**What This Project Does**

**Project/Tool Description:** Encrypted Cloud File Sync

This tool securely encrypts files and syncs them with Google Drive, protecting sensitive data in the cloud while giving full control over encryption keys.

**Main Functionalities:**

**File Encryption:**

Encrypts files from a local folder using a unique encryption key for each file.

Wraps individual file keys with a master key for extra security.

**Google Drive Integration via API:**

Uses Google Drive API to upload encrypted files to the cloud.

Downloads encrypted files from Google Drive when decryption is needed.

Checks for duplicates using both local metadata and Drive API queries to prevent multiple uploads.

**Master Key Management:**

Generates a master key to encrypt all file keys.

Supports KEK (Key Encryption Key) to encrypt the master key locally.

Ensures master key security while keeping it usable for decryption.

**Decryption:**

Allows decryption of files from Google Drive using the master key (and KEK if enabled).

Saves decrypted files in a separate local folder.

**Automatic Key Rotation:**

Can rotate the master key automatically every 7 days.

Updates all file keys securely to the new master key without re-encrypting the files themselves.

**Metadata Management:**

Maintains a JSON file of file keys and encryption metadata.

Prevents accidental duplicate encryption or upload.

**Interactive Terminal Menu:**

Simple menu for decrypting files or exiting the program.

**APIs Used:**

Google Drive API – for uploading, downloading, and managing encrypted files in the cloud.

Google OAuth API – for secure authentication and authorization to access Google Drive.

**Summary:**

This tool provides a secure, cloud-integrated solution for encrypting, storing, and managing sensitive files using Google APIs. It ensures strong encryption, key management, and automated key rotation while keeping your workflow simple and secure.