Flash Drive Encryptor (AES-GCM)

Professional Documentation & Industry Applications

Prepared by: [Your Company/Team Name]
Date: 2025

Introduction

The Flash Drive Encryptor is a Python-based application that provides strong AES-GCM encryption for securing sensitive files on flash drives or other storage media. It comes with both a command-line interface and a graphical user interface (GUI), making it accessible for both technical and non-technical users.

Key Features

- AES-256 encryption in GCM mode (confidentiality + integrity).
- Derives encryption keys securely from passphrases using PBKDF2.
- Supports both file and directory encryption/decryption.
- Option to recursively process subdirectories.
- Ability to delete original files after encryption or decryption (with caution).
- Cross-platform: works on Windows, Linux, and macOS.
- User-friendly GUI for easy operation.

Encryption Workflow

The following diagram illustrates the encryption process using AES-GCM. A passphrase is converted into a key via PBKDF2, which is then used to encrypt files. Each file has its own salt and nonce to ensure uniqueness and security.

[Insert Diagram: Passphrase -> PBKDF2 -> AES-GCM -> Encrypted File]

Practical Applications in Industry

- Healthcare: Protecting patient records on portable media to comply with HIPAA and other data protection standards.
- Finance: Securing sensitive client data and financial reports stored on removable drives.
- Legal Sector: Encrypting case files and evidence shared on physical media to ensure confidentiality.
- Corporate Environments: Safeguarding intellectual property, product designs, or sensitive strategy documents.
- Government and Defense: Ensuring classified information remains secure when transferred via flash drives.
- Education and Research: Protecting research data, exam papers, and confidential student records.
- Personal Use: Safeguarding personal files, ID scans, and private media while traveling with flash drives.

Setup Instructions

1. Install Python 3.7 or later.
2. Ensure 'flash_encrypt.py' and 'flash_encrypt_gui.py' are in the same folder.
3. Install required dependencies: pip install pycryptodome.
4. On Linux, install tkinter if missing: sudo apt-get install python3-tk.
5. Run the application: python3 flash_encrypt_gui.py.

Usage Guidelines

1. Open the application and select a file or directory.
2. Enter a secure passphrase.
3. Choose whether to encrypt or decrypt.
4. Optionally enable recursive processing or file deletion.
5. Click 'Run' and monitor progress in the log window.

Best Practices

- Always use a strong, unique passphrase that is not reused across systems.
- Do not enable 'Delete originals after operation' unless absolutely necessary.
- Regularly back up encrypted files to multiple secure locations.
- Verify decryption on test files before deploying widely in production.

Conclusion

The Flash Drive Encryptor provides a simple yet powerful way to safeguard sensitive data on removable storage devices. Its strong encryption and ease of use make it highly practical across industries where data protection is critical.