**WhisperSend: User Guide**

# **1. Project Description**

WhisperSend is a secure, peer-to-peer file-sharing web application, built with a focus on encryption and privacy. Users can securely transfer files or initiate chat conversations without relying on a central server. The app employs asymmetric encryption for securing communications, using public and private keys generated at the session level.

# **2. Project Setup**

## **Dependencies**

The project is built using Vite as a development environment, Preact for UI components, and PeerJS for peer-to-peer communication.

The following packages are installed as dependencies:  
  
 - Core Dependencies:  
 - @emoji-mart/data - Emoji data set for chats  
 - @emoji-mart/react - Emoji component for React/Preact  
 - emailjs-com - For sending emails  
 - ethers - Handles Ethereum-related encryption and wallet generation  
 - peerjs - Provides peer-to-peer connection and communication  
 - preact - Lightweight React alternative for faster performance  
 - preact-router - For handling in-app navigation  
 - react - UI components (Preact-compatible)  
 - react-icons - Icons for UI design  
 - react-toastify - Toast notifications for alerts and messages  
  
 - Development Dependencies:  
 - @preact/preset-vite - Vite preset for Preact  
 - @tailwindcss/aspect-ratio - Tailwind plugin for handling aspect ratios  
 - @tailwindcss/forms - Tailwind plugin for form styling  
 - @tailwindcss/typography - Tailwind plugin for typography styling  
 - autoprefixer - Adds vendor prefixes to CSS rules  
 - postcss - Post-processing for CSS  
 - prettier - Code formatter for consistent code styling  
 - tailwindcss - CSS framework for styling

## 

## **Installation**

1. Clone the repository:  
 $ git clone https://github.com/jessicamirov/WhisperSend.git  
 $ cd WhisperSend  
  
 2. Install the dependencies:  
 $ npm install  
  
 3. Run the development server:  
 $ npm run dev  
  
 The application will run on http://localhost:3000.

# **3. Features**

**- Peer-to-Peer File Sharing**: Secure and direct file transfer using PeerJS.  
 **- Asymmetric Encryption:** Files are encrypted using the public key of the recipient and can only be decrypted with their private key.  
 **- Mnemonic Management:** Users are provided with a mnemonic phrase for encryption keys, which they need to save for future sessions.  
 **- Real-Time Chat:** Secure messaging and emoji sharing between connected peers.  
 **- Encryption/Decryption Services:** Users can encrypt and decrypt files directly from the app interface.

**Deployment run:**

You can also visit this link to access the website:

<https://whispersend.vercel.app/>

**Exploring Main Pages and Key Features**

Here are the steps required to properly use the site, create a secure chat, and encrypt or decrypt files as needed.

