Một trong hai cách tiếp cận tấn công mã đối xứng

Chọn một:

a. Tấn công duyệt toàn bộ

b. Tấn công tìm khóa

c. Tất cả đều sai

d. Tấn công tìm bản rõ

Hệ thống mã hóa Vigenere thuộc lớp biến đổi nào?

Chọn một:

a. Phép thế

b. Gamma Xoring

c. Mã hóa khối

d. Hoán vị

Tường lửa thực hiện những chức năng nào sau đây ?

Chọn một:

a. chức năng lọc những luồng thông tin đi qua

b. (hàm) chức năng biến đổi mã hóa các luồng thông tin

c. chức năng trung gian khi thực hiện các tương tác giữa các mạng

Hàm băm sử dụng mấy khóa:

Chọn một:

a. Tất cả đều sai

b. Ba khóa

c. Một khóa

d. Hai khóa

Mã cổ điển là mã :

Chọn một:

a. Mã đối xứng

b. Mã có hai khoá là khoá

c. Mã thay thế hoặc mã hoán vị

d. Hoán vị

Mã khóa công khai

Chọn một:

a. Có thể dung khóa public để mã hóa

b. A và B đều đúng

c. A và B đều sai

d. Dùng 1 khóa để mã hóa và 1 khóa để giải mã

Mã Ceasar thuộc lớp biến đổi nào ?

Chọn một:

a. Phép thế

b. Mã hóa khối

c. Hoán vị

d. Gamma Xoring

Những nguy cơ nào yêu cầu đưa tường lửa vào thành phần trang thiết bị của cơ quan

Chọn một:

a. những nguy cơ truy cập trái phép vào mạng bên ngoài từ mạng bên trong

b. những nguy cơ xâm nhập trái phép vào mạng nội bộ từ mạng bên ngoài

c. những nguy cơ xuất hiện lỗi của người sử dụng, người điều phối và người quản lý

d. Đáp án a, b

RSA là giải thuật

Chọn một:

a. Mã khóa riêng

b. Tất cả đều sai

c. Mã công khai

d. Là tên của một tổ chức quốc tế về mã hóa

Mã nào sau đây là mã không đối xứng?

Chọn một:

a. Mã Stream

b. RSA (Rivest-Shamir-Alderman), El Gamal

c. AES

d. DES (Data Encryption Standart)

Độ dài các thanh ghi X, Y, Z trong hệ mã dòng Tiny A5/1 lần lượt là:

Chọn một:

a. 9, 6, 8

b. 19, 22, 23

c. 22, 19, 23

d. 6, 8, 9

Mã hóa là gì ?

Chọn một:

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. Tất cả đều đúng.

c. 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

d. Môn khoa học (và thực tế ứng dụng nó ) về các phương pháp và phương thức giải mã

Thuật toán DES có kiến trúc nào?

Chọn một:

a. Kiến trúc SQUARE

b. Mã Feistel

c. Mã luồng (stream cipher)

d. Tất cả đều sai

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

Chọn một:

a. 56 bit

b. 48 bit

c. 64 bit

d. 128 bit

Hệ mã hóa hiện đại bao gồm những hệ mã sau:

Chọn một:

a. Mã hóa dòng, mã hóa khối.

b. Mã hóa đối xứng, mã hóa bất đối xứng, hàm băm mật mã.

c. Hàm băm, mã hóa dòng, mã hóa khối

d. Mã hóa đối xứng, mã hóa bất đối xứng

Điều gì quyết định độ tin cậy của thuật toán DES?

Chọn một:

a. Tính nghiệm của các phương trình đại số

b. kích thước của khóa

c. Tất cả các yếu tố trên

d. Phân tích các số lớn thành các thừa số nguyên tố

ECB (Electronic Code Book ), CBC ( Cipher Block Chaining ), OFB (Output Feed Back), CFB(Cipher Feed Back ) là gì?

Chọn một:

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 AES

d. Là những chế độ làm việc của thuật toán Rijndael

Thuật toán nào sau đây không phải là đối xứng ?

Chọn một:

a. El-Gamal

b. IDEA

c. DES

d. RC5

Đặc tính đặc biệt của các thuật toán mã hóa khối là :

Chọn một:

a. Tất cả đều đúng

b. 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

c. 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

d. 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

Mã hóa đối xứng có mấy khóa:

Chọn một:

a. Một khóa

b. Hai khóa

c. Không có khóa

d. Tất cả đều sai

Khi nào thì cần đưa tường lửa vào trong thành phần trang thiết bị của cơ quan

Chọn một:

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

Phần mềm ngăn chặn hành vi:

Chọn một:

a. Tất cả đều đúng

b. Phát hiện code có hại trước khi chúng thực hiện

c. Theo dõi các hành vi trong thời gian thực của hệ thống

d. Theo dõi các tham số của hệ thống

Các nguy cơ mất an toàn thông tin bao gồm:

Chọn một:

a. Lỗi phần mềm, Nguy cơ phá hoại.

b. Lỗi người dùng hoặc lỗi hệ thống, Vi phạm sở hữu trí tuệ, Nguy cơ phần mềm, Lỗi phần mềm, Nguy cơ phá hoại

c. Vi phạm sở hữu trí tuệ, Nguy cơ phần mềm, Lỗi phần mềm

d. Lỗi người dùng hoặc lỗi hệ thống, Nguy cơ phần mềm, Lỗi phần mềm, Nguy cơ phá hoại

Độ dài khóa K con trong một vòng lặp của hệ mã DES là:

Chọn một:

a. 48 bít

b. 56 bít

c. 32 bít

Những mã nào sau đây là đối xứng?

Chọn một:

a. RSA (Rivest-Shamir-Alderman)

b. El Gamal, AES.

c. Đáp án A, C.

d. DES (Data Encryption Standart)

Những thuật toán nào sau đây là thuật toán đối xứng ?

Chọn một:

a. DES, RC5

b. Tất cả

c. Blowfish

d. AES, RC6

Mã thay thế (substitution cipher) là gì ?

Chọn một:

a. 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

b. Là một dạng mật mã thuộc hệ mã vòng

c. Mật mã luồng mà ở đó Gamma xoring được sử dụng để mã hóa dữ liệu

d. 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.

Độ dài các thanh ghi X, Y, Z trong hệ mã dòng A5/1 lần lượt là:

Chọn một:

a. 19, 23, 22

b. 6, 8, 9

c. 19, 22, 23

d. 22, 19, 23

Giải mã là :

Chọn một:

a. khôi phục các thông tin đã bị mã hóa lại dạng ban đầu với sự giúp đỡ của khóa tương ứng.

b. Là quá trình tìm lại bản mã dựa vào khóa của hệ mã đó.

c. Tất cả đều sai.

d. 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.

Thãm mã khi không biết khóa

A a và b sai vì phụ thuộc vào giải thuật

B. Bài toán dễ

C. a và b sai vì phụ thuộc vào khóa

D. Bài toán khó