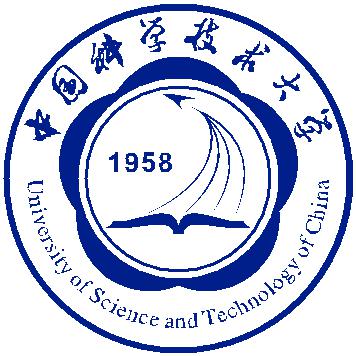


本科研究报告

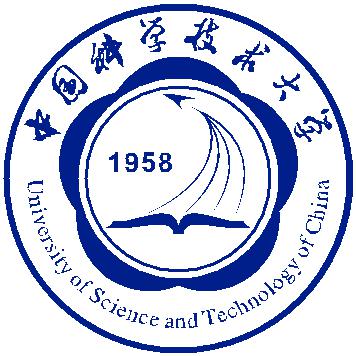


AES加密，解密工具

|  |  |  |  |
| --- | --- | --- | --- |
| 作者姓名： |  | 吴立凡 | |
|  |  |  |  |
| 学科专业： | 网络空间安全 | | |
|  |  |  |  |
| 导师姓名： |  | 李卫海 | |
|  |  |  |  |
| 完成时间： |  | 2020年5月 | |
|  |  |  |  |

University of Science and Technology of China

A research report for bachelor’s degree



AES encryption and decryption tools

|  |  |
| --- | --- |
| Author : | Lifan Wu |
| Speciality : | Cyberspace Security |
| Supervisor : | Weihai Li |
| Finished Time : | May, 2020 |

致谢

感谢CSDN的前辈们，他们的论文博客为本次实验提供了丰富的经验与建议。本次实验的结果验证也使用了CSDN上的工具。如果不是他们的帮助，这篇文章的完成也会变得无比艰难。

另外也要感谢所有教过我的老师们，他们所教授的许多内容都成为了我实践的坚实基础。在此特别感谢李卫海老师，他所教授的密码学导论为这篇论文提供了莫大的帮助。

目录

[摘要 5](#_Toc72941478)

[关键词 6](#_Toc72941479)

[Abstract 6](#_Toc72941480)

[Keywords 6](#_Toc72941481)

[正文： 7](#_Toc72941482)

[题目要求 7](#_Toc72941483)

[效果 7](#_Toc72941484)

[代码文件简述 7](#_Toc72941485)

[AES算法流程 8](#_Toc72941486)

[AES输入分组 9](#_Toc72941487)

[AES算法子密钥生成 10](#_Toc72941488)

[AES的轮函数 11](#_Toc72941489)

[AES解密 12](#_Toc72941490)

[加密在题目1中使用的书籍 12](#_Toc72941491)

[对密文进行统计分析 13](#_Toc72941492)

# 摘要

随着密码破译技术和电子计算机的发展，DES安全性上的不足越发明显。新的分组加密算法AES出现并取而代之，成为了被美国国家标准技术协会（NIST）选中的全新密码方案，在安全性、算法复杂度等方面表现良好，被广泛应用于金融、电信、政府数据等领域的数据加密中。本次研究使用c语言实现了整个密码方案，代码主要由子密钥生成、加密、解密工具等部分组成，并对一整本《圣经》进行了加密，对加密后的结果做了统计分析。