**Homepage:**

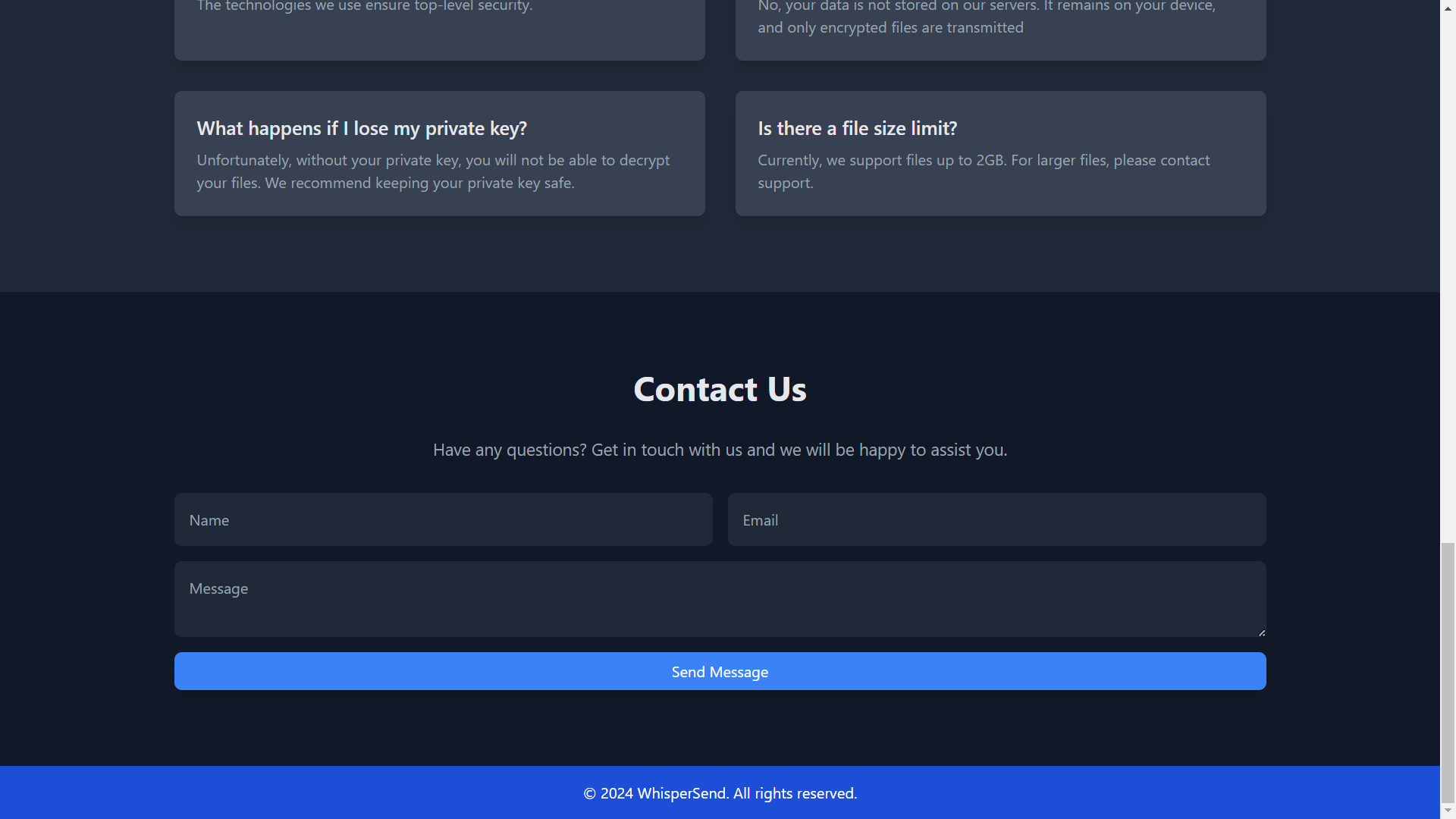
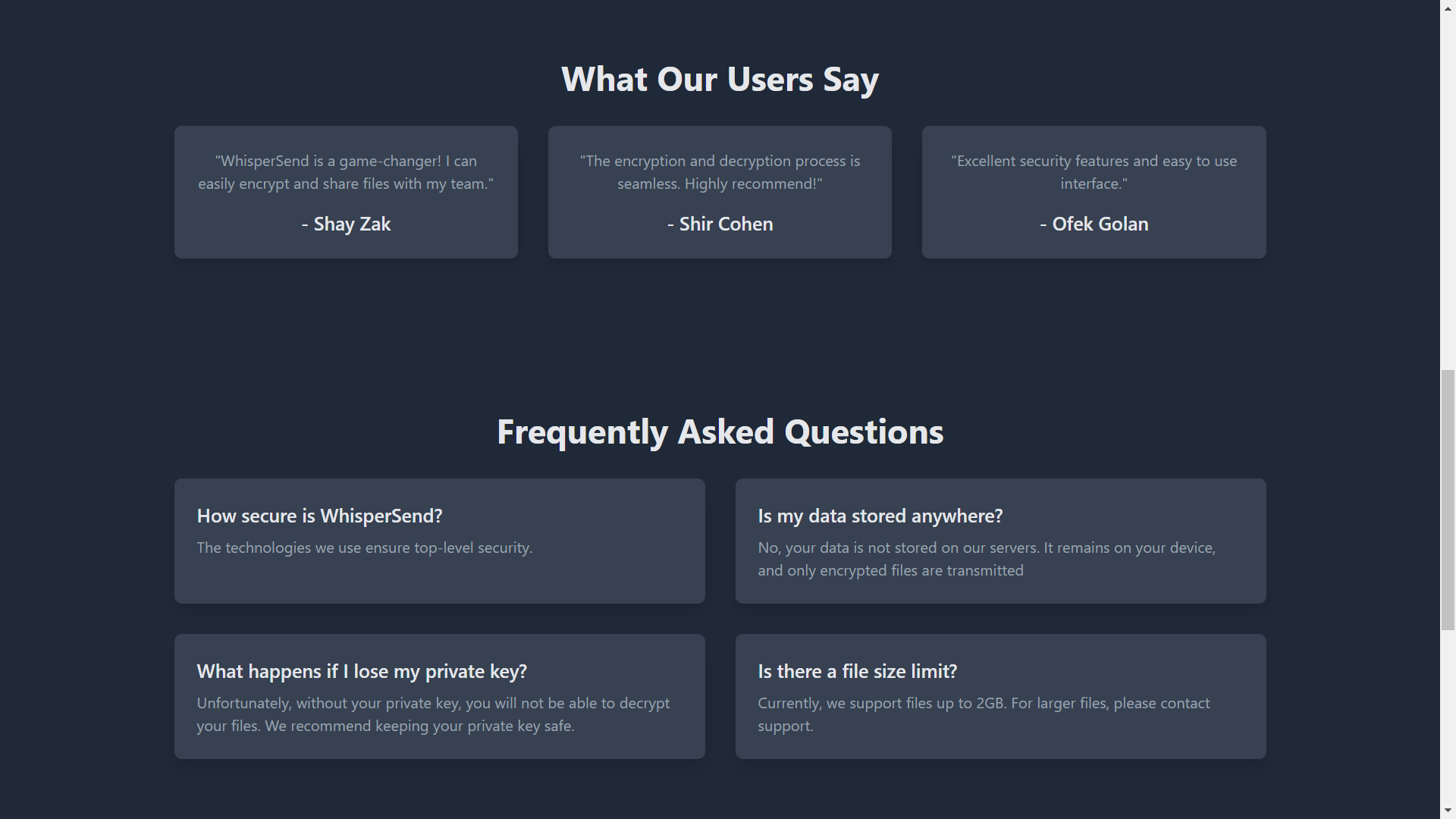
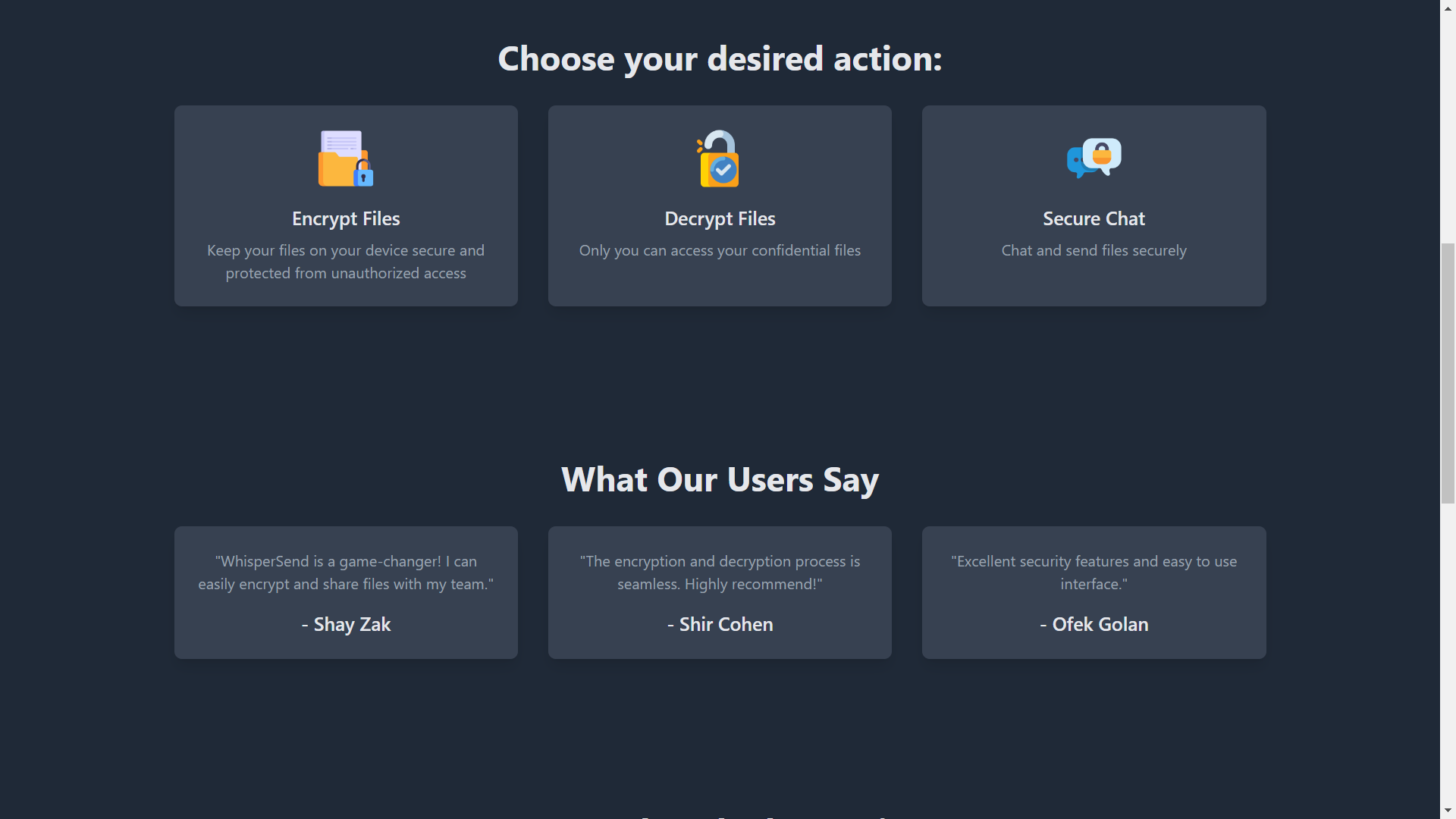
Upon visiting, you'll see a summary of the site's features and services.

