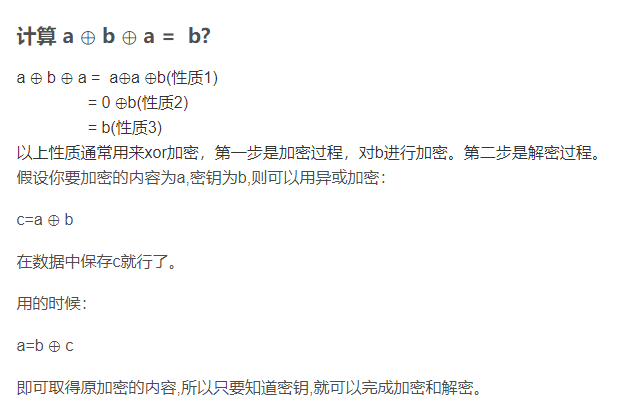
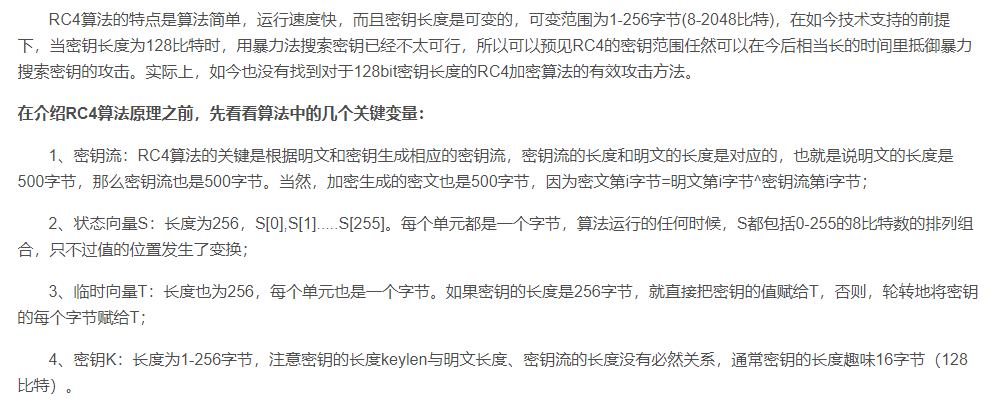
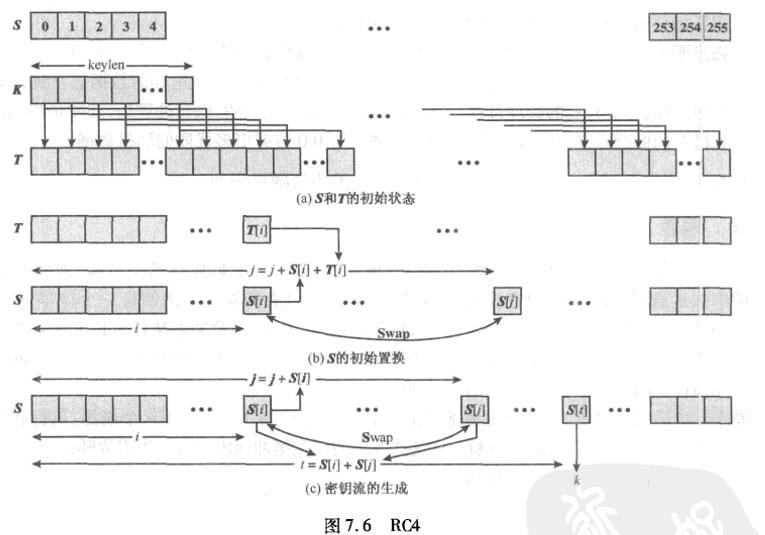
常见特征  
1.ascii偏移 Str[i]+=x这样子  
2.异或：很明显，异或符号 ^  
3.可逆加密   
类似：  
(ord(Destination[i]) & 3)) | ((ord(Destination[i]) & 0xC) >> 2) | ord(Destination[i]) & 0xF0)  
有很多异或且运算，都是再加密一遍就行  
md5:密文是32位的a-f,0-9组成,输入有限制，一般是97-122（小写字母）或者65-90（大写字母）  
sha256:密文是64位a-f,0-9组成，输入有限制，一般是97-122（小写字母）或者65-90（大写字母）  
rc4:密钥是六位，有什么s盒t盒生成啥的  
des:代码复杂，密钥8位，一点进去就一堆函数的  
这两个要注意，出题我觉得很难对中间加什么东西，但是可以对密钥改变一下，比如前年的第四题就是对密钥的ascii都加了个2，然后rc4  
仿射：%26  
base64:应该不会出这么个题，但是不排除密钥或者密文用base64处理过，  
64个字符（英文大小写、数字和+、/）以及用作后缀等号，其实关键就是有=比较明显，但不是所有的都有等号，看着像就试试

