**1. ENCODE/DECODE: Mã hóa/ Giải mã**

- Encode- mã hóa là quá trình chuyển đổi dữ liệu từ một định dạng này sang một định dạng khác bằng cách sử dụng một phương pháp một bảng mã đã được công bố công khai.

- Decode- giải mã, ngược lại với quá trình mã hóa. Nó chuyển đổi truyền dữ liệu thông tin liên lạc được mã hóa và các tập tin với tình trạng ban đầu của họ.

- Mục đích của việc chuyển đổi này là để tăng khả năng sử dụng các dữ liệu đặc biệt là trong các hệ thống khác nhau.

- Một số loại phổ biến là: hash(md5), mã hóa bất đối xứng (PUBLIC KEY ENCRYPTION), Base64 và BinHex.

- UTF8, UTF16- Là phương thức Encoding rất phổ biến để miêu tả bảng mã Unicode trên bộ nhớ.

- Encode biến đổi thông tin để giữ tính toàn vẹn.

**2. ENCRYPT/DECRYPT: Mã hóa/Giải mã**

-Encrypt cũng là một quá trình chuyển đổi dữ liệu được sử dụng các thuật toán mã hóa. Nó chuyển đổi các dữ liệu ban đầu thành một định dạng mà chỉ có thể giải mã được nếu có khóa phù hợp.

-So sánh với encode thông thường ở trên, khi mà ta chỉ cần dùng đúng công cụ encode để decode ngược lại là xong. Nhưng với encryption, quá trình mã hóa sẽ kèm theo 1 secret-key hay là 1 mã bảo mật mà chỉ người tạo biết được.

Do đó, để có thể giải mã, chúng ta cẩn có đủ 3 thông tin :

* Đầu tiên chắc chắn là đoạn dữ liệu đã bị mã hóa
* Thuật toán dùng để mã hóa
* Cuối cùng quan trọng nhất vẫn là key mật mà người tạo đã sử dụng cho thuật toán này.

- Decrypt - Giải mã là một quá trình chuyển đổi dữ liệu được mã hóa ở dạng mà con người hoặc máy tính có thể đọc và hiểu được. Phương pháp này được thực hiện bằng cách hủy mã hóa văn bản theo cách thủ công hoặc bằng cách sử dụng các khóa được sử dụng để mã hóa dữ liệu gốc.

- Mục đích của mã hóa là để bảo mật thông tin, người có quyền được xem mới xem được.

-Hai trong số các phương pháp mã hóa được sử dụng rộng rãi là mã hóa khóa đối xứng và mã hóa khóa công khai. Trong mã hóa khóa đối xứng, cả người gửi và người nhận chia sẻ cùng một khóa được sử dụng để mã hóa dữ liệu. Trong mã hóa khóa công khai, hai khóa khác nhau nhưng về mặt toán học có liên quan được sử dụng.

-Mã hóa là một phương pháp chuyển đổi dữ liệu với sự tăng thêm của việc giữ bí mật. Encrypt sử dụng một thuật toán được gọi là cipher để mã hóa dữ liệu và nó có thể được giải mã khi sử dụng một khóa đặc biệt. Mã hóa là đặc biệt cần thiết khi giao tiếp qua một phương tiện không đáng tin cậy như internet, nơi mà thông tin cần phải được bảo vệ với các bên thứ ba khác. Phương pháp mã hóa hiện đại tập trung vào việc phát triển các thuật toán mã hóa (ciphers) đễ khó để phá vỡ.

Encrypt là một quá trình chuyển đổi dữ liệu bình thường thành một dạng không thể đọc được trong khi Decrypt là một phương pháp chuyển đổi dữ liệu không đọc được / mã hóa thành dạng ban đầu của nó.

Mã hóa được thực hiện bởi người đang gửi dữ liệu đến đích, nhưng việc giải mã được thực hiện ở người đang nhận dữ liệu.

Thuật toán giống nhau với cùng một khóa được sử dụng cho cả hai quá trình mã hóa-giải mã.

- Thư viện sử dụng: aes.c + aes.h: Thư viện TinyAes để mã hoá và giải mã