----------------------- Staganography --------------------------

Các thuật toán giấu tin: thuận nghịch, wulee, CPT, MCPTE

* LSB chung:   
  Giấu tin: Thay từng bit của tin vào bit cuối cùng của từng byte ảnh. Bit có trọng số thấp nhất ( bít ít quan trọng nhất Least Significan Bit )
* Encode:  
  1. Chuyển ảnh về dạng 1 chuỗi byte

2. Chuyển tin đã mã hóa về 1 chuỗi byte.

3. Lấy độ dài của tin ( xem có bao nhiêu byte )

4. Chuyển độ dài tin vào trong 4 byte. (32 bit )

5. Giấu 32 bit chiều dài tin vào 32 byte đầu tiên của ảnh bằng encode\_text

6. Giấu tin bằng encode\_text ( từ vị trí byte thứ 33 của ảnh )

* kiểm tra độ dài của tin ( tính theo bit ) + số byte ảnh đã được sử dụng nếu lớn hơn số byte ảnh gốc thì ko thể giấu tin.
* chạy từ byte đầu tiên đến byte cuối cùng của tin. b để lưu bit cần giấu, sau đó giấu tin vào bit cuối của mỗi byte ảnh.

7.Trả về 1 ảnh đã được giấu tin.

* Decode:  
  1. Lấy 1 bức ảnh, chuyển bức ảnh về dạng byte  
  2. Phải tìm chiều dài của tin, sử dụng 1 biến length để lưu chiều dài tin.  
  3. Tạo 1 biến result kiểu byte có số phần từ bằng chiều dài của tin  
  4. Chạy từ đầu tin cho đến cuối tin, chạy 8 bit cho mỗi byte của tin, sẽ lấy được
* LSB Questions:  
  1. Tính bảo mật?   
   - AES mã hóa tin  
   - Dù hacker giải mã đc ảnh đã giấu tin nhưng cũng chỉ ra các bản mã AES   
   nên không biết cái nào là bản rõ   
  2. Khả năng kiểm tra có tin trong ảnh bất kỳ?  
  3. Ưu điểm nhược điểm LSB? Đảm bảo an toàn và bảo mật thông tin tập trung vào các kỹ thuật giấu tin để có thể giấu được nhiều thông tin nhất. THông tin mật được giấu kỹ trong một đối tượng sao cho người khác khó phát hiện.
* 4. Thủy vân số là gì?Thủy vân số là một quá trình nhúng dữ liệu gọi là thủy vân hoặc chữ ký số hoặc thẻ hoặc nhãn vào một đối tượng đa phương tiện mà thủy vân có thể được phát hiển hoặc trích lọc sau đó để chứng minh nguồn gốc của đối tượng. Đối tượng có thể một ảnh, hoặc audio hoặc video.
* AES chung:

AES là tiêu chuẩn mã hóa nâng cao, vận hành dựa trên ma trận 4x4 đc gọi là state

AES làm việc với khối dữ liệu 128bit, độ dài khóa 128, 192, 256bit. Các khóa mở rộng sử dụng thủ tục sinh khóa Rijindael

Kích thước của khóa quyết định số vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã

10 vòng lặp - 128bit

12 vòng lặp - 192bit

14 vòng lặp - 256bit

* Encrypt:  
  1. Chuyển khóa thành mảng byte  
  2. Đầu vào là khóa ở mảng byte trả về kết quả là hàm byte đã được băm

3. chuyển về mảng key có kích thước 16 phần tử

4. key là khóa bí mật

5. tạo cipher rồi chuyển nó thành mảng byte

6. thực hiện mã hóa trên mảng byte rồi chuyển byte sang dạng Base64 để hiển thị

Decrypt:  
 Ngược lại ngoại trừ phép biến đổi AddRoundKey() không thay đổi vì chính bản thân nó là một phép biến đổi thuận ngịch do chỉ áp dụng một phép toán XOR  
 2.

* AES Question:

1. AES là gì?

2. Các thuật toán mã hóa: DES, AES, RSA

3. Tại sao dùng AES? độ an toàn cao. chống lại được một số kĩ thuật tấn công. tốc độ mã hoá nhanh. khả năng ứng dụng cao. có khả năng mở rộng khoá. tù tước tới giờ chưa có cuộc tấn công thành công nào.

4. Quá trình mã hóa?

mở rộng khóa: các khóa phụ dùng trong vòng lặp được sinh ra từ khóa chính sử dụng thủ tục sinh khóa Rijindael

Vòng khởi tạo:

Addroundkey: mỗi byte trong state đc kết hợp vs khóa sử dụng XOR

Vòng lặp chính:

Subbytes: thay thế phi tuyến tính byte trong state = byte khác sử dụng bảng tham

chiếu

ShiftRows: mỗi dòng trong state được dịch 1 số bc theo chu kỳ

Mixcolumns: Trộn các cột kết hợp 4 byte trong mỗi cột

Addroundkey

Vòng cuối k mixcolumns

Rijindael:

ưu điểm: độ an toàn cao, chống lại được 1 số kt tấn công: vét cạn, tuyến tính, vi sai

tốc độ mã hóa nhanh, được tích hợp sẵn pứng

Khả năng ứng dụng cao trong hầu hết lĩnh vực

có khả năng mở rộng

Nhược điểm: khó khăn trong vấn đề quản lý khóa và phân phối khóa

cấu trúc thuật toán đơn giản

ko chống lại được kỹ thuật tấn công kênh kề

NOTE: cơ sở toán học AES dựa trên phép + & x trên trường GF(2^8)