Frequently Asked Questions - Check the FAQ section for answers to common questions, making it easier to navigate the site.

What Our Users Say- Read feedback from other users to learn about their experiences with our services.

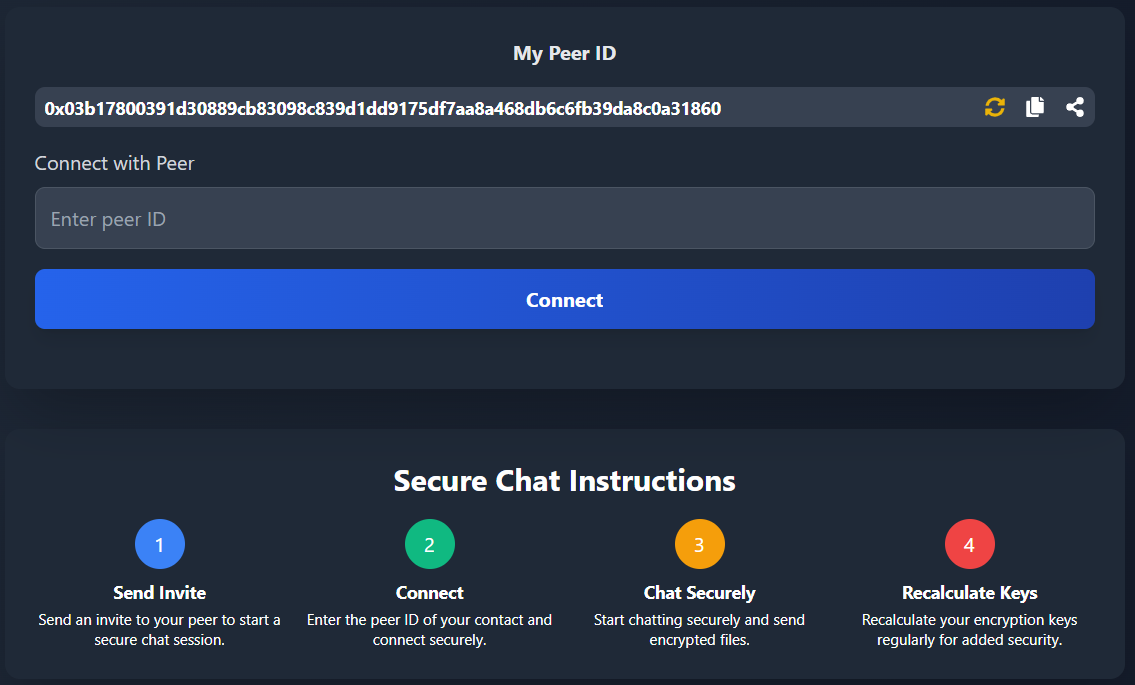
Contact Us - For further inquiries, use the contact form to send us a message directly via email.

