***AN TOÀN BẢO MẬT THÔNG TIN***

**1.Lý thuyết**

T

- Theo luật của Kirchoff thì độ an toàn của hệ mã phụ thuộc vào yếu tố: Khóa.

- Theo Shannon, để che giấu sự dư thừa thông tin bản rõ là: Bản mã có sự lộn xộn và sự rườm rà.

- Theo Shannon, hệ mã an toàn tuyệt đối nếu : Khóa có độ dài tối thiểu là tương đương độ dài thông báo.

- Theo Shannon, entropy được hiểu là gì: Đo khối lượng thông tin của thông điệp.

- Trong hệ mã khối , sử dụng bảng thay thế số liệu ( s-box) cho biểu thức tính toán để: tăng tốc độ tính toán.

- Trong hệ mã VIGENERE, nếu áp dụng bộ ký tự ASCII cho không gian bản rõ và bản mã thì với khóa độ dài 10 sẽ có số lượng khóa:

- Trong hệ mã hóa khóa công khai nhận định nào sau đây là ĐÚNG: Sử dụng khóa công khai để mã hóa, khóa bí mật để giải mã.

- Trong các hệ mã hóa sau hệ mã nào không phải hệ mã khóa công khai: DES

- Trong các hệ mã hóa sau hệ mã nào không phải hệ mã hóa khóa bí mật : Trapdoor

- Trong các hệ mã hóa sau hệ mã nào không phải hệ mệ hóa khóa khối: DSA

- Trong hệ thống kết hợp giữa RSA và AES thì chức năng của các hệ mã hóa là : AES mã hóa thông điệp, RSA mã hóa hóa của AES

Ư

- Ứng dụng của mật mã bao gồm: Bảo mật dữ liệu, xác thực toàn vẹn thông tin, chữ ký số vầ quản lý khóa.

C

- Các cách tăng sự an toàn của bản rõ trong hệ mã là: Nén bản rõ, che giấu mối quan hệ giữa bản rõ và bản mã, tăng sự phụ thuộc giữa bản mã và bản rõ

- Các yếu tố không ảnh hưởng dến sự an toàn của một hệ mật mã: độ dài bản mã.

- Có mấy phương pháp chính cho việc mã hóa và giải mã : Ba – Mã hóa khóa đối xứng, Mã hóa khóa công khai, hàm băm.

- Các hộp mật ( S – box ) của giải thuật DES: đầu vào chuỗi bit độ dài 48 và sinh các chuỗi 32 bit

- Có mấy chế độ sử dụng mã khối: 4 ( ECB, CBC, CFB, OFB)

- Các hệ mã khóa cổ điển là hệ mã: Mã hóa một hoặc cụm ký tự rời rạc

- Chế độ sử dụng mã khối nào là phổ thông: CBC

- Chế độ sử dụng mã khối nào không sử dụng giá trị IV ( Initialization Vector ): ECB.

- Cấu trúc đại số của DES khiến : Độ phức tạp không tăng nếu mã hóa lặp nhiều lần với các khóa cùng kích thước.

- Chữ ký số là : Sử dụng khóa bí mật để ký , khóa công khai để kiểm tra chữ ký

L

- Lược đồ của hệ mật mã có mấy thành phần: 5 tập khác nhau ( P,C,K,E,D)

P: là không gian bản rõ.

C: là không gian bản mã.

K: là không gian khóa.

S

- SKC được hiểu là : Hệ mã khóa đối xứng

( SKC là Symmetric Key Cryptosystem )

- Số lượng hộp mật (S-box) của giải thuật DES: 8

- So với hệ mã hóa khối, hệ mã mật khóa công khai có đặc tính gì : có tốc độ tính toán chậm.

P

- PKC được hiểu là : Hệ mã khóa phi đối xứng - Hệ mã khóa công khai

( PKC = Public Key Cryptosystem )

H

- Hệ mã khóa dòng được biết là: Một hệ mã khóa đối xứng

- Hệ mã AES có mấy bảng thế S- box cho quá trình mã hóa: 1

- Hiện tượng lộ bản rõ trong thuật toán RSA được hiểu: Kết quả mã hóa không thay đổi so với thông điệp gốc

N

- Nghịch đảo của một số nguyên a trong tập là số : tồn tại theo điều kiện.

- Nhận định nào là SAI trong hệ mã khóa PKC: Sử dụng một khóa mật chung cho cả hai hệ mã

- Nhận định nào sau đây ĐÚNG về chữ ký số : Một phép kiểm tra trong đó nhiều người có thể kiểm tra nhưng chỉ một người được tạo chữ ký.

- Nhược điểm của các hệ mật mã khóa công khai: Tốc độ xử lý của thuật toán chậm

K

- Kết luận nào sau đây là đúng cho DES: là hệ mã hóa dựa trên mã Lucipher

- Kết luận nào ĐÚNG cho hệ mã hóa trên đường cong Elliptic: Khóa riêng là một điểm trên đường cong

- Kết luận nào ĐÚNG cho hệ mã hóa tren đường cong Elliptic: Độ dài khóa nhỏ hơn RSA nhưng đáp ứng độ an toàn

- Kết luận nào ĐÚNG : Hệ mã Merkle- Hellman có cửa bẫy là khóa siêu tăng.

- Kết luận nào SAI: Hệ mã hóa ELGAMAL luôn tồn tại hiện tượng bản rõ trùng bản mã

- Kết luận nào SAI: Hệ mã hóa ELGAMAL được ứng dụng rộng rãi

- Kết luận nào SAI: Hệ mã khóa Merkle- Hellman có độ dài khóa nhỏ

- Kết luận nào SAI với hệ mã khóa ECC: ECC dễ triển khai cài đặt

- Kết luận nào SAI : Hệ mã Merkle- Hellman được ứng dụng rộng rãi trong chữ ký số.

- Kết luận nào ĐÚNG: Mật mã ECC được ứng dụng trong chữ ký số

- Kết luận nào ĐÚNG: Hệ mã PKC cho phép mã hóa khóa của hệ mã SKC

- Kết luận nào ĐÚNG: Hệ mã Merkle – hellman an toàn kém so với RSA

A

- AES có mấy khóa chính ( khóa chủ ) : 3

Ba khóa chủ có độ dài là 128, 192 và 256

D

- Độ dài khóa chính ( khóa chủ) của AES: 128 ,192 và 256 bit

M

- Mệnh đề nào sau đây SAI: DES có các khóa con độ dài 32 bit.

- Mô hình mã hóa kết hợp giữ hệ mã hóa công khai và bí mật được sử dụng là : Sử dụng hệ mã hóa bí mật mã hóa thông điệp , hệ mã hóa công khai mã hóa khóa bí mật và cùng truyền.

V

- Với hệ mã hóa AES có số vòng lặp: 10 (128) ,12( 192) hoặc 14( 256).

G

- Giải thuật mã hóa AES sử dụng khóa chủ độ dài 192 có số vòng lặp: 12

Y

- Ý tưởng của hệ mã hóa Knapsack ( Merkle – Hellman ) là : Bài toán đóng thùng.

- Ý tưởng của hệ mã hóa RSA: Tính khó giải của bài toán phân tích một số thành 2 thừa số nguyên tố.

- Ý tưởng của hệ mã hóa ELGAMA: Tính khó giải của bài toán LOGARIT rời rạc