Especificación de la API de Chat en Tiempo Real

Funciones de Encriptación y Desencriptación

La API proporciona dos funciones para cifrar y descifrar mensajes:

1. `encryptMessage(message)`: Esta función toma un mensaje como entrada y lo cifra utilizando el algoritmo AES (Advanced Encryption Standard) con una clave secreta "secret-key". El mensaje cifrado se devuelve como una cadena de texto.

2. `decryptMessage(encryptedMessage)`: Esta función toma un mensaje cifrado como entrada y lo descifra utilizando la misma clave secreta "secret-key". El mensaje descifrado se devuelve como una cadena de texto.

Funciones del Servidor

Función principal del servidor:

El servidor se inicia utilizando Express y Socket.IO. El código se encuentra en un archivo externo y se importa utilizando `require("./sockets")(socketio)`.

Manejo de Conexiones de Socket:

- Cuando un cliente se conecta al servidor (`io.on("connection", ...`), se ejecutan las siguientes acciones:
  - Se registra un mensaje de "Nuevo usuario conectado" en la consola.
  - El servidor escucha el evento "enviar mensaje" y cifra el mensaje antes de enviarlo a todos los clientes conectados.
  - El servidor escucha el evento "nuevo usuario" para agregar nuevos usuarios al chat.
  - El servidor escucha el evento "disconnect" para eliminar a los usuarios desconectados.

Función de Actualización de Usuarios:

- La función `actualizarUsuarios()` se utiliza para enviar la lista de usuarios conectados a todos los clientes. Los nombres de usuario se envían en un evento llamado "usernames".

Funciones del Cliente

- El cliente es una página HTML que incluye formularios para ingresar el nombre de usuario y enviar mensajes. También muestra el chat en tiempo real y la lista de usuarios conectados.

- El cliente utiliza el script JavaScript para interactuar con el servidor a través de Socket.IO.

- El cliente desencripta los mensajes antes de mostrarlos en el chat.