**File Encryptor**

**Description:**

This program offers a user-friendly interface to encrypt any file using AES and Fernet (Select from the dropdown menu of “Encryption Type”) and decrypt it later if needed. To run the file encryptor, open the “Open\_Here” folder and run “File\_Encrypt”

**Encrypting**

**Encrypt AES:**

When encrypting with AES, ensure the encryption key is 16, 24, or 32 characters because AES requires the key to be 128-bit, 192-bit, or 256-bit. The 16 represents the 128-bit, the 24 represents the 192-bit, and the 32 represents the 256-bit.

**Encrypt Fernet:**

Fernet requires a specific key that is 128-bit URL-secure. This key can be obtained by clicking “Generate Key for Fernet.” That would create a file called “mykey.key” (Each time it is clicked, a new key is generated in the same file. **Note:** Move the file to a different folder if you need it for later and you want to generate a new one. After the key is generated, copy the key and paste it into the “Encryption Key” box (Don’t use the same key for all files as it is not recommended for security purposes).

**Decrypting**

**Decrypt AES:**

Make sure AES is selected in the “Encryption Type,” then select the file you want to decrypt. Enter the key that was used during encryption into the “Encryption Key” box. Click decrypt, and the file should be decrypted. **Note:** If the original (unencrypted file) is in the same destination as the encrypted file, the original file will be overwritten if they have the same name.

**Example:**

File password1.docx was encrypted, then file password1.docx was modified. Decrypting password1.enc would return password1.docx before modification. (To avoid this, rename password1.docx to password2.docx after modification to prevent an overwrite)

**Decrypting Fernet:**

Make sure Fernet is selected in the “Encryption Type,” then select the file you want to decrypt. Copy and paste the key that was used during encryption into the “Encryption Key” box. Click decrypt, and the file should be decrypted. **Note:** If the original (unencrypted file) is in the same destination as the encrypted file, the original file will be overwritten if they have the same name.

**Example:**

File password1.docx was encrypted, then file password1.docx was modified. Decrypting password1.enc would return password1.docx before modification. (To avoid this, rename password1.docx to password2.docx after modification to prevent an overwrite)