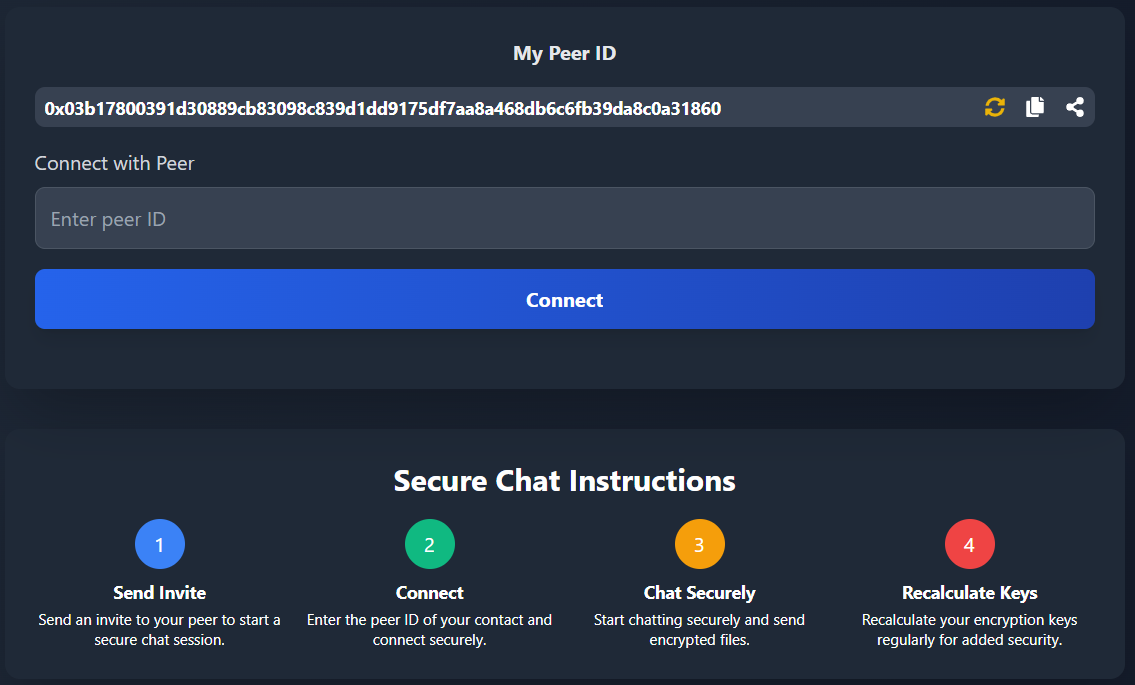




**Chat Page-**

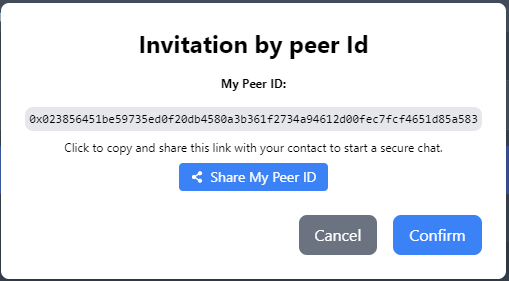
In the Chat page, you can connect to a desired Peer. To do so, copy the PeerID of the person you wish to connect with and click on the "Connect" button. If an invalid PeerID is entered, an appropriate error message will be displayed.

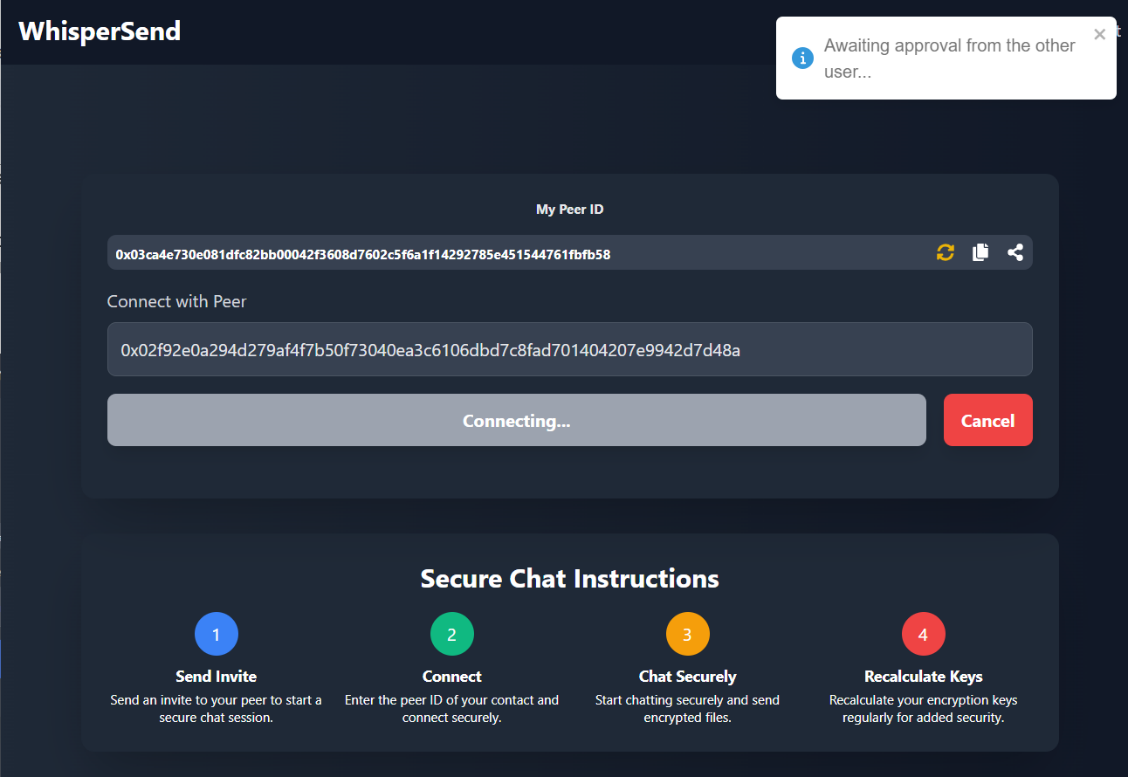




** Recalculate Key:** You can replace your encryption keys whenever you want to renew them, which will create a new session on the website.

