



Detailed User Manual: MisiemCrypt AES-256

Software Version: 2.0 (Windows Context Menu Integrated)

Publisher: StacjaMiś | Michał Kordyszewski

Contact: kontakt@stacjamis.pl

Website: www.stacjamis.pl

Developer Support: <https://buycoffee.to/stacjamis>

1. About the Program

MisiemCrypt AES-256 is a lightweight, modern, and intuitive application designed for maximum security of your sensitive data. The program allows for lightning-fast protection of files and entire folders using ZIP archives encrypted with the advanced AES-256 algorithm – an international cryptographic standard utilized by financial institutions and government agencies. This tool is the perfect solution for business and professional environments: it allows for the secure encryption of documents and data before sending them via e-mail or instant messaging platforms, ensuring full compliance with data protection requirements (GDPR). This "One-Click" application requires no installation, environment configuration, or internet connection.

2. Step by Step: How to use the application?

The program offers four main modules. Choose the one that suits your needs:

Module D: Quick Actions from Windows Context Menu (Most Convenient)

Allows for instant encryption and decryption directly in the system, without opening the main program window.

- How to enable: Close the program if it's open. Right-click the "kryptor.exe" file and select "Run as administrator". In the main window, click the red button "  Add to Windows Menu". You only need to do this once!
- Packing multiple files: Select any files or folders, right-click and choose "Send to" -> "Secure in MisiemCrypt".
- Unpacking on the fly: Right-click a secured .zip archive and select "  Secure in MisiemCrypt AES". The program will automatically detect the archive and switch to unpacking mode.



Module A: Pack files with password

Used to encrypt single or multiple selected files from the open application.

- Launch the application and click the "Pack files with password" button.
- In the file explorer window, select the files you want to protect. (Tip: hold down the CTRL key to select multiple individual files).
- A window prompting for a password will appear. Enter a strong password and confirm by clicking OK.
- Choose a location on your drive where the program should save the generated, secure .zip file and give it a name.

Module B: Pack folder with password

Used to encrypt entire directories (including all subfolders and files within them) while maintaining their original structure.

- Click the "Pack folder with password" button.
- Select the target folder on your drive and click "Select folder".
- Enter a secure password that will serve as the key to your archive.
- Choose the destination where the secure .zip file should be saved.

Module C: Unpack archive

Used to decrypt and extract data from secured archives.

- Click the "Unpack archive" button.
- Locate and select the secured .zip file on your drive.
- Enter the correct password that was used during the packing process.
- Select the destination folder where the decrypted files should be extracted.

3. Critical Security Warning

The AES-256 algorithm used in the program does not have any "backdoors" or password recovery mechanisms. In the event of a forgotten or lost password, decrypting the data and recovering the files is technologically impossible, regardless of the computer hardware used. The user bears full responsibility for the secure management of their passwords.

4. Detailed Privacy Policy and Legal Compliance (GDPR / CCPA)

When creating MisiekCrypt AES-256, our priority was to ensure absolute discretion regarding your actions. Therefore, the program was designed following the highest "Privacy by Design" standards.

- **100% Offline Operation (Local Processing):** The application does not require an internet connection to function. All packing, encryption, and decryption operations take place entirely locally on your device's storage and processor.
- **No Data Collection:** The program does not collect, process, store, or transmit any personal data, metadata, entered passwords, IP addresses, or the contents of encrypted files.
- **No Telemetry or Spyware:** The application is completely free of analytical scripts, trackers, and any error-reporting mechanisms directed to external servers.
- **Compliance with European GDPR (RODO):** Since the software does not process any personal data within the meaning of EU data protection regulations, the use of the application is compliant with GDPR guidelines by default. StacjaMiś does not act as a Data Controller or Data Processor for the program's users.
- **Compliance with US Regulations (CCPA / CPRA):** The application meets the strict requirements of US privacy protection laws, including the California Consumer Privacy Act (CCPA). We guarantee that no user data is "sold" or "shared" with third parties, as the software does not acquire any data whatsoever.

5. Copyright and End-User License Agreement (EULA)

© 2026 Michał (Misiek) Kordyszewski. StacjaMiś. All rights reserved.

This software ("MisiekCrypt AES-256") is provided under a Freeware license. By using the program, you agree to the following terms:

- **Permitted Use:** You have the right to freely download, copy, and use the program on any number of computers. The software may be used for both private and commercial (business) purposes.
- **Restrictions:** Reverse engineering (decompilation), modification of the source code or application interface, and the removal of the creator's copyright notices are strictly prohibited.
- **No Resale:** The application is and will always remain free. It is prohibited to sell, license, or include it in paid software packages without the written consent of the author.
- **Disclaimer of Warranties:** The program is provided "as is". StacjaMiś and Michał Kordyszewski bear no responsibility (financial, legal, or moral) for data loss, hardware damage, business interruptions, or any other direct or indirect damages resulting from the use or inability to use the program (including situations arising from a forgotten cryptographic password). The user uses the software entirely at their own risk.

Do you like the program and did it make your life easier? Creating secure tools is my passion. If you want to support the further development of my projects, you can do so by buying me a symbolic, virtual coffee: <https://buycoffee.to/stacjamis>

