End-to-End Secure Chat

The Basics

The chat is a one-on-one system, with a middleman. The two “participants” are the clients. The middleman is the server. One client sends a message to the server; the server receives that message and passes it on the other client; the other client receives the message.

The Security Part

The clients will hold a “key” that will encrypt and decrypt messages on their end.

Example: Sender client sends a message to its receiver client. Sender will type up their message and “send” it. Before the message leaves the sender, the message is encrypted and **then** it gets sent to the server. The server will receive the encrypted message and then passes the message along to the receiver. The receiver will receive the encrypted message, decrypt it, and then the client “receives” the message (they are able to read it).

Potential classes

- Server

- Client

Potential relationships