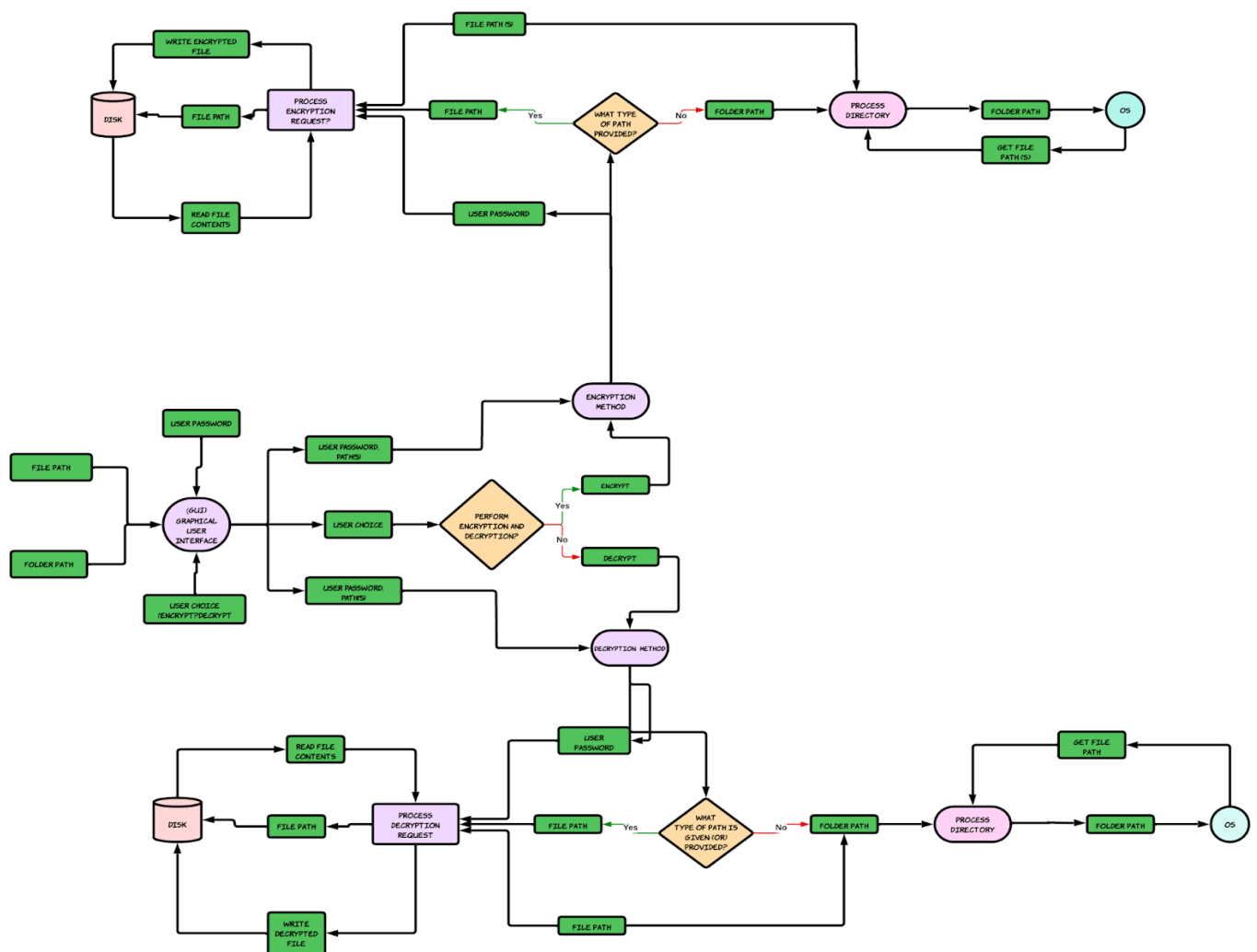# APPLICATION WORK FLOW:-

The application workflow is designed to ensure a seamless yet highly
secure process for encrypting and decrypting user files. Here's a
detailed look at the steps involved:

