# 密码学des实验报告

### 第 2 次作业

### 内容  
1. 网上搜索DES的源代码。  
2. 利用DES源代码实现下面功能：  
1. 给定某个Sbox的输入差分情况下，计算所有输入对和所有Sbox输出差分的分布情况  
2. 统计DES算法在密钥固定情况，输入明文改变1位、2位，。。。64位时。输出密文位数改变情况。  
3. 统计DES算法在明文固定情况，密文改变1位、2位，。。。64位时。输出密文位数改变情况。  
  
为了具有客观性，2，3小题需要对多次进行统计，并计算其平均值。  
  
### 上交内容要求  
选用自己熟悉的语言实现上述要求。上交内容包括程序源代码和一份简单的实验报告（电子版本）  
  
### 参考内容  
可以参考`（校园网） [http://10.21.49.130/](http://10.21.49.130/" \t "http://web.qun.qq.com/announce/_blank)` 中的相关内容。

## 实现方法

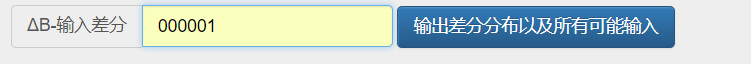
主要是看到第二点中有个多次实验并且统计的问题，所以想到采用数据可视化的方法来呈现统计的结果效果应该非常不错。Python的matplotlib库对数据可视化的支持非常好，所以主要的思路就是采用web做前端，然后python做后台，把matplotlib库产生的东西呈现给前端，des源码采用python的源码，前端采用bootstrap和jQuery框架，后台采用flask做框架

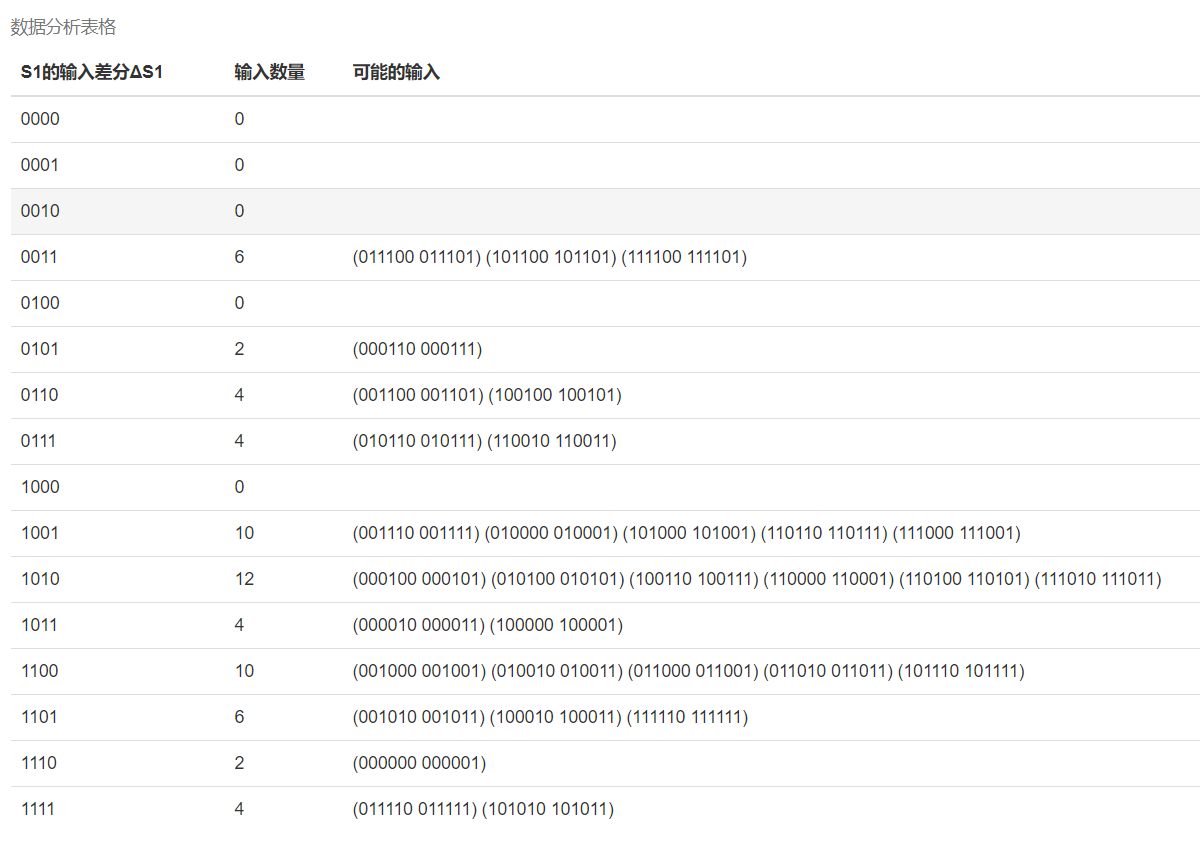
## 给定某个Sbox的输入差分情况下，计算所有输入对和所有Sbox输出差分的分布情况

