bo
- ba
- po

Câu hỏi 114

Đoạn văn câu hỏi

$X=E_k(Y)$. Bản mã là

Select one:

- X
- D
- Y
- K

Câu hỏi 115

Đoạn văn câu hỏi

Chiều dài tối thiểu mặc định của mật khẩu là ?

Select one:

- 3 đến 5 ký tự
- tùy trường hợp
- 8 ký tự
- 12 đến 15 ký tự

Câu hỏi 116

Đoạn văn câu hỏi

Chỉ phát ra biểu sai về Mã đường cong elliptic

Select one:

- Độ an toàn thấp hơn RSA
- Các tính toán là tương đương RSA
- Dung khóa công cộng và khóa riêng để tính toán khóa phiên
- Ít tốn vùng nhớ do xử lý ít hơn RSA

Câu hỏi 117

Đoạn văn câu hỏi

Cho bản mã $y = 24$ khóa riêng là $p = 3, q = 13, e = 7$. Khi giải mã bản mã y với khóa trên theo hệ RSA ta sẽ thu được bản rõ nào sau đây ?

Select one:

- 12
- 15
- 24
- 7

Câu hỏi 118

Đoạn văn câu hỏi

Mã hóa feistel có kích thước khóa lớn thì sao?

Select one:

- Dễ mã hóa, mã hóa nhanh
- Mã hóa chậm
- Khó mã hóa
- Khó mã hóa, mã hóa chậm

Câu hỏi 119

Đoạn văn câu hỏi

cho bản mã “SR” khóa k là:

8 5

5 4

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 $y = kx$

Select one:

- no
- ne
- nh
- ni

Câu hỏi 120

Đoạn văn câu hỏi

Cho hoán vị

1 2 3 4 5

5 1 3 4 2

Khi mã hóa bản rõ “pasca” theo mã hoán vị ta sẽ thu được bản mã nào sau đây ?

Select one:

- APSAC
- APDCA
- APDXE
- APSCA

Câu hỏi 121

Đoạn văn câu hỏi

Cho bản mã $y = 2$ khóa riêng là $p = 3, q = 11, e = 7$. Khi giải mã bản mã y với khóa trên theo hệ RSA ta sẽ thu được bản rõ nào sau đây ?

Select one:

- 2
- 3
- 8
- 12

Câu hỏi 122

Đoạn văn câu hỏi

Luật An ninh mạng do cơ quan nào chủ trì soạn thảo?

Select one:

- a. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng
- b. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an
- c. Bộ Công an
- d. Ban Cơ yếu Chính phủ

Câu hỏi 123

Đoạn văn câu hỏi

Các yếu tố ảnh hưởng đến sự an toàn thông tin máy tính được chia thành mấy nhóm chính?

Select one:

- 2
- 4
- 3
- 5

Câu hỏi 124

Đoạn văn câu hỏi

cho bản rõ “jomio” khóa k=5. Khi mã hóa bản rõ với khóa k theo hệ mã dịch vòng ta sẽ thu được bản mã nào sau đây?

Select one:

- OHVOT
- OHTMT
- OTRNT
- GEVOIT

Câu hỏi 125

Đoạn văn câu hỏi

Giải mã là:

Select one:

- quá trình tấn công hệ mật để tìm bản rõ và khóa bí mật
- quá trình biến đổi thông tin từ dạng đọc được sang dạng không đọc được

- quá trình biến đổi thông tin từ dạng không đọc được sang dạng đọc được
- quá trình tấn công hệ mật thu thập thông tin

Câu hỏi 126

Đoạn văn câu hỏi

Cho hệ mật mã Affine. $K=(a,b)$ là khóa của hệ mật mã này. Hãy chọn khóa K?

Select one:

- (27,15)
- (15,30)
- (17,20)
- (13,17)