User Authentication:-

The user initiates the application and is prompted to enter a secure passphrase. This
passphrase will be used as a key component in encrypting the File Encryption Key.
The application employs a Key Derivation Function (KDF) to convert the user passphrase
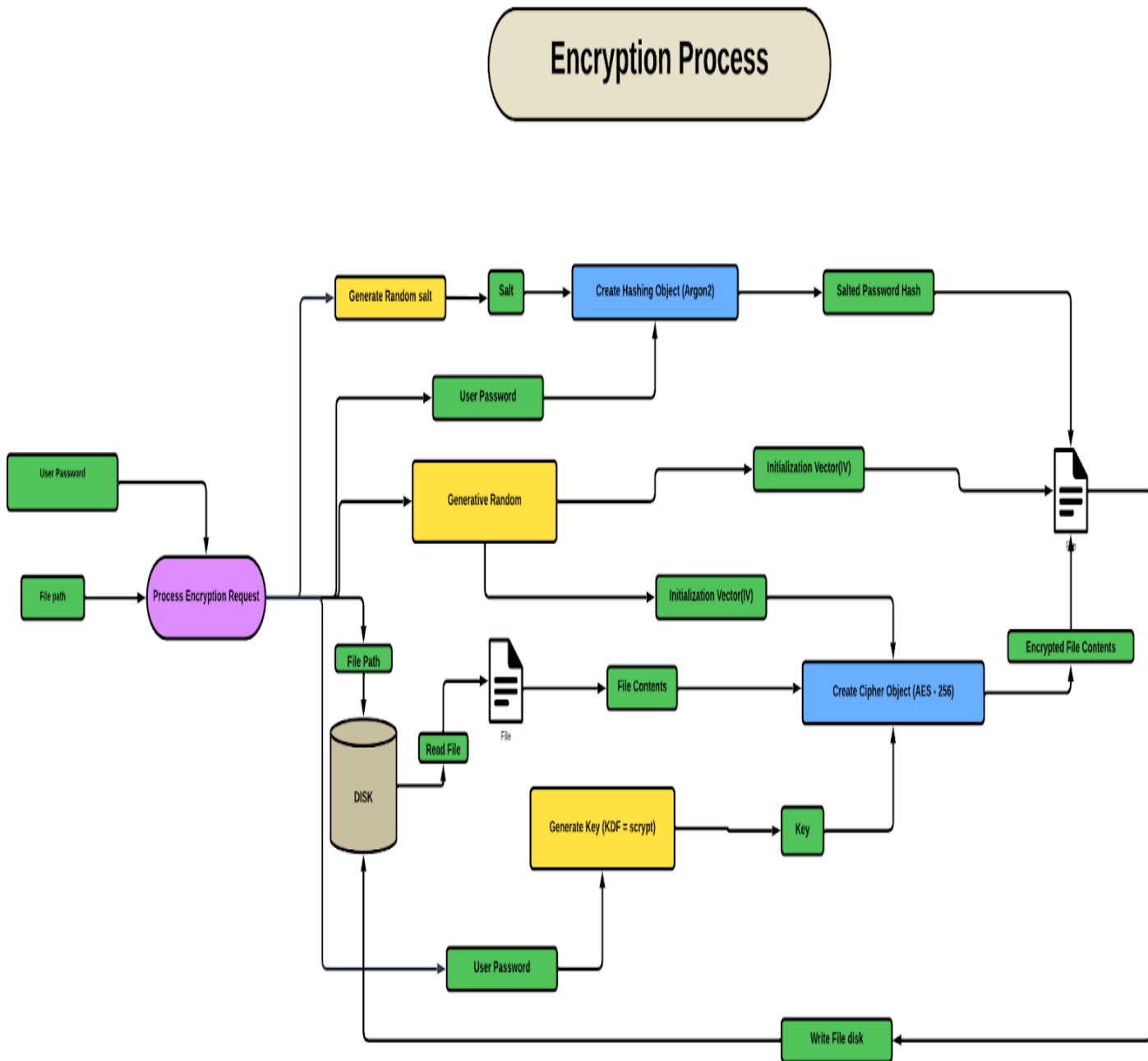into a cryptographic key.

File/Director Selection:-

The user selects the file or directory they wish to encrypt from the file system.
The application allows browsing through directories and choosing multiple files if needed

File Encryption:-

**A random File Encryption Key is generated using a secure random number generator.
The selected file or directory is encrypted using AES-256 encryption with the generated File Encryption Key**

Encryption Process

Generate Random salt → Salt → Create Hashing Object (Argon2) → Salted Password Hash

User Password

User Password

File path

Process Encryption Request

Generative Random → Initialization Vector(IV)

Initialization Vector(IV)

File Path

Read File

File

File Contents → Create Cipher Object (AES - 256)

DISK

Encrypted File Contents

Generate Key (KDF = scrypt) → Key

User Password

Write File disk

Decryption Process:

When the user needs to access the encrypted file, they must enter their passphrase.
The application uses the KDF to derive the decryption key from the user passphrase.
If the passphrase is correct, the File Encryption Key is decrypted.
The decrypted File Encryption Key is then used to decrypt the file, making it accessible to the user.