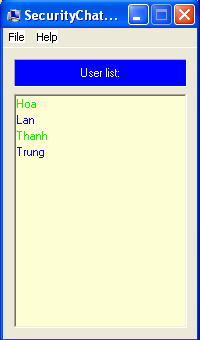
1. **Xây dựng chương trình SecurityChatServer**:

**2.1.1** **Giao diện:**

**

**Trong đó**:

* User list: Danh sách các users đã đăng nhập vào hệ thống chat
* Menu File =>Taskbar: thu nhỏ SecurityChatServer trên thanh Taskbar

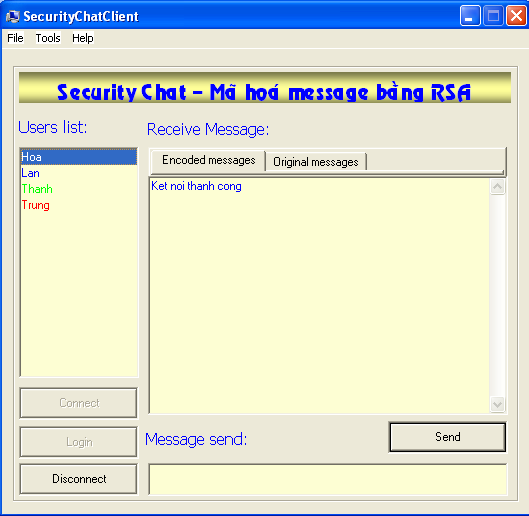
File =>Exit: Kết thúc chương trình

**2.1.2** **Hoạt động**:

* Khởi động: tạo socket, lắng nghe, chờ kết nối
* Khi có yêu cầu kết nối từ phía Client: thêm một user mới vào danh sách các user chưa login (chưa có tên)
* Khi Client login: Loại bỏ user từ danh sách các user chưa login (chưa có tên), thêm user đã login (có tên) vào danh sách các user chính thức, sau đó gởi danh sách tất cả các user đã đăng nhập vào server.
* Khi một user muốn chat với user khác, user đó sẽ gởi yêu cầu tạo khóa, server sẽ tạo một nhóm mới (nếu nhóm đó chưa tồn tại) gồm hai user sẽ chat với nhau. Từ đó, với mỗi yêu cầu nhận được từ phía client, server chỉ có nhiệm vụ chuyển đúng đến nơi nhận.
* Khi một user ngưng kết nối, server sẽ xóa bỏ các nhóm có tên user đó.

1. **Xây dựng chương trình SecurityChatClient**:

**2.2.1** **Giao diện:**

****

**Trong đó**:

* Users list: Danh sách các users có trên server
* Encoded messages: Nội dung trao đổi giữa hai user đã được mã hóa
* Original messages: Nội dung trao đổi giữa hai user đã được giải mã (bản gốc)
* Connect: Kết nối đến server
* Login: Sau khi kết nối thành công, login in vào hệ thống với user name và password
* Disconnect: Hủy kết nối (ngưng chat)
* Message send: Ô nhập nội dung trao đổi
* Send: Gởi message đã nhập.
* Menu: File => Exit: kết thúc chương trình.

Tools => Option: cho phép tuỳ chọn có bắt buộc phải nhập password mỗi lần muốn đọc Original messages hay không.

Help=>How to use SecurityChat…: hướng dẫn sử dụng chương trình

**2.2.2** **Hoạt động**:

* Sau khi khởi động, click vào nút Connect để kết nối đến server.
* Sau khi kết nối thành công, login vào hệ thống với user name và password.
* Khi login thành công, nhận danh sách các users có trên server và hiển thị trên danh sách Users list, có thể bắt đầu chat.
* Khi một user muốn chat với user khác, chọn tên user đó từ danh sách, nhập thông tin muốn gởi đi, nhấn nút Send. Quá trình gởi thông tin này được thực hiện trong một qui trình khép kín như sau:
  1. Gởi yêu cầu tạo khóa đến user nhận.
  2. Khi nhận được yêu cầu tạo khóa, tạo khóa công khai và khóa bí mật, khóa công khai gởi đến user đã yêu cầu, khóa bí mật lưu lại dùng để giải mã
  3. Khi nhận đuợc khóa công khai, dùng khóa này mã hoá message đã nhập trên ô Message send, sau đó gởi đi.
  4. Khi nhận được message đã được mã khoá, dùng khoá bí mật đã tạo trước đó giải mã message này và hiển thị trên cửa sổ Original messages, còn bản đã mã hoá hiển thị trên cửa sổ Encoded messages.