AES 算法算法报告

实验目的

熟悉 AES 算法加密和解密的过程，并且通过编程实现算法，达到对 txt 文件内容加解密的目的。

实验环境

JAVA
Eclipse
Windows
JDK 1.8

实验内容

用 java 语言实现 AES 算法，要求：

1. 程序能够读入指定的 txt 密钥文档；
2. 可以对指定的 txt 文档进行加密或者脱密处理，并生成对应的密文或者明文 txt 文档。

实验步骤

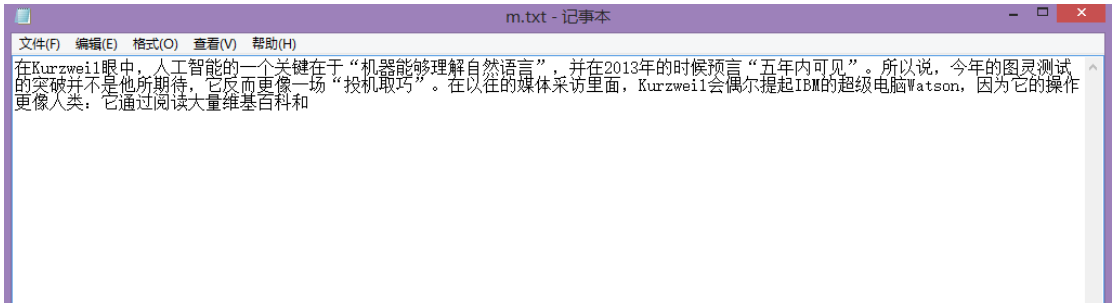
下面将通过运行过程来说明实验的步骤：
本次实验的源码主要包括三个类，分别是：AES.class, Encryption.class, Decryption.class，其中 AES.class 是主类，其他两个分别对应加密和解密的类。
注意，本次所有的 txt 文档都必须存在 D 盘根目录下才能正常读取。创建的新文档也会存在 D 盘根目录下。并且输入文件名直接输入文件名，不需要加后缀.txt

运行过程：

运行程序，出现如下信息：

```
**************************************************
What do you want to do? Please enter the number of the exact operation
1.Encode some file
2.Decode some file
3.Exit
Your choice:
```

输入 1 对指定的文档进行加密，并自己命名输出密文的文件名；输入 2 解码指定文件内容，并自己输入输出明文的文件名，输入 3 退出程序。
下面我们在 D 盘根目录下存入一个 m.txt 文件，其内容为：



我们在程序中输入 1,进入加密模式：

```
Your choice: 1
**************************************************
All files must be put in directory: D:/
Enter the file name of the password without .txt
```

我们输入 password 文件名作为密码文件名，m 文件作为明文输入文件，c 文件作为密文输出文件，password 中随便输入一串数字

```
Enter the file name of the password without
password
Not a valid file, please enter again:
```

如果文件不合法，就需要重新输入

因为 password 文件不存在，所以创建后重新输入

```
**************************************************
All files must be put in directory: D:/
Enter the file name of the password without .txt
password
Not a valid file, please enter again:
password
Enter the file name to be encrypted without .txt
```

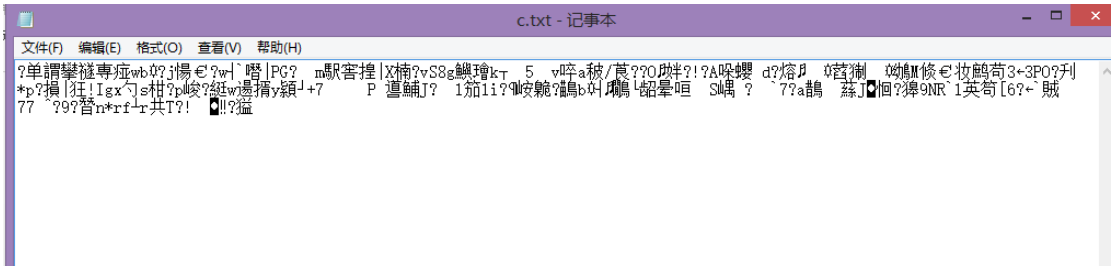
挤下来输入 m 和 c

```
**************************************************
All files must be put in directory: D:/
Enter the file name to be encrypted without .txt
m
Enter the file name to output the encrypted data without .txt
c
Encryption done!
**************************************************
```

查看 c.txt

```
All files must be put in directory: D:/
Enter the file name of the password without .txt
password
Not a valid file, please enter again:
password
Enter the file name to be encrypted without .txt
m
Enter the file name to output the encrypted data without .txt
c
Encryption done!
```

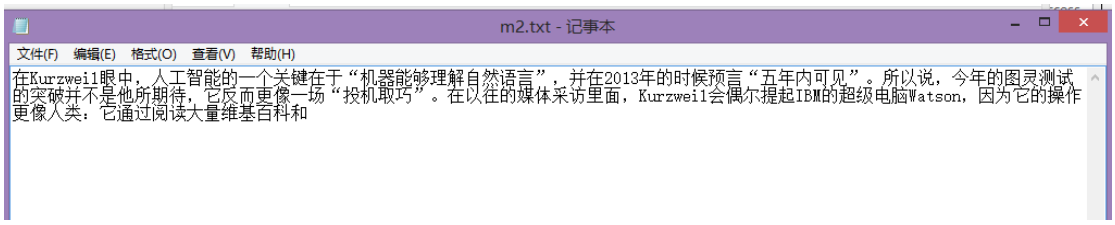
加密完成，可以在 D 盘根目录下看到一个 c.txt，是密文的文件



接下来继续解码，同样按提示读入相同的密码文件，并且输入密文文档和输出明文文档，这里输出到 m2.txt

```
All files must be put in directory: D:/
Enter the file name of the password without .txt
password
Enter the file name to be decrypted without .txt
c
Enter the file name to output the decrypted data without .txt
m2
Decryption done!
Decryption. 在Kurzweil眼中，人工智能的一个关键在于“机器能够理解自然语言”，并在2013年的时候预言“五年内可见”。所以说，今年的图灵测试的突破并不是他所期待，它反而更像一场“投机取巧”。在以往的媒体采访里面，Kur
************************************************************
```

除了控制台会输出解密信息，D 盘根目录下面也会产生一个 m2.txt 文件，用以保存明文信息



对照前面明文信息，发现完全相同。

详细的实现过程，在源码中有详细的注释信息。

实验的难点

对 AES 包的接口函数不熟悉，也没能找到详尽的说明，因此在使用过程中摸索花费了不少的时间。

另外，在读取 txt 文件的格式上做过了多种尝试，最后发现还是用字节的方式读取最方便，另外，在一开始的解密总是出错，后来发现和 txt 文件的编码格式有关。

由于接口函数比较全面，功能比较强大，因此并没有遇到其他方面的问题。