前端是一个很普通的html布局



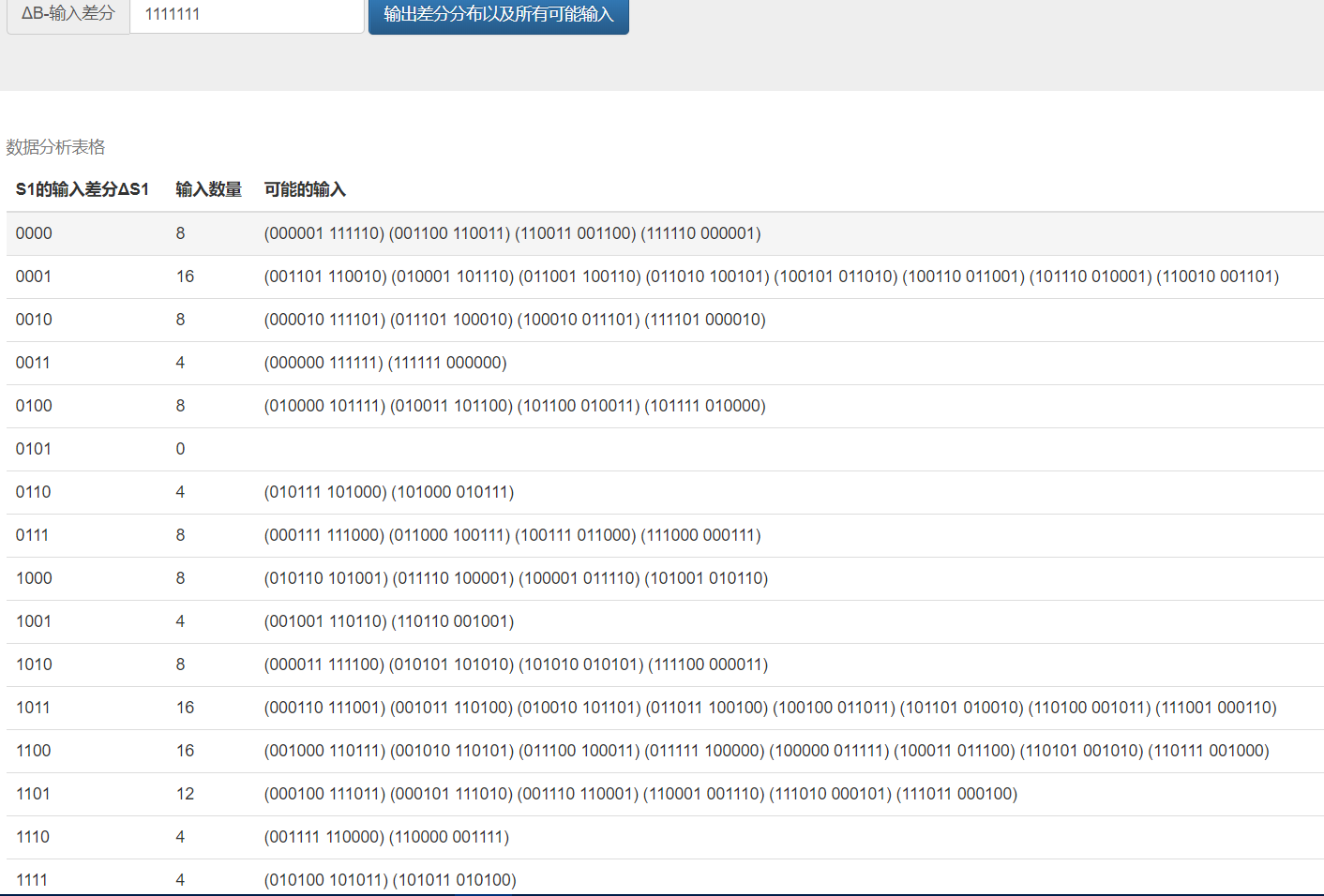
输入000001

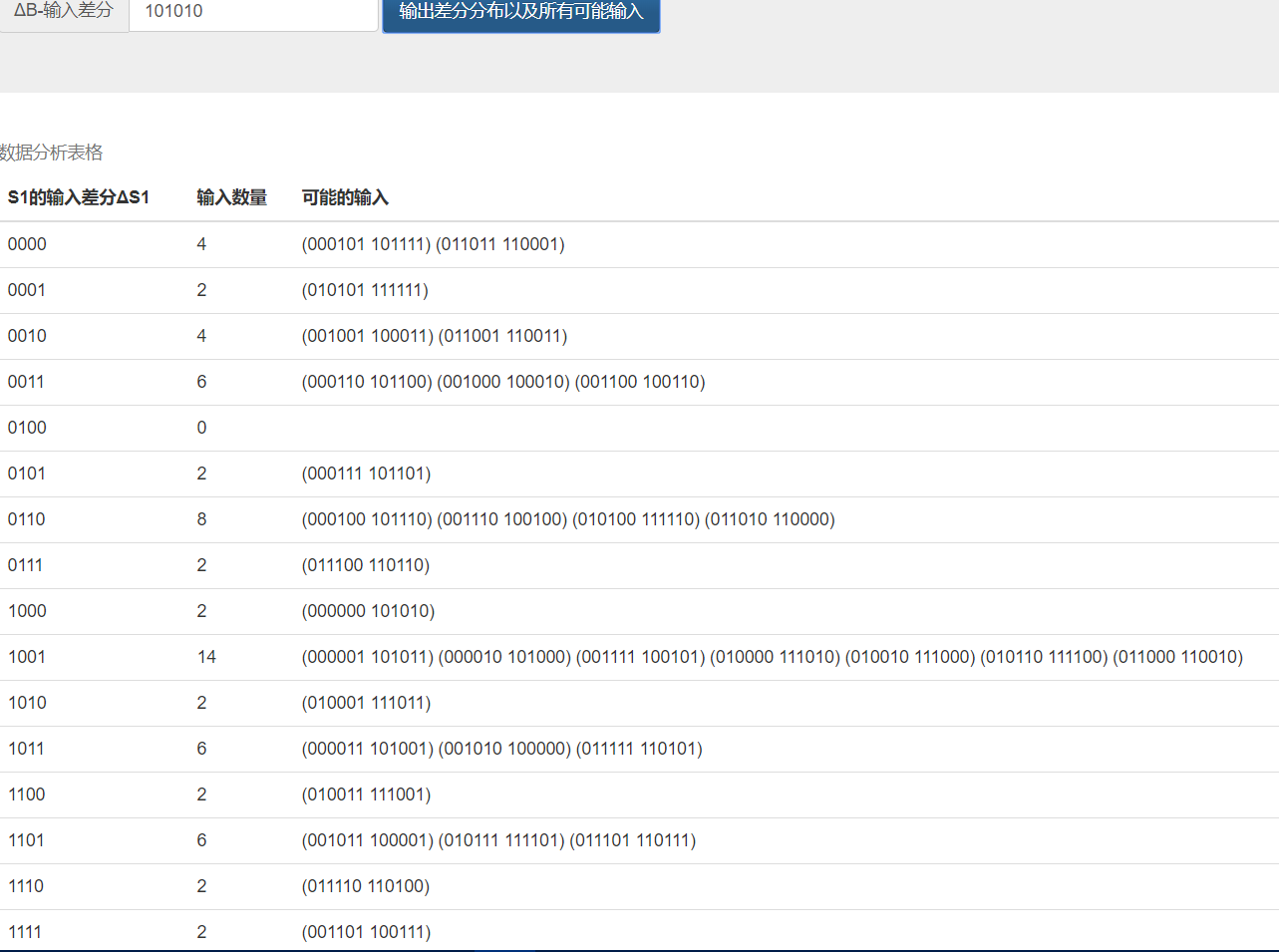


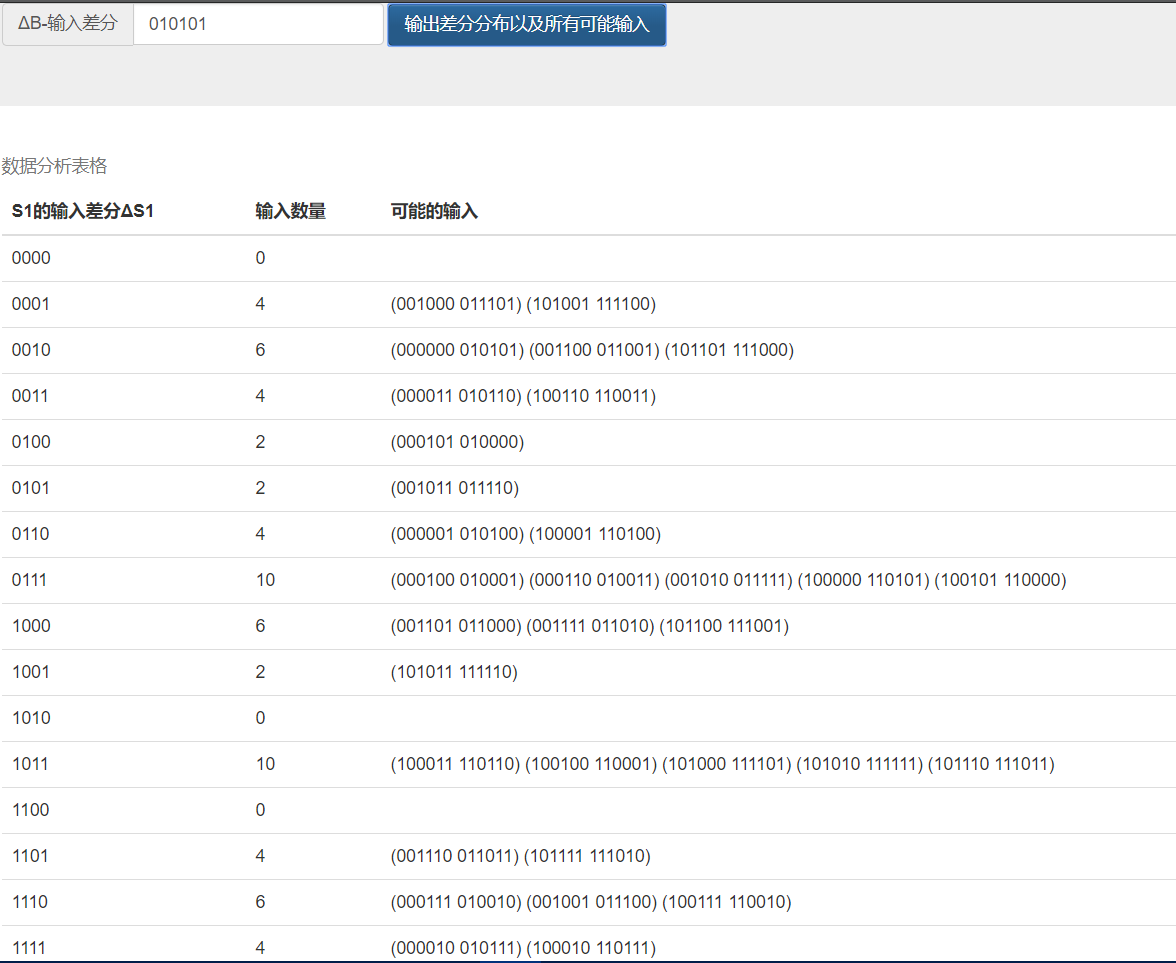


可以看到已经实现了书本上的样例