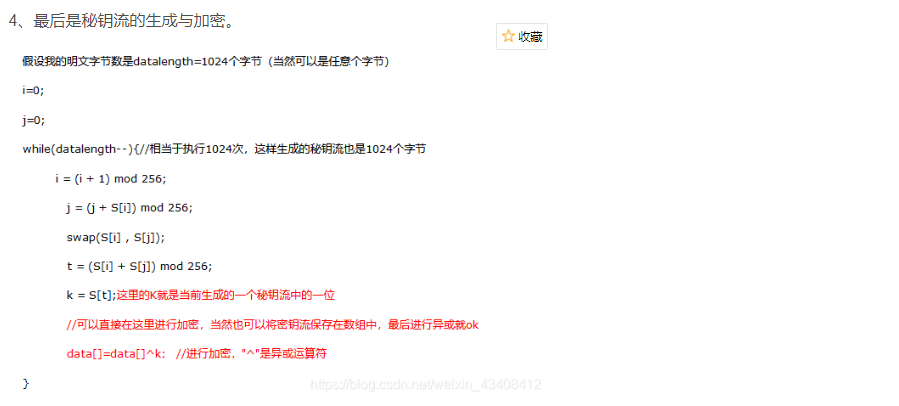
异或密码

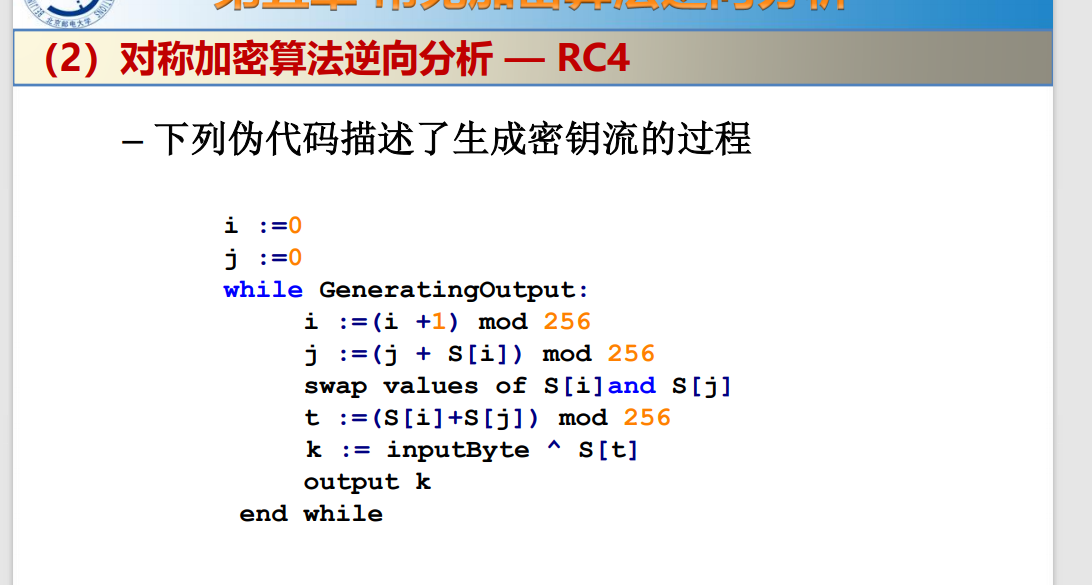


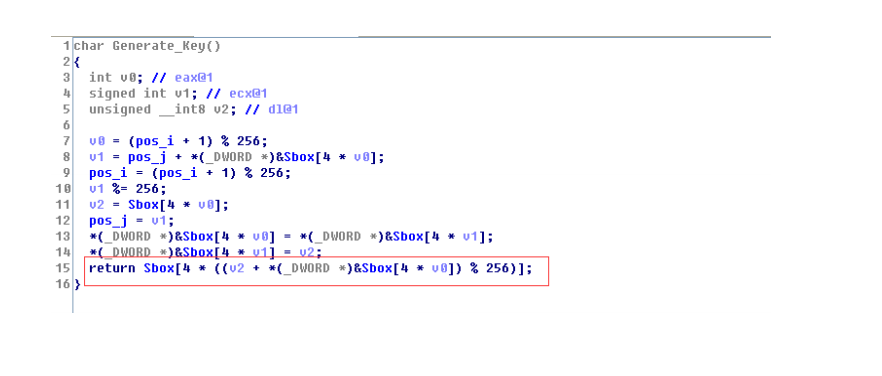
RC4