# 关键词

AES 有限域上的分组密码 轮函数 频率统计 子密钥生成 信息安全

# Abstract

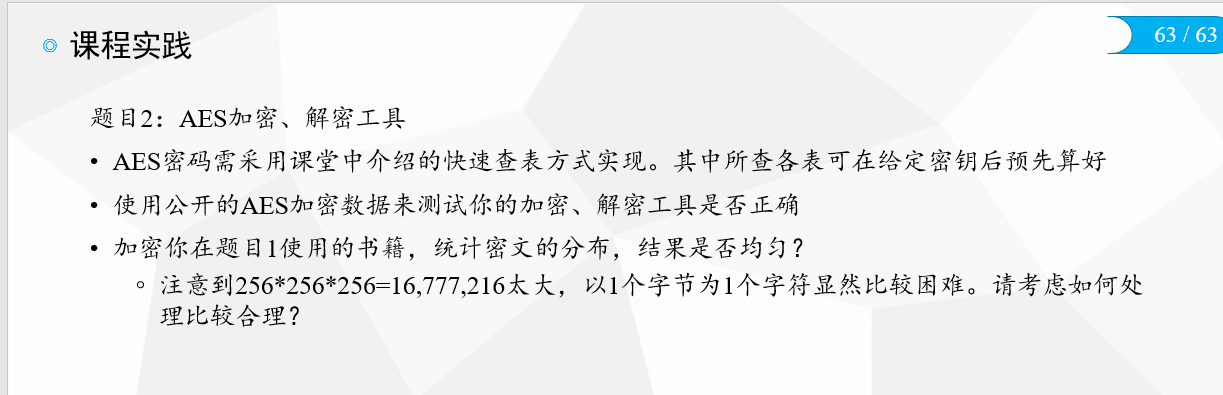
With the development of password breaking technology and electronic computers, the security deficiencies of DES have become more and more obvious. The new block encryption algorithm AES appeared and replaced it. It has become a new encryption scheme selected by the National Institute of Standards and Technology (NIST). It performs well in terms of security and algorithm complexity, and is widely used in finance, telecommunications, government data, etc. This study uses the C language to implement the entire cryptographic scheme. The code is mainly composed of sub-key generation, encryption, and decryption tools. The entire "Bible" is encrypted, and the encrypted results are statistically analyzed.

# Keywords

AES block cipher on finite field round function frequency statistics subkey generation information security

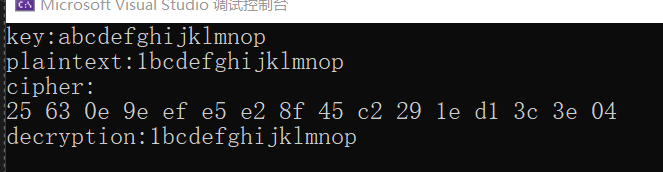
# 正文：

## 题目要求



## 效果

本代码实现了AES算法经行加密、解密，先上效果图：



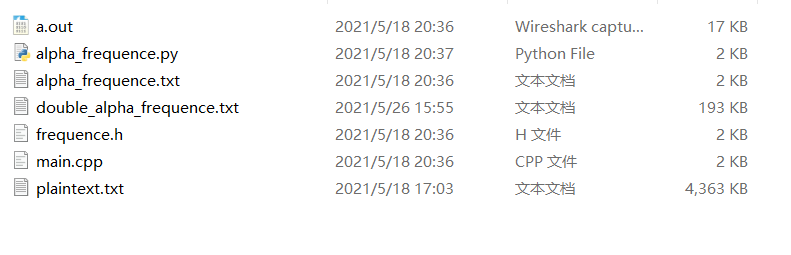
经过公开的AES加密工具可以验证，我写的AES算法是没有问题的。

## 代码文件简述

本程序前一部分“AES加密、解密工具”源代码存放在“AES加密、解密工具”文件夹里面，由以下几个文件组成，decrypt.h实现了AES算法的加密功能，encrypt.h实现了AES中的解密部分，init\_key.h实现了密钥矩阵的初始化，key.txt保存了密钥，main.cpp为程序的主部分，table.h存放了AES算法所使用到的一些常数矩阵。还有plaintext.txt存放第二部分要加密的文件《圣经》，cipher.txt存放加密后的结果。由于我实在linux上完成这个实验的，所以有一个linux makefile，AES也是main.cpp经编译后的elf文件

