实验报告1

陈旻 SA18225036

1 具体思路

根据提示，空格space的ASCII码二进制形式为0010 0000。大写字母A～Z的ASCII码二进制形式为0100 0001～01011010，小写字母a～z的ASCII码二进制形式为 0110 0001～01111010。因此若用space和字母做xor操作，则相当于字母切换大小写，而两个字母做xor操作，结果将不在字母范围内。另外由于xor操作的特点，将两个密文做xor操作相当于将两个密文对应的明文做xor操作，如果结果中某个位置出现字母，则说明这两个明文的其中一个在该位置可能为空格，所以基本思路是对11个密文分别做两两xor操作，然后通过结果判断不同明文中可能存在空格的位置，然后将对应位置上的密文和space做xor操作，就可得到对应位置的密钥信息，当获取足够多的密钥信息后，就可以对最后一个目标密文进行解密了。

需要注意的是两个密文xor的结果中出现的字母不一定是space字符和字母xor的结果，从字母的ASCII码可知，小写字母的前四bit是0110，大写字母的前四bit是0100，所以如果某个字符的ASCII码前四bit是0010或0011这样的形式，那么它和字母xor的结果也可能是另外一个字母，而文本中经常出现的“?”，“!”和“:”等字符就符合这样的特征。另外如果两个文本正好在同一个位置上有空格，则xor操作后该位置得到的字符将是“NULL”。所以对于特定密文，要判断其对应明文可能存在空格的位置的话，我的想法是将该密文和其他10个密文分别做xor操作，每一次操作后记录结果中出现字母的位置，得到一个集合，最终一共得到10个集合，某一个位置在这10个集合中出现的次数越多，越说明该密文对应的明文在该位置可能是空格，因此空格位置的判定条件就是该位置在10个集合中出现的次数。