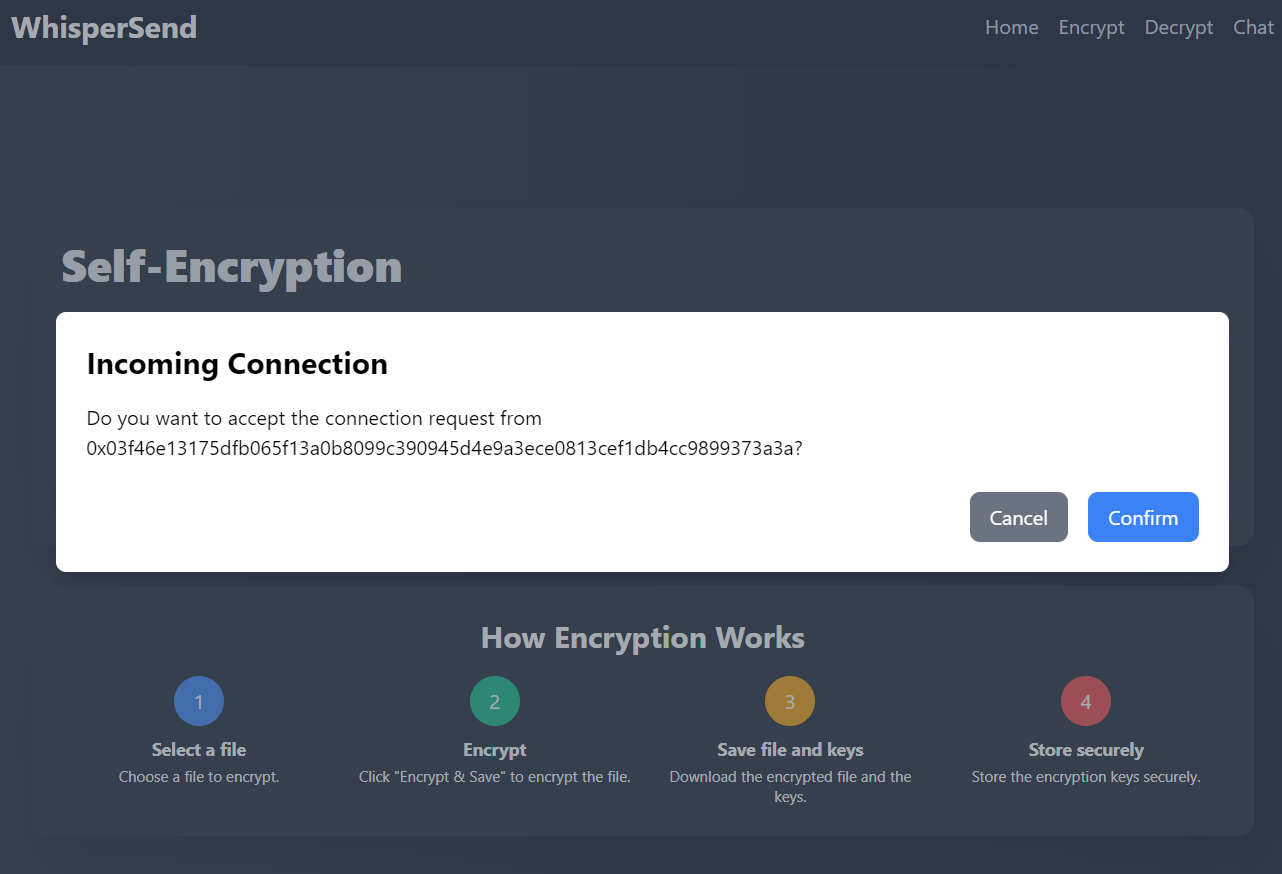
 **Copy Peer Id:** You can copy your peer Id.

 **Invitation share link:** You can send your connection information through a variety of social networks or through email.



 **Cancel connection:** You can click on the "Cancel" button to cancel the connection request, which will terminate the connection attempt

**Incoming Connection Message:**

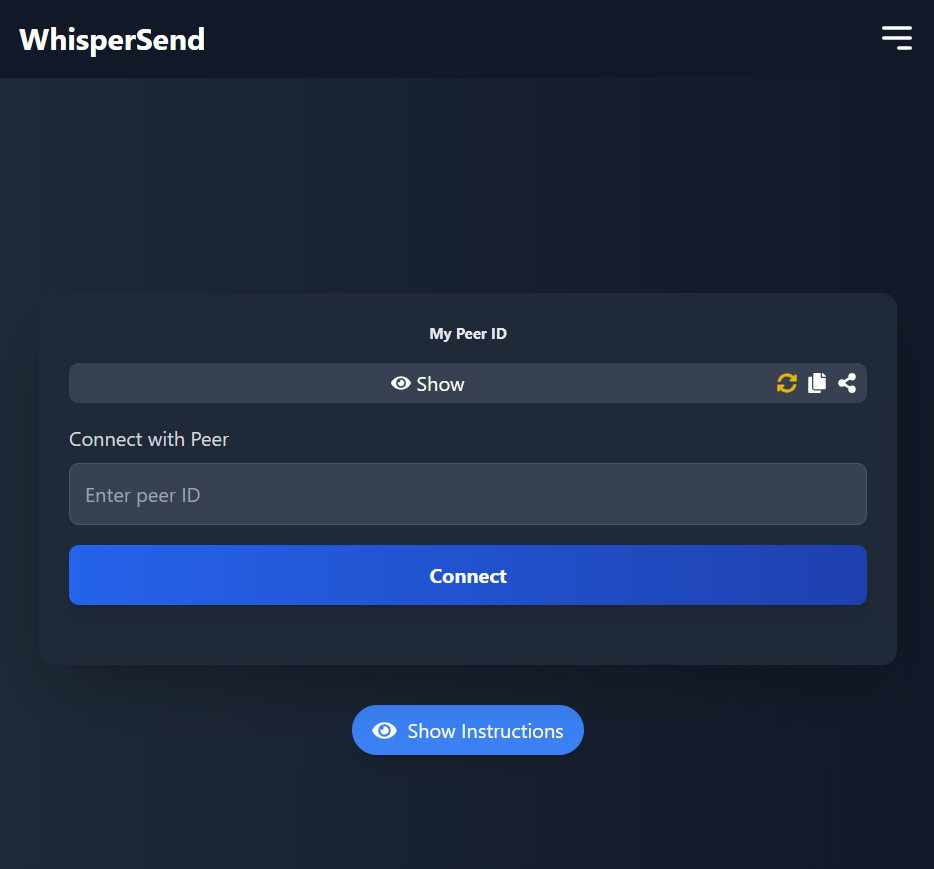
When a user wants to start a conversation with you, a notification will be displayed. Only after you accept the request, both of you will be connected and redirected to the chat page.