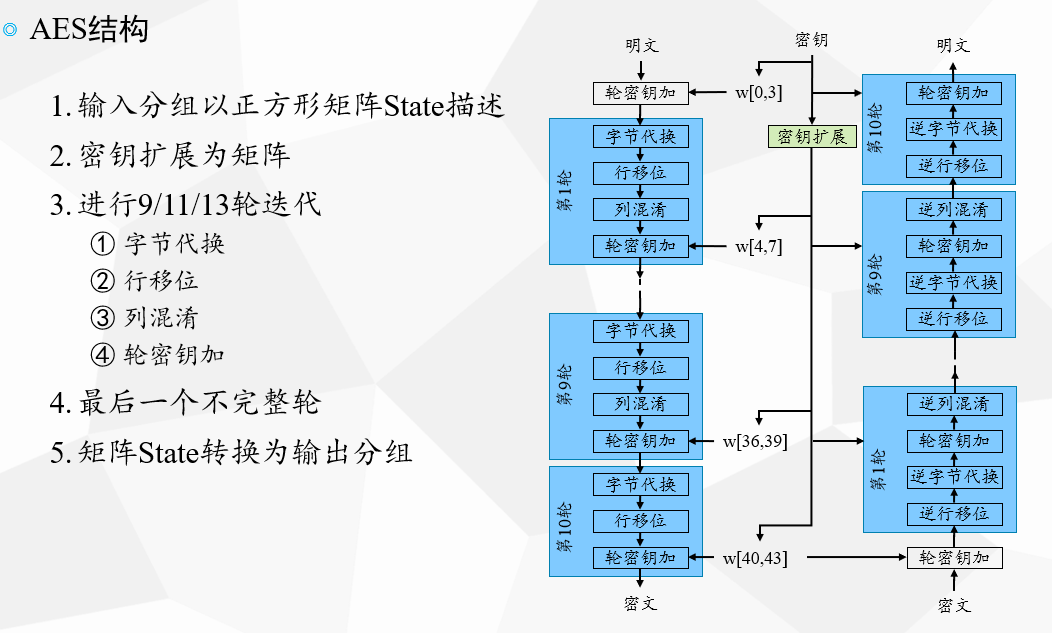
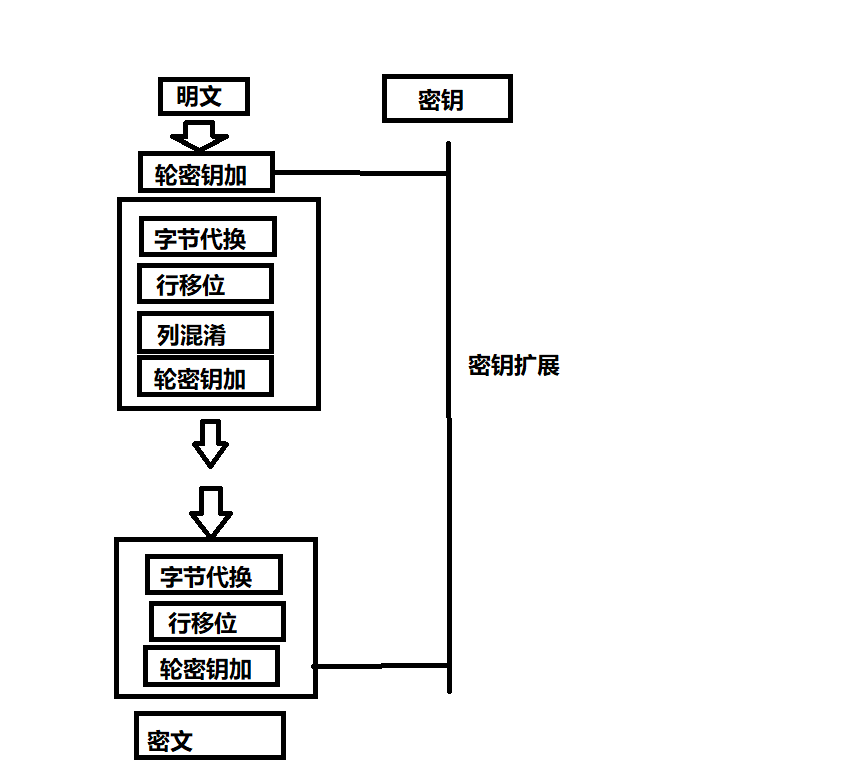


至于实验后一部分的内容“统计密文比特频率”所使用到的代码，放在了“统计频数”文件夹中，这一部分文件是由实验1中的文件经过一定的改写而来的，主要是统计的分类由26个字母改为256个比特串，alpha\_frequence.py则用于图像的可视化处理。



## AES算法流程

AES算法为有限域上的分组密码，一次加密将一个长度为128b (16B, 4W)的明文和长度为128b (16B, 4W)或192b (24B, 6W)或256b (32B, 8W)的密钥可逆映射到128b (16B, 4W)的密文空间上。AES加密流程图如图所示：

