|  |  |  |  |
| --- | --- | --- | --- |
| STT: | Mã SV: | Họ và tên: | Ngày: |
| 19 | B2113328 | Lê Tuấn Đạt | 26/02/2025 |

Yêu cầu**:** Sinh viên viết ngắn gọn về sự hiểu biết của mình về các nội dung 4 buổi thực hành

Lưu ý**: Không được sử dụng AI để viết**

**Nội dung:**

**Bài Thực hành 1:**

Em hiểu gì về mật mã **Affine**? Nguyên tắc mã hóa, giải mã, độ dài Khóa? Độ an toàn và khả năng có thể bị suy khóa như thế nào?

**Bài Thực hành 2:**

Em hiểu gì về mật mã **DES**? Nguyên tắc mã hóa, giải mã, độ dài Khóa? Độ an toàn của DES và khả năng có thể bị suy khóa như thế nào?

**Bài Thực hành 3:**

Em hiểu gì về mật mã **RSA**? Nguyên tắc mã hóa, giải mã, độ dài Khóa? Độ an toàn của RSA và khả năng có thể bị suy khóa như thế nào?

**Bài Thực hành 4:**

Em hiểu gì về **Băm** trong ATBMTT? Nguyên tắc mã hóa, giải mã, độ dài Khóa? Độ an toàn của Hàm băm và khả năng có thể bị suy khóa như thế nào?

**BTH 1:**

- Mật mã Affine: Là mật mã cổ điển, dễ hiểu, sử dụng một hàm toán học tuyến tính để mã hóa và giải mã thông điệp.

- Nguyên tắc mã hóa: Sử dụng công thức toán học để biến kí tự này thành kí tự khác.

- Nguyên tắc giải mã: Dùng Euclid mở rộng để nghịch đảo phần mã hóa.

- Độ dài khóa: Khóa gồm hai số a và b. Hai số này phải cực lớn và a phải là số nguyên tố cùng nhau với m, b thuộc đoạn [0, m - 1]. Nếu m = 26, độ dài khóa là 312.

- Độ an toàn và khả năng bị suy khóa:

+ Dễ bị vét cạn.

+ Dễ bị phá bằng cách phân tích tần suất hoặc tấn công thống kê.

**BTH 2:**

- Mật mã DES: Là mật mã đối xứng, mã hóa dữ liệu theo từng khối 64 bit bằng cách sử dụng 8 bit để kiểm tra chẵn lẽ và 56 bit còn lại là khóa.

- Nguyên tắc mã hóa: Thực hiện biến đối ở khối hoán vị khởi đầu. Sau đó, thực hiện 16 vòng biến đổi với cùng một chức năng, trong đó, sử dụng các toán tử thay thế và hoán vị. Cuối cùng, sử dụng hoán vị cuối.

- Nguyên tắc giải mã: Áp dụng ngược lại với mã hóa, chỉ thay đổi thứ tự khóa con.

- Độ dài khóa: Chỉ sử dụng 56 bit để lưu trữ khóa trong tổng số 64 bit.

- Độ an toàn và khả năng bị suy khóa:

+ Không gian khóa nhỏ, dễ bị vét cạn.

+ Dễ bị tấn công với các phương pháp tấn công hiện đại.

**BTH 3:**

- Mật mã RSA: Là mật mã bất đối xứng, dùng hai khóa riêng biệt cho mã hóa và giải mã.

- Nguyên tắc mã hóa: Dựa trên bài toán Trung Hoa: Phân tích một số lớn thành tích của hai số nguyên tố. Quá trình mã hóa bao gồm:

+ Tạo khóa: Sau khi hoàn tất, khóa công khai sẽ gửi cho mọi người và giữ riêng khóa bí mật.

+ Mã hóa: Sử dụng khóa công khai để mã hóa thông điệp.

- Nguyên tắc giải mã: Sử dụng khóa cá nhân để giải mã dựa trên định lý Euler.

- Độ dài khóa: Độ dài khóa của RSA lớn hơn nhiều so với AES, vì nó dựa trên bài toán phân tích nhân tử. Hiện nay, tiêu chuẩn tối thiểu là 2048 bit. Nếu bảo mật cao hơn, có thể ưu tiên 4096 bit.

- Độ an toàn và khả năng bị suy khóa:

+ Độ an toàn chấp nhận được trong bối cảnh công nghệ có điển, được ứng dụng trong trao đổi khóa và chữ ký số.

+ RSA có thể bị phá nếu máy tính lượng tử được phát triển.

**BTH 4:**

- Băm:

+ Là giải thuật sinh ra các giá trị băm tương ứng với mỗi khối dữ liệu.

+ Hàm băm nhận đầu vào có độ dài bất kỳ và tạo ra đầu ra có độ dài cố định. Nó chỉ ánh xạ một chiều, không cần khóa.

+ Mục đích là kiểm tra tính toàn vẹn của thông điệp.

+ Là hàm một chiều, không thể băm ngược lại để tìm văn bản gốc.

- Nguyên tắc mã hóa: Quy trình băm như sau:

+ Nén dữ liệu thành một chuỗi ngắn hơn.

+ Chia đầu vào thành các khối, xử lý tuần tự qua các vòng lặp với phép toán logic, hoán vị, và cộng modulo.

- Nguyên tắc giải mã: Vì hàm băm là hàm một chiều, nên không có cách giải hàm băm.

- Độ dài khóa: Hàm băm không dùng khóa, nhưng độ dài đầu ra là cố định và phụ thuộc vào thuật toán được sử dụng. Hiện nay, SHA-256 (256 bit) đang phổ biến.

- Độ an toàn và khả năng bị suy khóa:

+ Phụ thuộc vào thuật toán, độ dài đầu ra, và cách triển khai.

+ SHA-3 có thể được ưu tiên hơn thiết kế linh hoạt trong trường hợp máy tính lượng tử phát triển.