### 一些其他的样例







可以看到，差分分析对于DES的S盒分析非常有效果，数据分布出现了不均匀的现象。

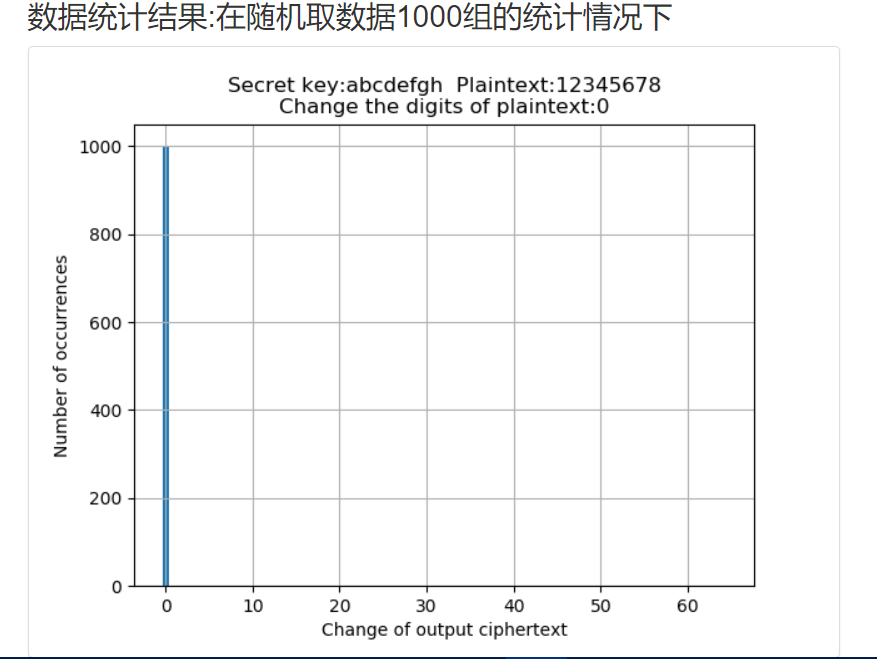
## 2. 统计DES算法在密钥固定情况，输入明文改变1位、2位，。。。64位时。输出密文位数改变情况。

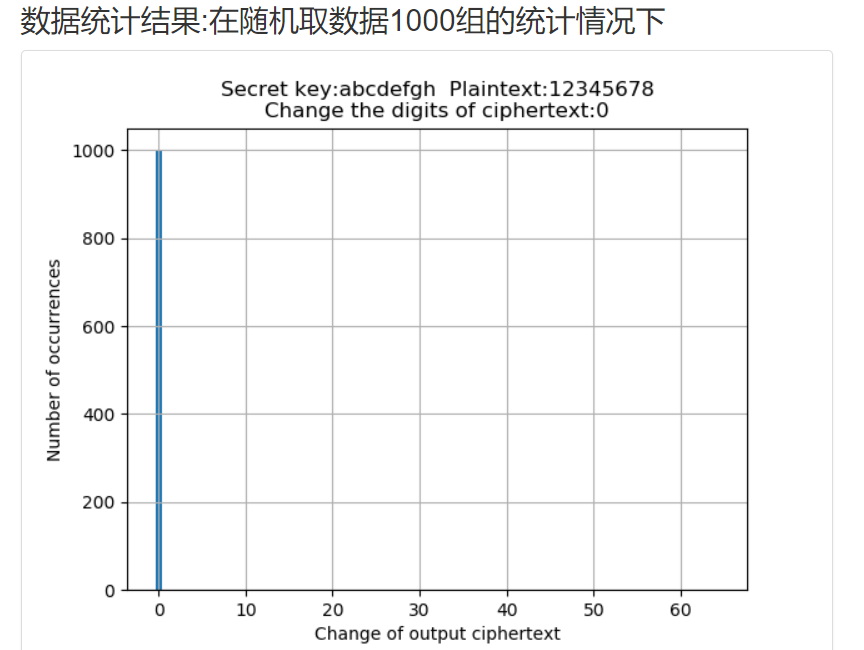
## 3. 统计DES算法在明文固定情况，密文改变1位、2位，。。。64位时。输出密文位数改变情况。

这两个任务可以同时做，后台的主要实现是，前端输入，明文跟密钥，然后选择改变位数A，以及任务类型。选了改变位数之后，后台随机测试1000组样例，产生一千串和原始串A位不同的目标串，运行16轮DES源码加密，统计输出结果中有多少位是和原始串的输出结果不一样的。然后用matplotlib库绘制好图片返回给前端

