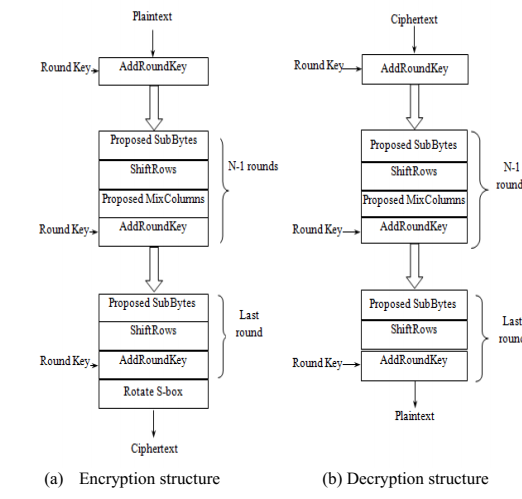
Thành viên nhóm:

* Hoàng Mai Trang
* Lương Hiển Vinh

**Ý tưởng: thông tin bằng thuật toán mã hóa AES.**

Đây là phương pháp mã hóa theo khối có kích thước khối và mã khóa thay đổi linh hoạt với các giá trị 128,192 hay 265 bit, phương pháp này thích hợp ứng dụng trên nhiều hệ thống khác nhau.



\*Quá trình mã hóa gồm 4 bước:

- AddRoundKey — mỗi byte của khối được kết hợp với khóa con, các khóa con này được tạo ra từ quá trình tạo khóa con Rijndael.

- SubBytes — đây là phép thế (phi tuyến) trong đó mỗi byte sẽ đƣợc thế bằng một byte khác theo bảng tra (Rijndael S-box).

- ShiftRows — đổi chỗ, các hàng trong khối được dịch vòng.

- MixColumns — quá trình trộn làm việc theo các cột trong khối theo một phép biến đổi tuyến tính.

\* Quy trình giải mã thực hiện qua các quy trình sau:

- Thực hiện thao tác AddRoundKey đầu tiên trƣớc khi thực hiện các chu kỳ giải mã.

- Nr −1 chu kỳ giải mã bình thƣờng: mỗi chu kỳ bao gồm bốn bƣớc biến đổi liên tiếp nhau: InvShiftRows, InvSubBytes, AddRoundKey,InvMixColumns.

- Thực hiện chu kỳ giải mã cuối cùng. Trong chu kỳ này, thao tác InvMixColumns được bỏ qua.

Người dùng muốn sử dụng chương trình thì cần đăng nhập vào tài khoản của bản thân, khi tài khoản chính xác thì người dùng sẽ được đưa đến trang chủ của chương trình nơi người dùng có thể đưa ra tài liệu, thông tin người dùng muốn mã hóa, sau đó chương trình sẽ mã hóa thông tin rồi đưa lại người dùng thông tin đã được mã hóa, người dùng cũng có thể đưa ra thông tin đã được mã hóa để chương trình tiến hành giải mã.