On small screens and mobile devices, those features will be displayed like this:



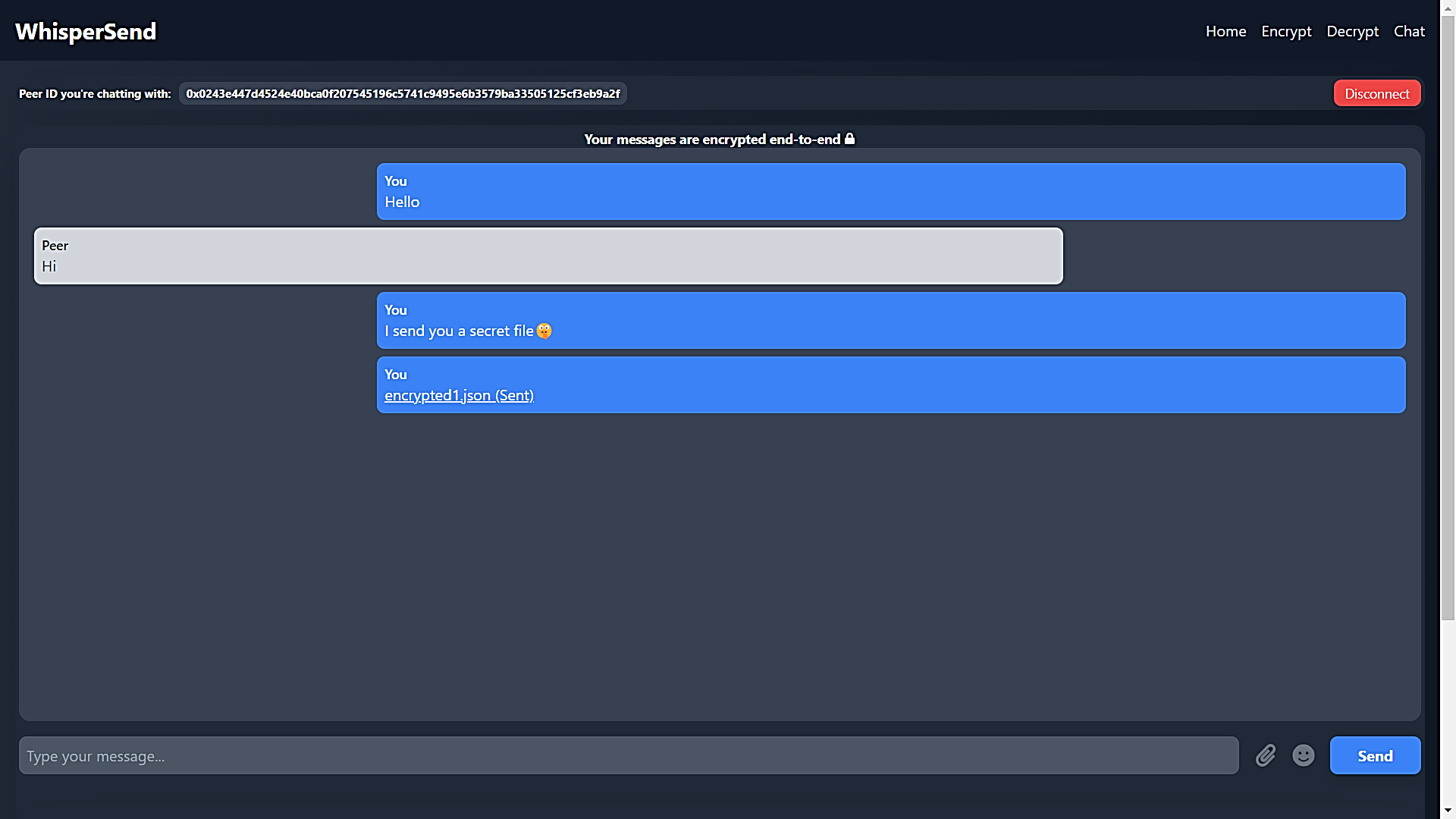
-Click this button to see your PEER ID.

-Click this button to watch the instructions.

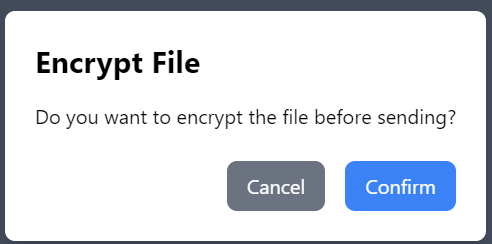


In the chat page, you can send and receive various file types—texts, images, documents, and more. To send an encrypted file, attach it and confirm encryption when prompted. If you wish to send the file unencrypted, select "Cancel Encryption." When receiving a file, if it's encrypted, you'll have the option to decrypt it or leave it as is.