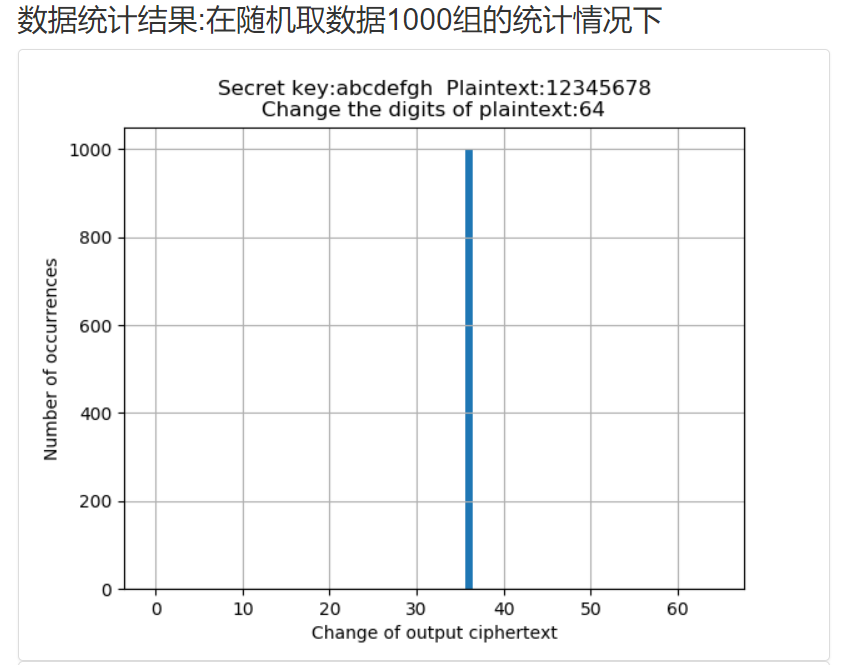


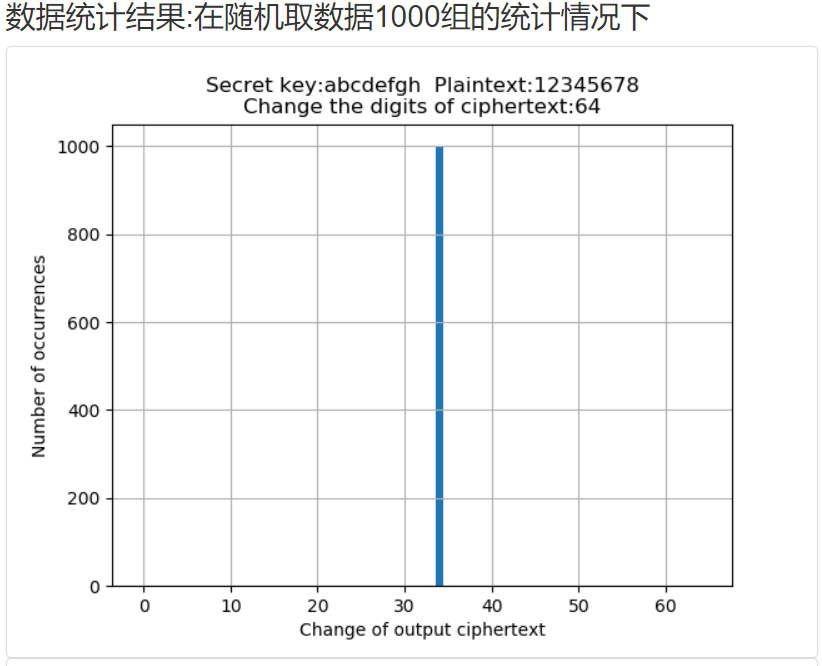
### 实验结果





首先是change of digits等于0的情况下任务2和任务3的输出，可以看到，1000组样例什么也没发生改变。达到了预期的效果。