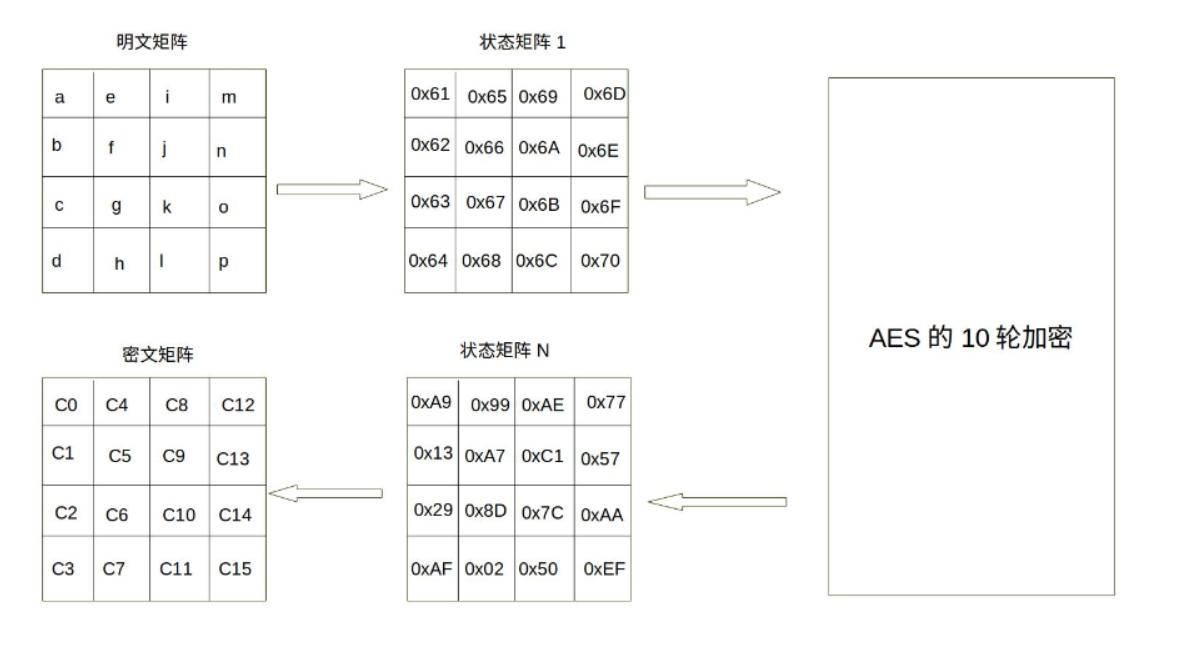


（图片来源：Crypt04-有限域上的分组密码.pptx 李卫海老师）

AES结构分为输入描述、子密钥生成、轮函数等部分组成，接下来对这些部分一一介绍：

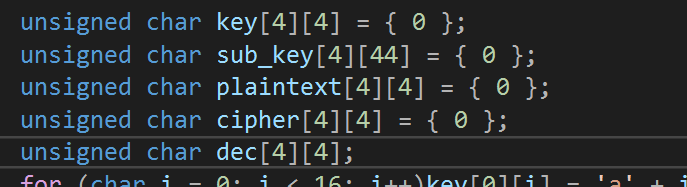
### AES输入分组

AES算法将输入用一个正方形矩阵来描述，如图所示：



（图片来源：https://blog.csdn.net/qq\_28205153/article/details/55798628）

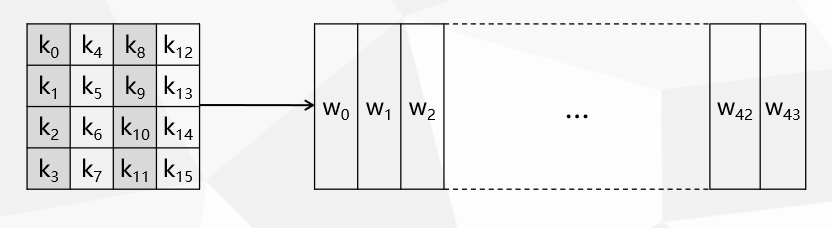
对应到程序，程序里的明文分组、密钥分组、密文分组均以4\*4矩阵表示，以一个字节为单位，如图：



