


```

1  from cryptography.fernet import Fernet # 암호화 라이브러리
2  import os # OS 라이브러리
3  import sys # 시스템 라이브러리
4  import hashlib # 암호화 라이브러리
5  import getpass # 비밀번호 입력 라이브러리
6
7
8  ✓ def main(): # 4. 메인 코드
9      # 5. 모드 선택
10     mode = int(input("암호화{(1)} / 복호화{(0)}: ".format(chr(128274), chr(128275))))
11
12     try:
13         filename = input("파일 이름을 입력해 주세요(확장자까지 모두!): ") # 6. 파일 이름 입력
14         with open(filename, 'rb') as original_file: # 7. 파일 읽어오기
15             original = original_file.read()
16             original_file.close()
17     except FileNotFoundError: # 7-1. 파일이 없을 때
18         print("그런 파일은 없어요...{}".format(chr(129768)))
19         main()
20     else:
21         if mode == 1: # 암호화
22             encrypted = certKey.encrypt(
23                 certKey.encrypt(original)) # 8-1. 파일 이중 암호화
24             encrypted_filename = filename + ".fileShelter" # 9. 확장자 덧붙이기
25             with open(encrypted_filename, 'wb') as result:
26                 result.write(encrypted) # 10. 저장
27                 result.close()
28             os.remove(filename) # 10. 원본 파일 제거
29
30         if mode == 0: # 복호화
31             decrypted = certKey.decrypt(
32                 certKey.decrypt(original)) # 8-2. 파일 이중 복호화
33             decrypted_filename = filename[0:-12] # 9. 확장자 변경 해제하기
34             with open(decrypted_filename, 'wb') as result:
35                 result.write(decrypted) # 10. 저장
36                 result.close()
37             os.remove(filename) # 11. 암호화된 원본 파일 제거
38         print("끝!")
39         input("아무 키나 눌러 프로그램을 종료하세요.")
40
41

```

```

41
42 print("""
43 암호화 도구 준비 끝{}
44 cert.key 인증서 파일이 동일 디렉토리에 존재하는지 다시 한번 확인해 주세요.
45 """.format(chr(9989))) # 시작 부분
46
47 try: # 시도
48     with open('cert.key', 'rb') as CertKeyFile:
49         certKey = Fernet(CertKeyFile.read()) # 1. 인증서 읽어오기
50         CertKeyFile.close()
51
52         passwd = "13c56b057a9776819bf622c848f800cfabec64095ea6cc380d230930482f8ec9" # 가상의 비밀번호 해시값
53         userPasswd = getpass.getpass("비밀번호: ") # 2. 사용자가 직접 비밀번호를 입력
54         sha = hashlib.sha256() # 암호화 준비
55         userPasswd = sha.update(userPasswd.encode(
56             'utf-8')) # 3. 인증 과정(해시 함수 사용)
57         userPasswd = sha.hexdigest() # 객체(데이터)로 나온 값을 문자로 표시
58         userPasswd = sha.update(userPasswd.encode(
59             'utf-8')) # 인증 과정 2차(해시 함수 사용)
60         userPasswd = sha.hexdigest() # 객체(데이터)로 나온 값을 문자로 표시
61         if userPasswd != passwd: # 3-1. 비밀번호가 틀릴 때 종료
62             print("비밀번호가 틀려요...{}".format(chr(129768)))
63             input("아무 키나 눌러 프로그램을 종료하세요.")
64             sys.exit()
65     except FileNotFoundError: # 1-00PS. 인증서가 없을 때 또는 인식이 안 될 때
66         print("인증서가 없거나 인식이 안 돼요!{}".format(chr(129768)))
67         print("프로그램과 같은 위치에서 cert.key라는 이름으로 존재해야 해요!")
68         input("아무 키나 눌러 프로그램을 종료하세요.")
69         sys.exit()
70 else:
71     while True:
72         main() # 3-2. 비밀번호까지 일치할 때 메인 암호화/복호화 코드 실행
73         ifContinue = int(input("계속!(1) / 그만!(0): ")) # 반복
74         if ifContinue == 0:
75             sys.exit()

```