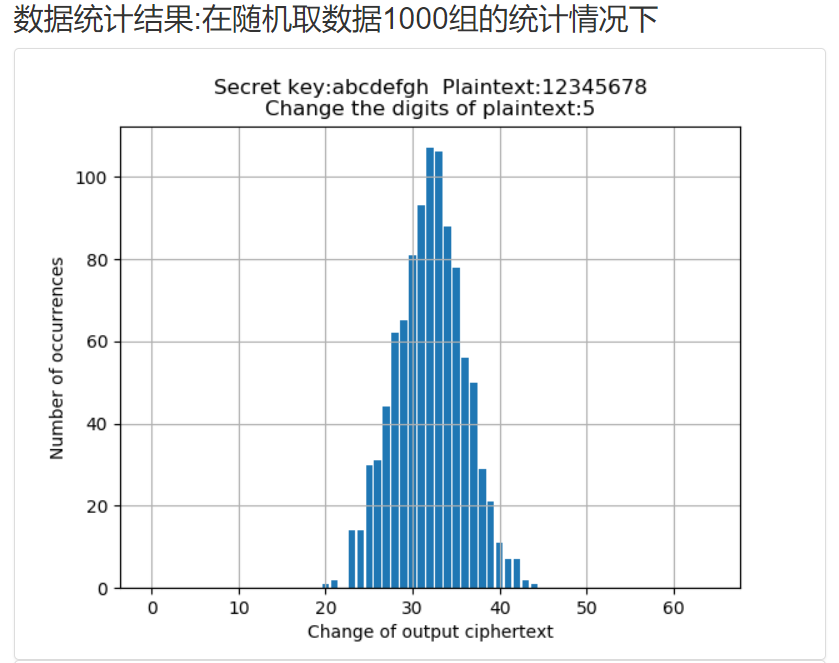


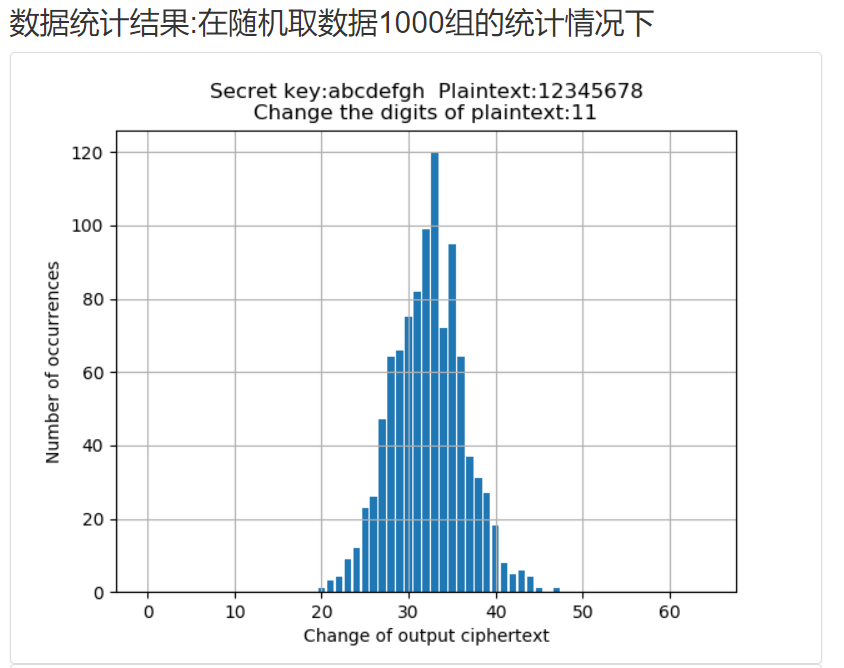


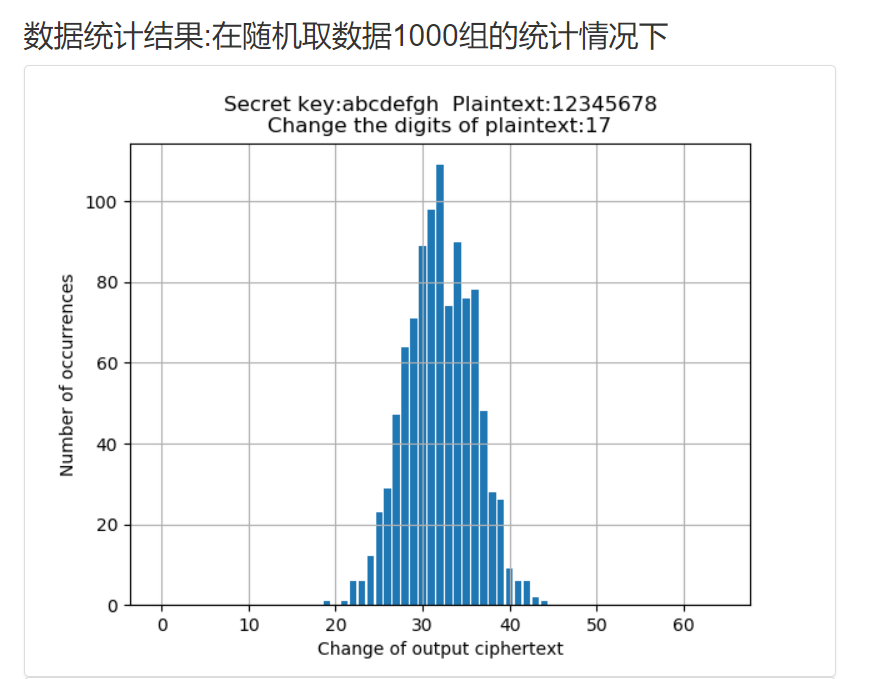
相反的，在极限数据改变64位的时候，1000组测试数据都集中在中间，其实1000组测试数据是一样的，因为都全部反转了。实验正确