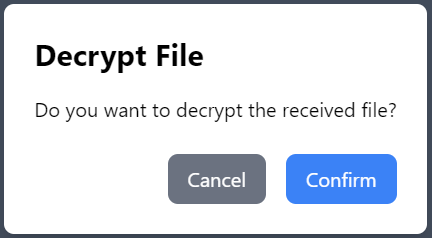
All messages in the chat are encrypted, ensuring your data remains secure and protected.



-Click here to send a file, you can choose if you want to Encrypt it or not.



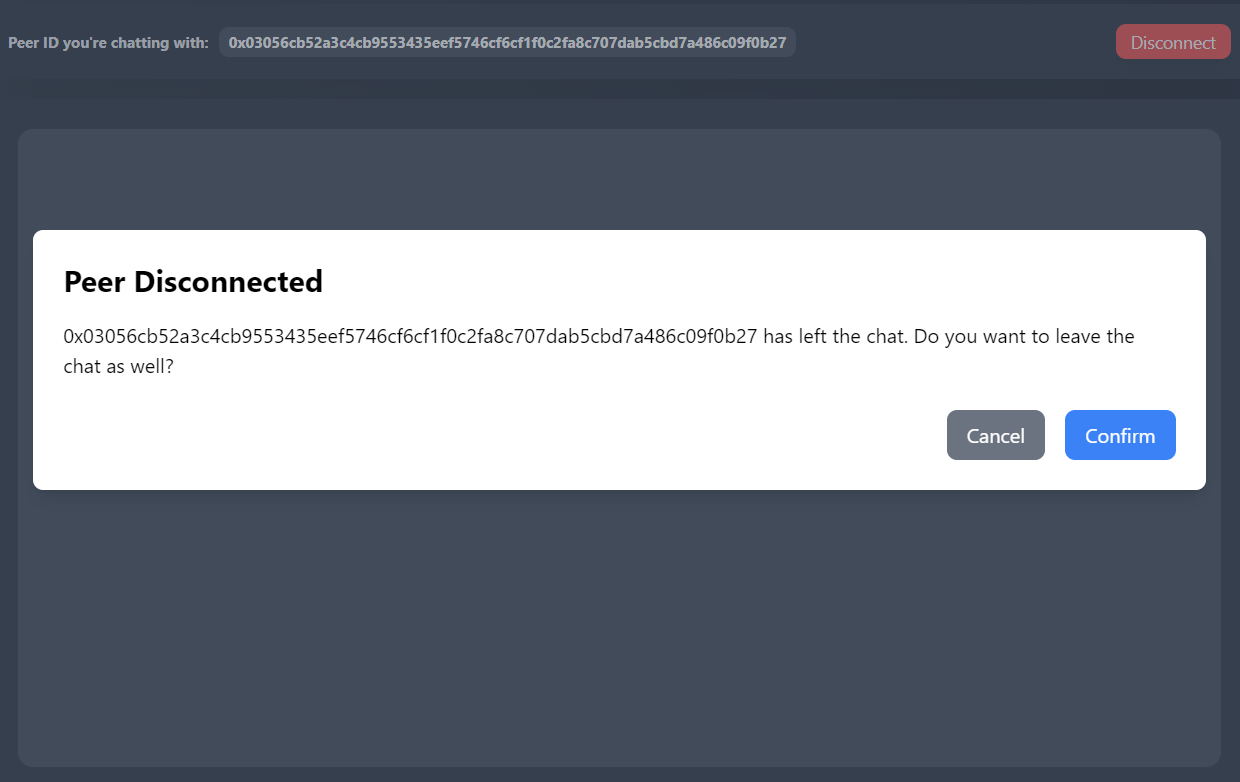
When you get an encrypted file, you need to choose if you want to decrypt it or download it as encrypted file. If you choose not to decrypt, you must save the PeerID of the person you're chatting with, otherwise, you won't be able to decrypt the file later.



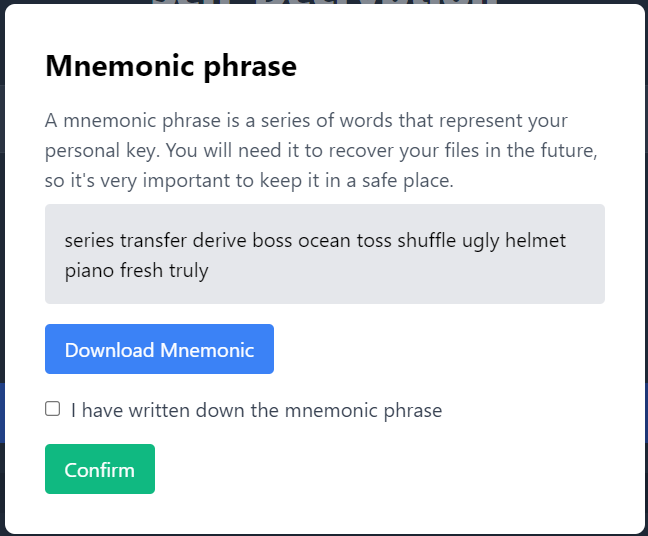


-Click here to disconnect from chat and end the connection with the other peer.