### AES算法子密钥生成

这一部分的代码实现放在了init\_key.h头文件里。

AES通过密钥扩展算法，将一个16字节的原密钥扩展为44\*4字节的密钥序列数组，每次轮密钥加运算使用4个字节，一共要加11轮



（图片来源：Crypt04-有限域上的分组密码.pptx 李卫海老师）

密钥扩展时，首先将4字的原始密钥放在前四字的密钥矩阵里，接着使用如下的递归方式扩展40个新列：

如果4不整除i：W[i]=W[i-4]⨁W[i-1]

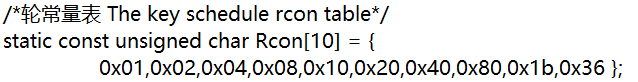
如果4整除i：W[i]=W[i-4]⨁g(W[i-1])

其中，g是一个复杂函数。

g分三步：1.字循环：四个字节循环左移一个字节

2.字节代换：用S盒对每个字节进行代换

3.与轮常量Rcon[j]异或

轮常量可以通过查表得到，已经存放在table.h文件中：

### AES的轮函数

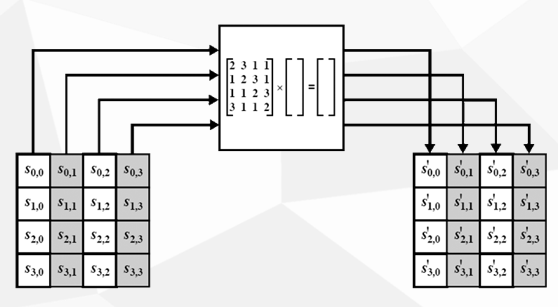
（本部分具代码在encrypt.h头文件中得到了实现）

AES算法共有10轮加密，首先对明文用w[0,3]经行轮密钥加，再经过9轮的字节代换、行移位、列混淆和轮密钥加，最后第10轮只需要经行字节代换、行移位和轮密钥加。

字节代换：字节代换是简单的查表操作，利用一个16\*16大小的sbox进行单字节代换，使用字节的高4位作为行值，低4位作为列值，取S盒中对应行列的元素输出，可以通过table.h头文件里的sbox数组来实现。

行移位：对状态矩阵进行操作，第一行不变，第二行循环左移一个字节，第三行循环左移两个字节，第四行循环左移三个字节。

列混淆：列混淆使用了GF(2^8)上运算，对每列独立进行操作，使用一个列混淆矩阵与每一列相乘。这一部分实际上也可以用查表的方法来替代，会更加简单高效，但是我还是直接使用函数来求解了。



