FileEncoder

This is a file encoder & decoder made with python, the basic encoding method is RSA. We also provide some check-sum methods.

若无法运行，请尝试执行如下命令

```
pip install pyqt5
pip install Crypto
pip install base64
pip install rsa
pip install pywin32
```

软件使用说明如下：

1，本软件提供RSA加解密，RSA签名认证，文件求和校验，AES加密。

2，如果电脑中已经有符合要求的 RSA 公钥和私钥，那么就不需要使用生成密钥对的功能了，直接使用现有的即可（注意！如果此时点击了生成密钥的功能，会无提示地覆盖掉用户文件夹中.ssh 文件夹中的文件，引起不必要的麻烦。如果没有的话，请按照软件的指示，生成 SSH 公钥和私钥。由于生成的密钥是 3072 位的，会稍微有点慢，请稍等。

3，RSA与AES加密前会进行base64处理（可能还有长度填充），所以此处加密的文档未必能在其它软件下正确解密。

4，使用 RSA 进行加密和解密时，请务必使用公钥进行加密，私钥进行解密，否则会出现错误。注意，指定文件保存目录与名字时请按需设定拓展名，否则程序会将源文件的拓展名赋给加密后的文件）同时，请务必确保使用的密钥是配对的，否则无法进行解密。 注意，使用的密钥是符合 PKCS1 标准的，openSSH 的密钥暂时无法使用 。

5，同理，进行RSA签名认证时，请使用私钥签名，公钥解密，并且请注意保留指纹以便查验，程序不会自动导出该值。

5，MD5，SHA256 是两种常用的求和校验，但是这种算法一般是不可逆的。软件中的这个功能只是用于数据校验，确保两个文件一致。在对大文件进行求和的时候可能比较慢，因为作者限制了一次只能读取 8096 字节进来，以防止读取文件时内存被超大文件对象占满

6，此AES加密仅使用了EBC，即没有偏移量的加密算法。注意，由于AES加密key长度必须为16的整数倍，所以不足16位的key会在后面补足\0，注意是\0，该符号不会输出但确实存在。同时，由于解密的字符串长度必须也是16的整数倍，所以加密和解密后的文本可能会多出几个空格（对应base64里面的等于号）