

Guidelines for Accessing Encrypted Thesis Files

1. Why is this file encrypted

This repository contains transcripts and documents related to my Master's thesis research. They include sensitive interview data and, therefore, are not stored in plain text. To ensure confidentiality, all files are encrypted with AES-256 (via GnuPG) before being published on GitHub.

Only contributors or researchers with the correct passphrase can access the contents.

2. File format

Encrypted files have the extension:

Interviews-Transcripts.docx.gpg

This means the original .docx has been encrypted using GPG (GNU Privacy Guard).

3. How to decrypt the file

On macOS / Linux

1. Open Terminal.
2. Navigate to the folder containing the file:
`cd /path/to/folder`
3. Run:
`gpg -d filename.docx.gpg > filename.docx`
4. Enter the passphrase when prompted.
5. Open the resulting .docx file with Microsoft Word or LibreOffice.

On Windows

1. Install Gpg4win (<https://www.gpg4win.org/>).
2. Right-click on the .docx.gpg file → Decrypt and Verify.
3. Enter the passphrase when asked.
4. The decrypted .docx will appear in the same folder.


Alternatively, you can use gpg from Command Prompt or PowerShell, just like on macOS/Linux.

4. Security notes

- Never share the decrypted .docx in public repositories.
- Store the passphrase in a password manager, not in plaintext.
- If you accidentally commit the unencrypted file, you must rewrite Git history (deleting in a later commit is not enough).

5. Contact

For access requests or troubleshooting, please contact:

 spadarosalvator@gmail.com