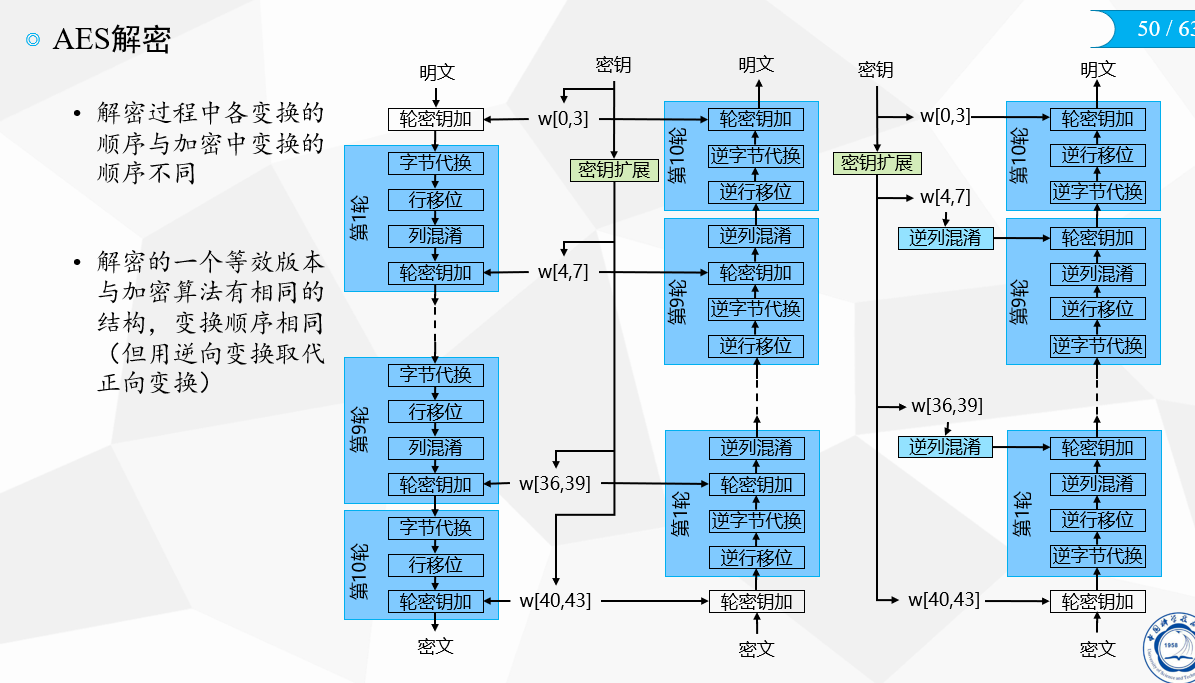
（图片来源：Crypt04-有限域上的分组密码.pptx 李卫海老师）

轮密钥加：直接将状态矩阵与对应的轮密钥相加，这里是在GF(2^8)中的加法。

### AES解密

（解密在decrypt.h中实现）

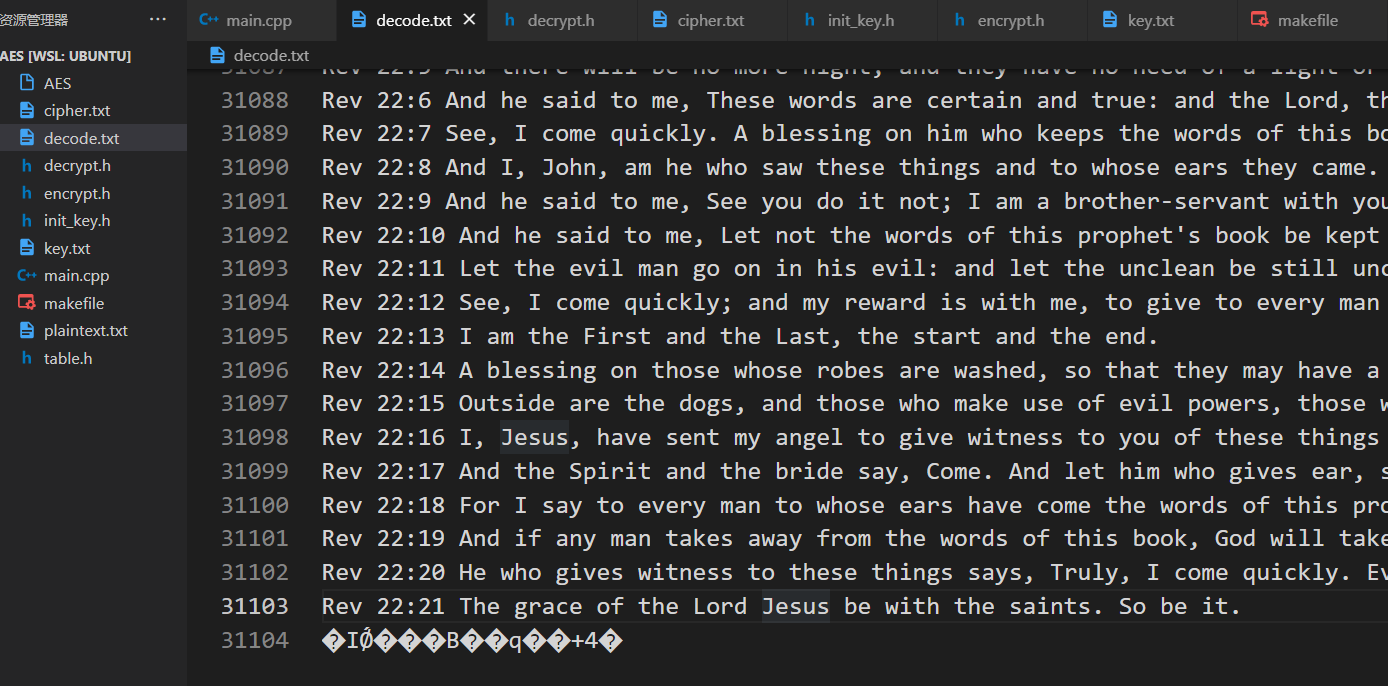
AES解密与加密算法有很多相同的部分，但是仅仅将变换改成加密的逆变换是不够的。AES解密过程中解密过程中各变换的顺序与加密中变换的顺序不同。具体流程图如下：



