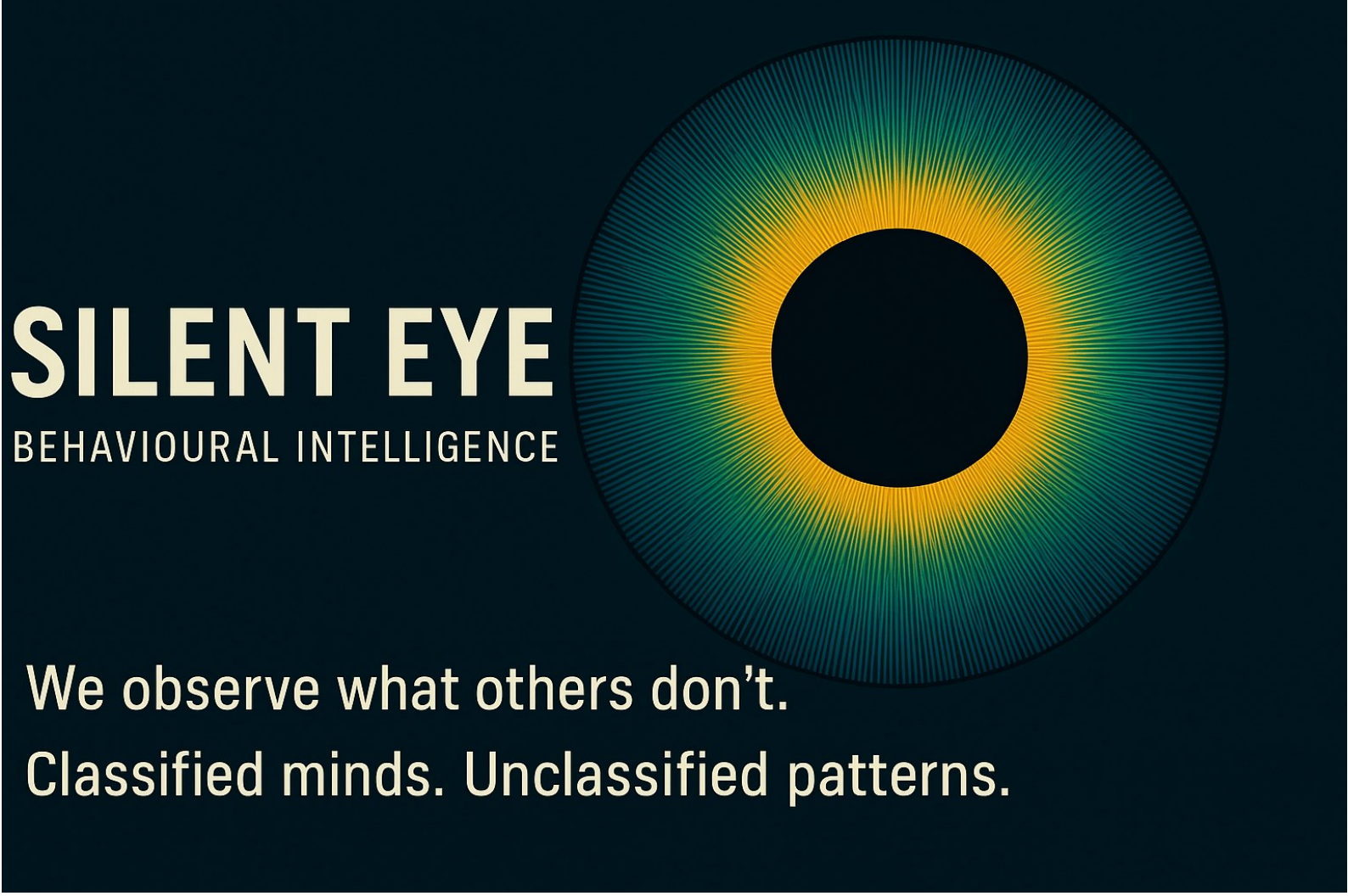

SILENT CHAT

Secure Chat & File Transfer – User Manual

What is SILENT CHAT?

SILENT CHAT is an ultra-secure desktop application for encrypted communication and file transfer between two computers.
There are **no central servers, no registration, no accounts, no metadata stored anywhere**.
All communication is **direct, peer-to-peer**, and protected by state-of-the-art encryption.
You are in full control of your data.
The final program is delivered as a standalone executable – you **do not need any other dependencies**. Just run and connect.

