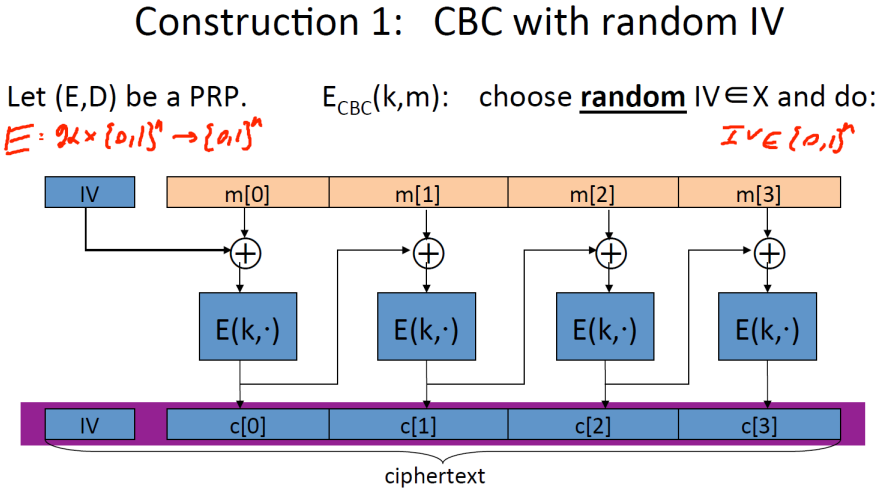
实验报告3

陈旻 SA18225036

1 具体思路

加密库里本身提供了CBC和CTR两种mode，但因为题目要求，所以使用最基本的ECB模式。实现只需要按照公开课ppt上的图来做就行，需要注意的就是对字符串的分块处理，不要把位置弄混了。



另外就是CTR模式下需要每次对IV做加1操作后加密，因为内置的AES加密函数接收的参数是字符串，所以先将字符串中要加1的字符转化为10进制，加1后再转化为字符，由于加1后可能发生进位，所以用递归函数实现。