When peer will disconnect from the chat the remain will be notify and can choose if to leave the chat also:



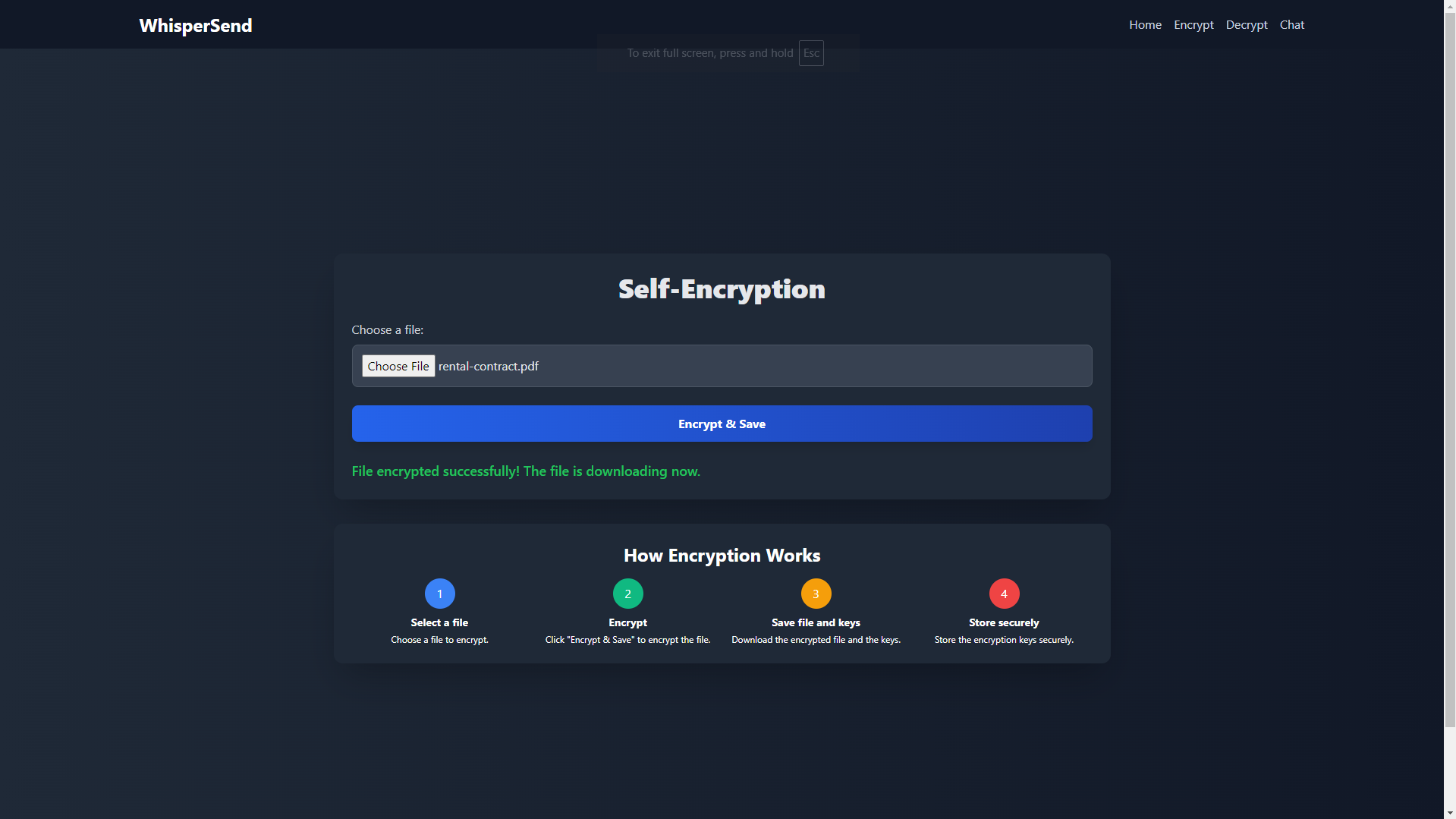
The mnemonic modal shows a sequence of words representing your session keys. It appears once on the encrypt, decrypt, and chat pages. You must save these words to decrypt files later. Confirm saving the mnemonic, or the notification will stay visible.



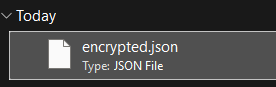
**Self-Encryption-**

Select a file from your computer that you wish to encrypt. The file will be encrypted using the encryption keys from your current session on the website.

To decrypt the file later, you will need to input the mnemonic you saved. The encrypted file will be automatically downloaded.

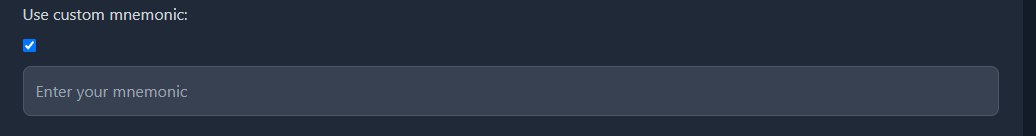


This is what the encrypted file will look like in your downloads:

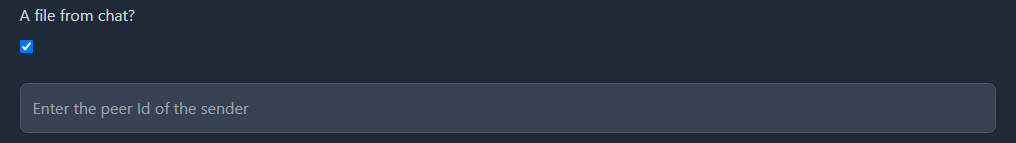


**Self-Decryption -**

On the decryption page, users can upload an encrypted file and choose from two options for decryption:

1.Input an old mnemonic: you can use a mnemonic saved from a previous session to decrypt older encrypted files.If you upload a file from a previous session, you will need to check the "use custom mnemonic" option and enter the mnemonic you saved from that session.

If it's a file you received encrypted in the chat, you will need to check the "A file from chat" option and enter the PeerID of the person who sent it to you.



2. Use the current session's mnemonic: If no key is entered, the file will be decrypted using the mnemonic from the current session on the website. If you encrypt and decrypt in the same session on the website, you can use it. If the decryption process is successful, the encrypted file will be automatically decrypted.

