Secure Chat

Our project is a simple encrypted messaging program. We are aiming to have a program that delivers a quick, reliable, functional program that prioritizes security. Our goal for this program is to create chat rooms that are created by people to have a chat by themselves and not to worry about their privacy.

This project offers its users a secure web based platform that will make use of several encryption methods to cypher and decypher their messages. This kind of communication will also provide rooms that are protected with user declared passwords. Unlike other applications in this web program we are not keeping any logs of users data so they can have their chat on a secure platform.

It is widely known that near current events about the most common chat application WhatsApp shares their user's information to companies and keeps data about our private contents.

Our project solves this problem by;
1. First of all we do not offer any registration process so people can use any nickname in the program as they please. This offers an anonymous platform and a secure platform.
2. Our project is not a data kept driven project so the messages will not be kept after the users close their chats the room alongside its messages will be terminated after the process.
3. Upon entering the program after the phase of choosing a nickname for chatting, the program will list password protected rooms that have been created by other users. Also users can choose to create its desired room for several purposes.
4. Upon sending every message in chat rooms will be encrypted then will be sent to the system our system will decrypt for every user in the chatroom. This way we will achieve end-to-end encryption.

This project will be a web driven program it will include modules as: Express, Nodemon and Socket.io;
1. Express will allow the program to host at the port which we will choose.
2. Nodemon package will save the settings and restart at any given change during the development in the program as well as starting the server.
3. Socket.io will allow us to have a real time experience. It delivers and gets information in real time so we can use our encryption methods and serve an interactive platform.

Because we have chosen to do our project in a web based platform and used javascript infrastructures we believe it will be easier to implement encryption and decryption methods. For now we haven't entirely decided on an exact encryption algorithm but we have a vision about how the system works.

1900005528 - Ahmet Kaan Memioğlu
1900005485 - Emrecan Üzüm
1900003587 - Şükrü Erim Sinal