Why Use SILENT CHAT?

- **Absolute Privacy**: There are **no intermediaries**. Your messages and files are never routed through a third party.

- **Strong Encryption**: Every bit of data is encrypted using AES-GCM (AES-256 in GCM mode), with unique random keys generated for each session.
- **No Metadata Leakage**: No message logs, no cloud storage, no server handshakes – nothing is stored, nothing is intercepted.
- **No Installation Required**: Just run the `.exe` on both computers. No need for admin privileges or additional software.
- **Open Design**: Encryption keys are never shared automatically – you control how, where, and when to exchange them.
- **Simplicity**: Minimal interface, one-click operation. If you can copy-paste, you can use SILENT CHAT.

System Requirements

- **Windows 10 or higher** (64-bit)
- Internet connection (or local network for LAN use)
- Outbound port access (default is 45678, but can be changed)
- The same executable must run on both computers

Security Model (How It Works)

- **Peer-to-peer only**: No relay servers, no cloud. The connection is direct.
- **End-to-end encryption**: Every message and file is encrypted on the sender's machine and only decrypted on the receiver's.
- **No password recovery, no logs**: If you lose your encryption key, there's no backdoor. If you close the chat, the history is gone forever.
- **Random strong keys**: Key generation uses cryptographically secure random bytes, encoded as base64.
- **No protocol negotiation over the network**: The only secret is the key – exchanged **manually and only once per session**.

Getting Started

1. Launch SILENT CHAT

Double-click the SILENT CHAT `.exe` on both computers. The main window opens.

2. Set Port (Optional)

- By default, port **45678** is used.
- If your firewall/router blocks this port or if you want extra privacy, choose a different port.
- The port **must be the same on both computers**.

3. Generate a Secure Encryption Key

- Click **Generate Key**.
  A long, random key will appear in the field.
- **Important**: This key is your session's secret. **Share it securely with your chat partner using a different channel** (e.g., WhatsApp, SMS, phone call, Signal, etc.).
- **Do not send the key using SILENT CHAT itself!**

4. Set Up IP and Role

- **Decide who is "waiting" (the server) and who is "connecting" (the client):**
  - One computer clicks **Wait for Connection** and tells the other their **public IP address** (displayed in the app).
  - The other computer enters that IP in the **IP field** and clicks **Connect**.
- Both must use the **same port and key**.

5. Connect

- Once the connection is established, both users can start exchanging encrypted messages and files.
- The chat window will show connection status, info, and all exchanged content.

File Transfer

- Click **File** to send any file (image, document, etc.).
- The recipient will be asked to save the file and, if it's an image, it can be previewed directly.

Security Best Practices

- **Exchange the encryption key only through trusted channels** – never send it over the same internet connection you will use for chat.
- **Change the key, IP, and port for every session** – this prevents replay and brute-force attacks.
- **Close the application after your session** – nothing is saved, so your messages and keys are never recoverable by third parties.
- **Do not use weak or short keys** – always use the built-in Generate Key function.

Troubleshooting

- If you cannot connect:

    - Check both computers' firewalls and router port forwarding (ensure chosen port is open).
    - Double-check that both sides use **the same key** and **the same port**.
    - Use the public IP address for connections across the internet; use local IP for LAN connections.
- If you see "Invalid key" or "connection closed", check that you have copied the key exactly, with no spaces or missing characters.

FAQ

Q: Is my chat really private?
A: Yes. All messages and files are encrypted on your computer before being sent, and only decrypted by the other end. No third party can intercept or read your data.

Q: What happens if I lose the key or close the app?
A: The session is lost and cannot be recovered. There are no logs, no cloud, and no way for anyone (including the author) to recover past data.

Q: Can I use this for group chats or more than two computers?
A: No. SILENT CHAT is strictly peer-to-peer (one-to-one) for maximum security.

Q: Is it open source?
A: Yes, the design is open for inspection and the source code is available if you need to audit or compile yourself.

Final Notes

SILENT CHAT is for users who want uncompromising privacy and control.
It is the digital equivalent of meeting in a dark alley with a one-time pad — except more convenient and much more secure.

If you value your privacy, distrust clouds and big tech, and want communication that leaves no trace, this is your tool.

Developed by Octávio Viana | Silent Eye Project | 2025