### 任务2和任务3各三组其他测试数据

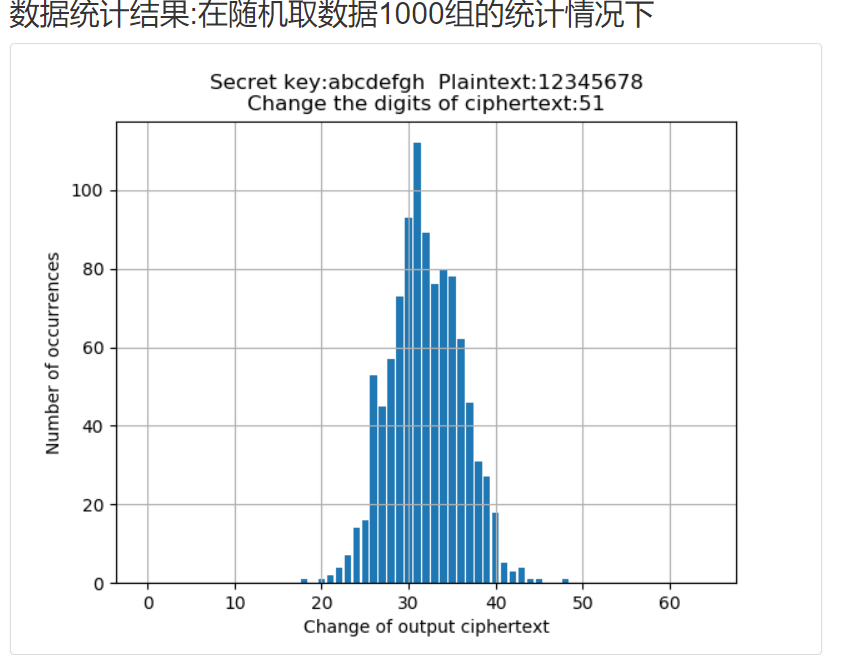
任务2

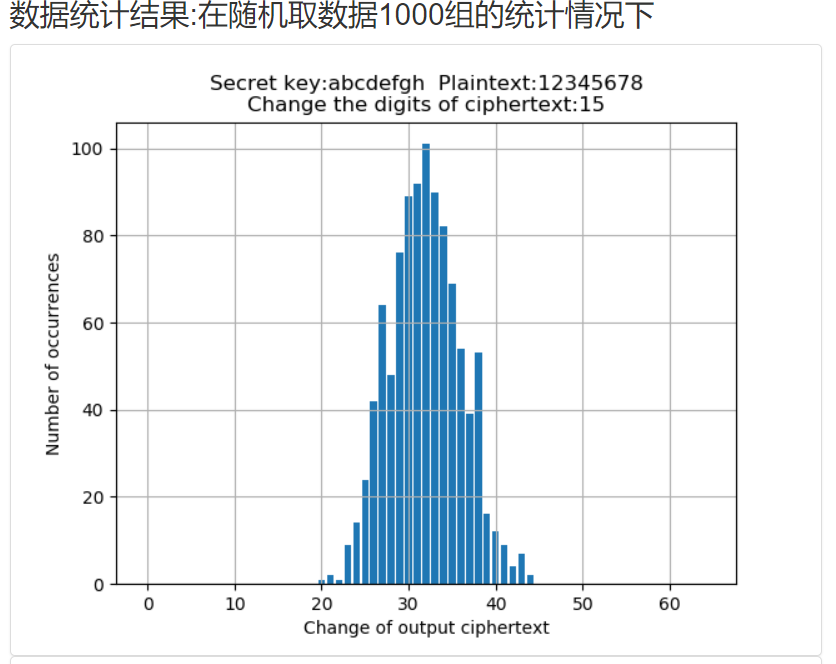


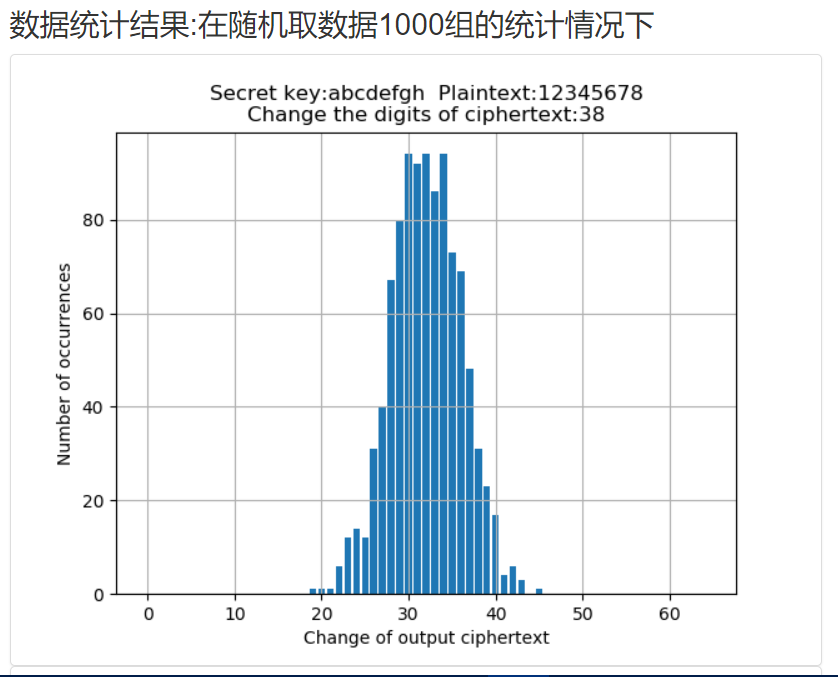




任务3

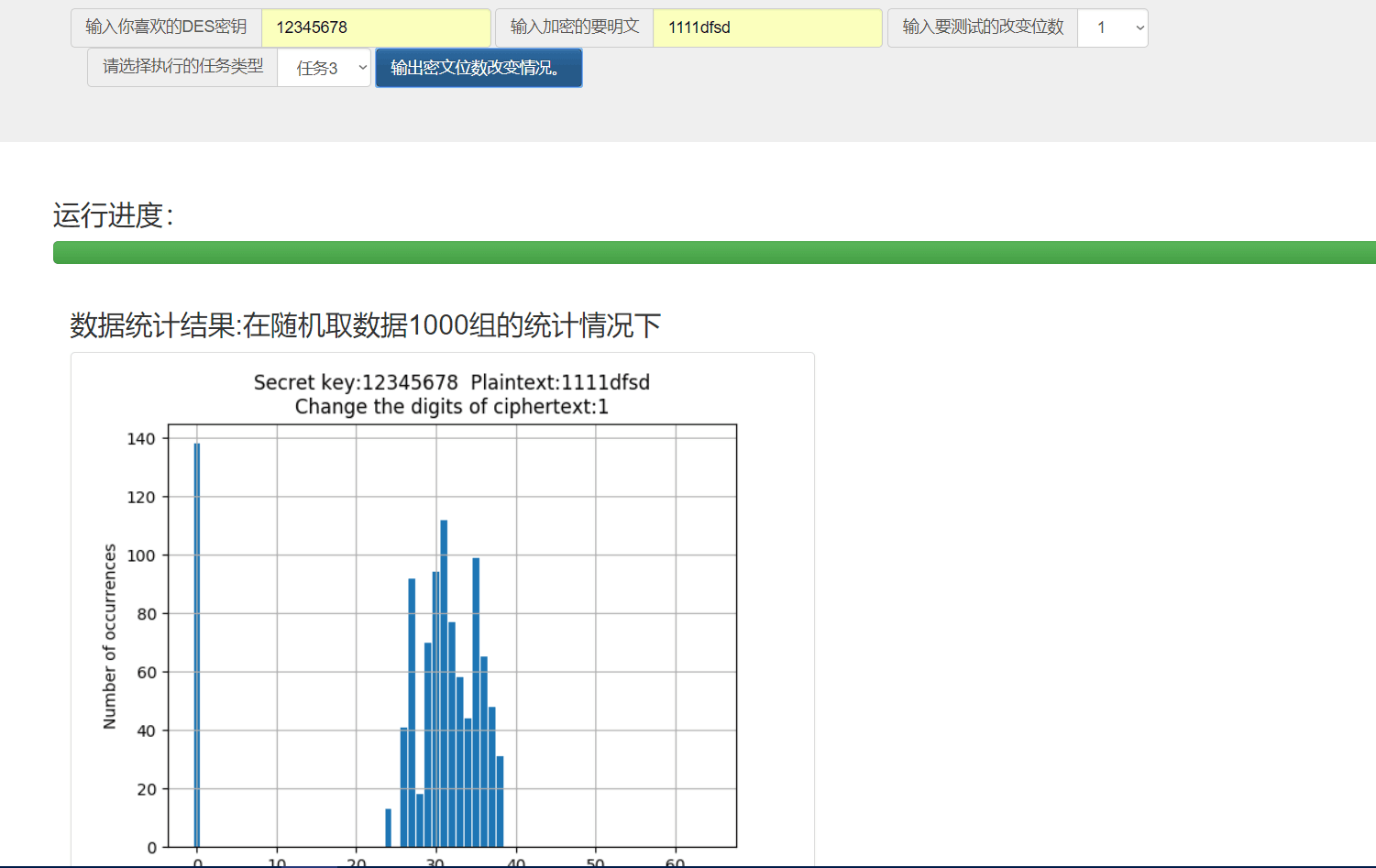




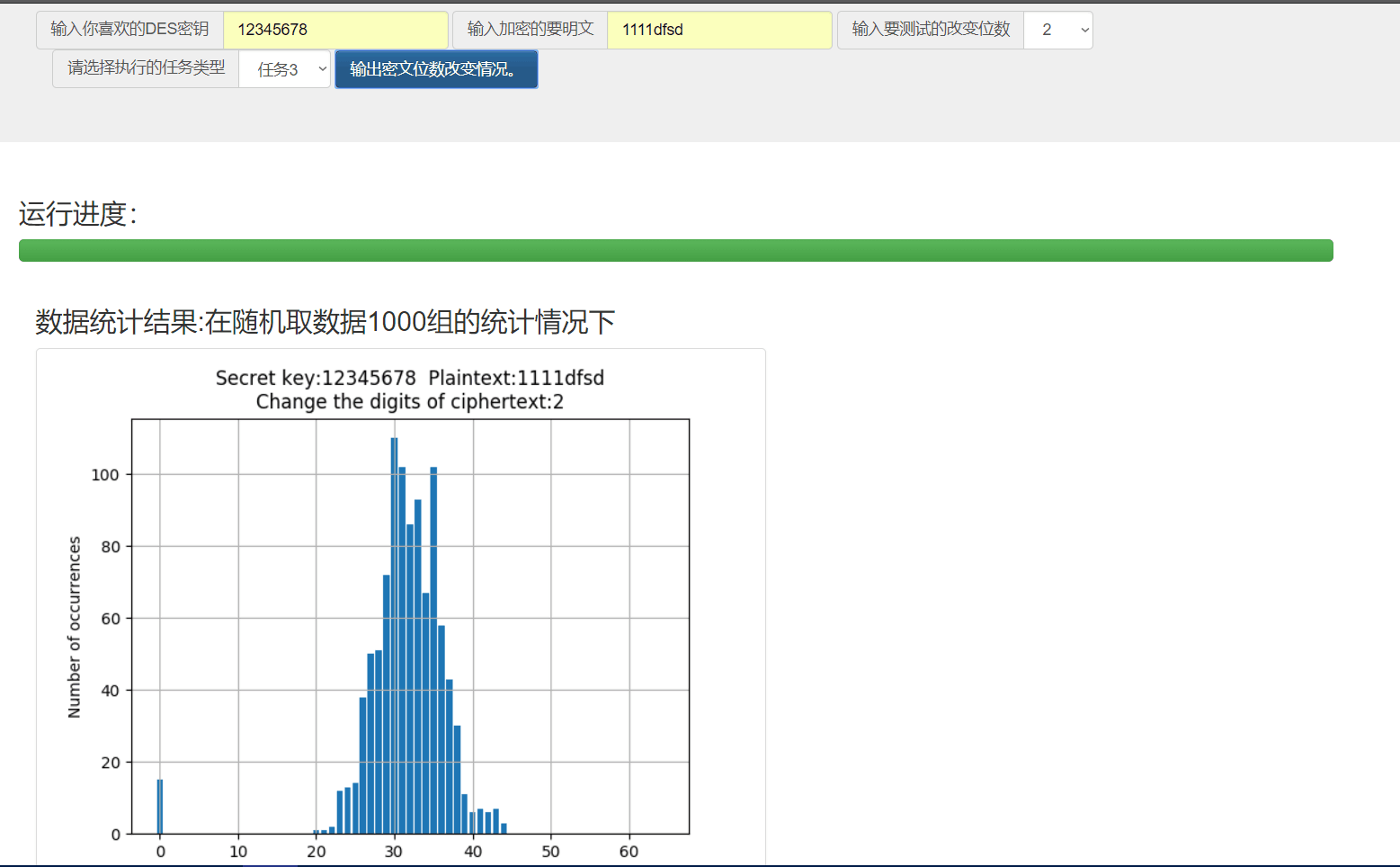


改变的位数普遍集中在中间，不多也不少，正是应正了书上所说的，0和1的数目在加密16轮之后是大致相同的，DES起到了很好的混淆作用，所以结果异或起来是有一半的不同的，普通的明文攻击很难发现其中潜在的规律。

# 额外的补充



由于密钥中64位中，只有56位是有用的，每个字节的第八位是奇偶校验位是不会用在加密上的，所以，密文只改变一位的时候，是有一定的概率修改到奇偶校验位导致结果不变



改变位数越多，同时改变到奇偶校验位的情况就变少了。