（图片来源：Crypt04-有限域上的分组密码.pptx 李卫海老师）

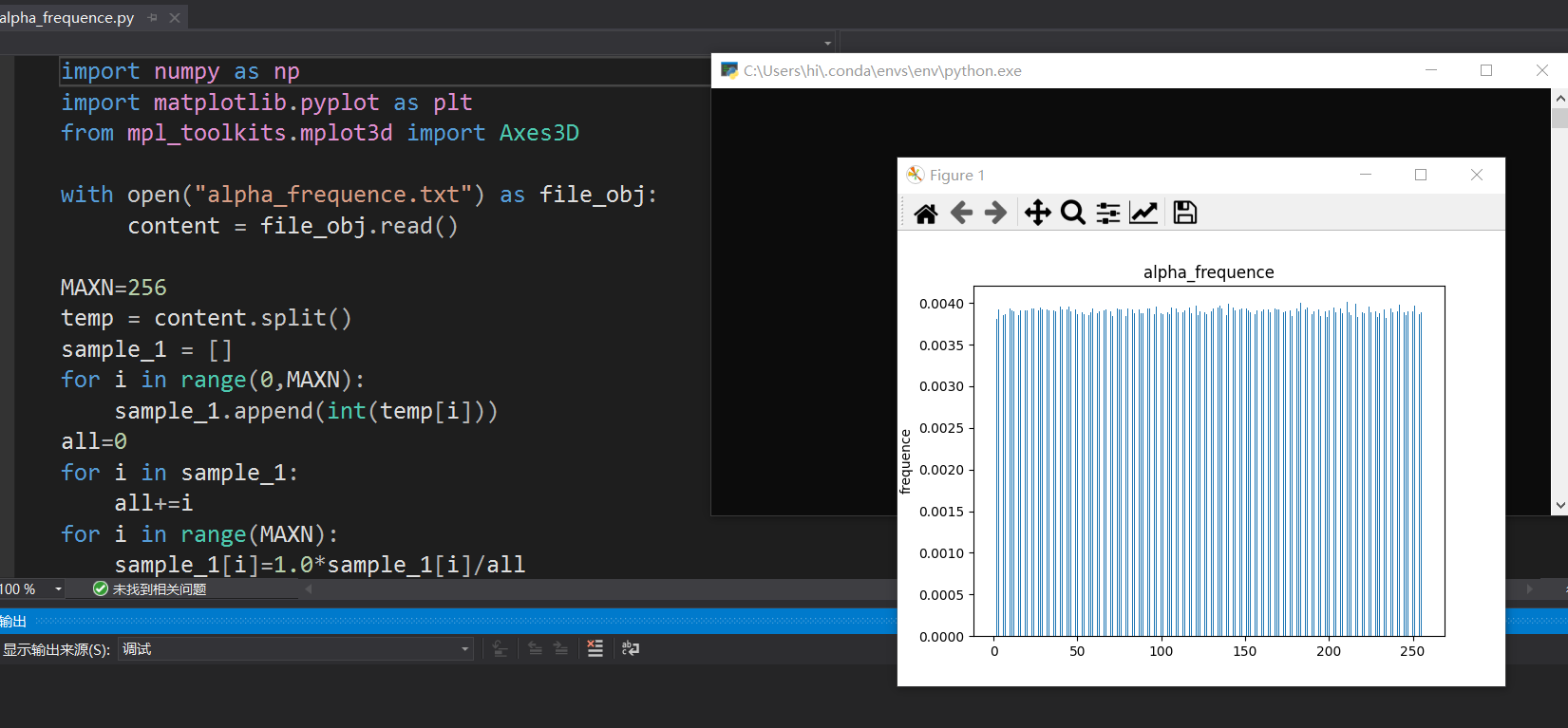
## 加密《圣经》

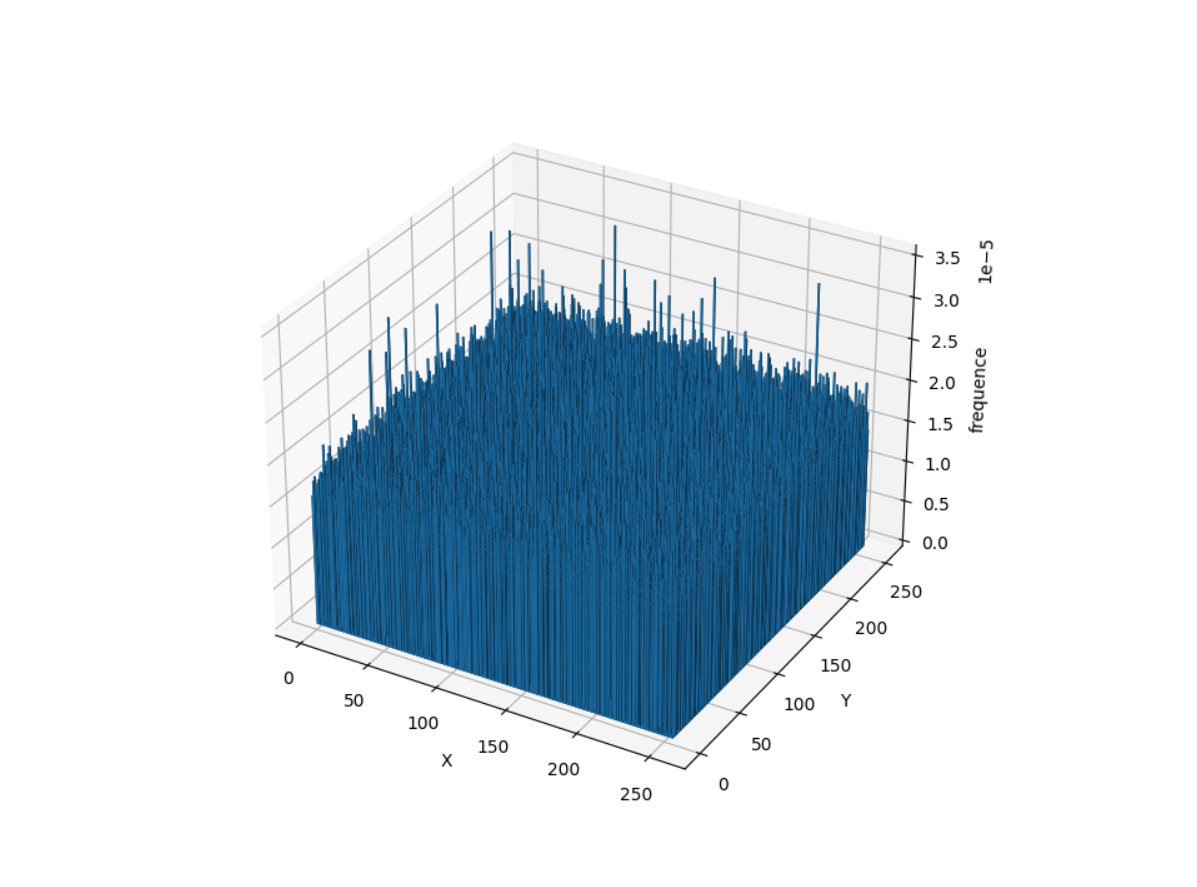
对整个文件经行加密并解密。将加密后的结果保存在cipher.txt文件里，将解密后的结果保存在decode.txt里。可以看出，decode.txt与plaintext.txt基本上完全一致，只有在decode.txt的最后出现了一些乱码，这是由于解密是以4\*4bytes的分组进行的，解密后的文件长度也必须是16的整数倍。不过这一点乱码并不影响接下来的统计分析，所以我就不对其进行处理了。



## 对密文进行统计分析

对于单字节和双字节，可以参考之前的字母统计分析，只需将代码稍微修改一下，将26个英文字母的分类改为256个字节串的分类。统计效果如下：





可以看出，AES算法的算法能够很好的消除分布中的统计特征，单字符、双字符出现次数的方差较小。