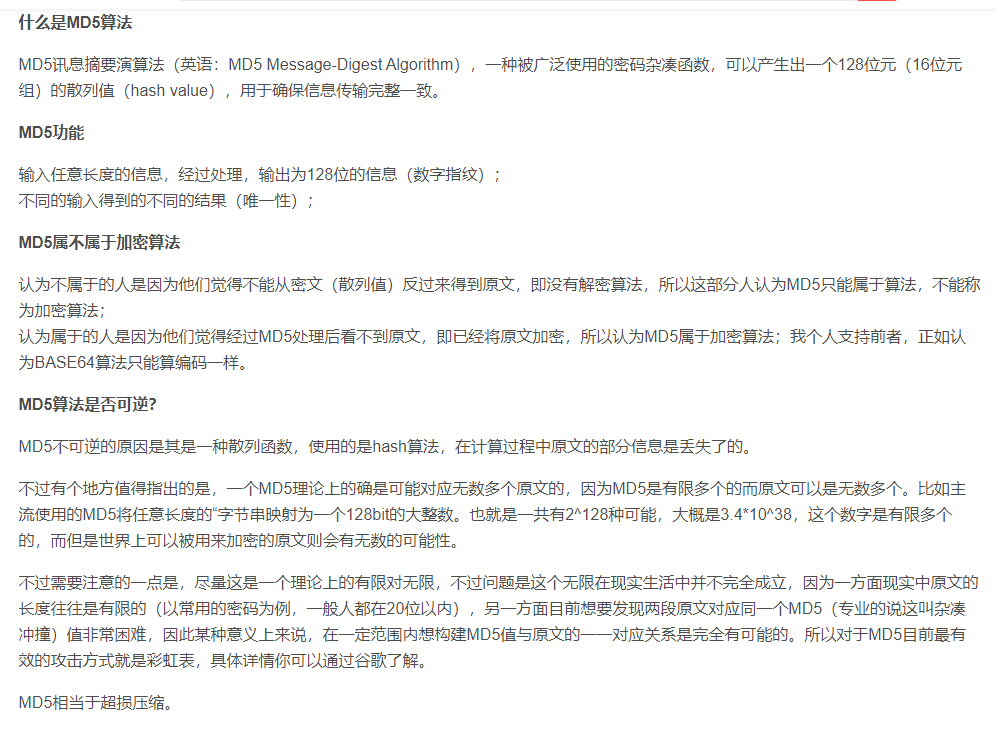


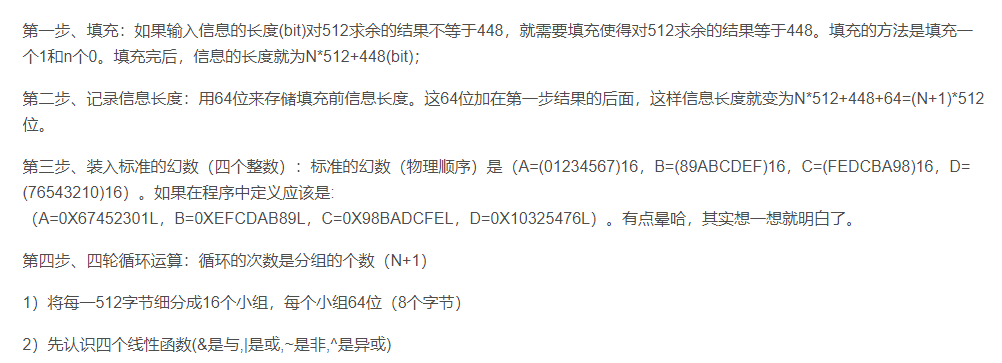






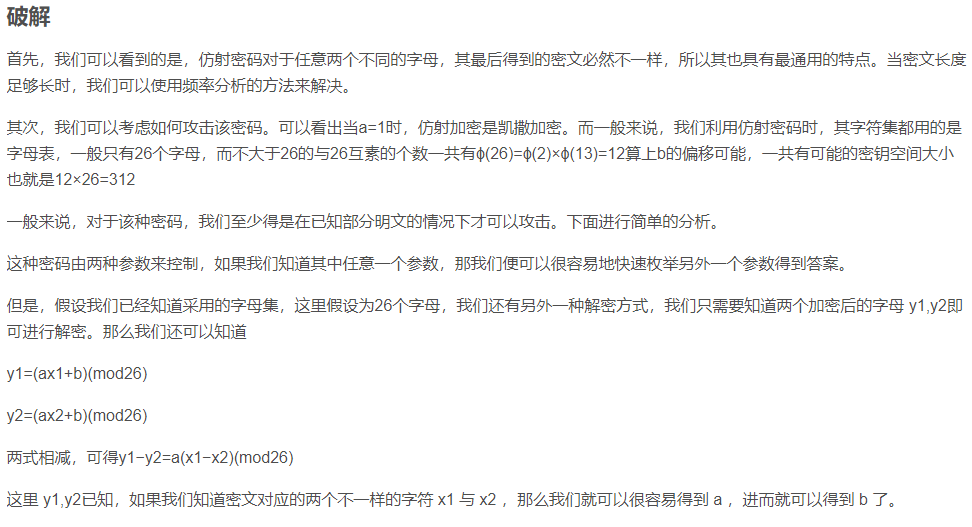
Md5





**仿射密码**





**Sha256**

**DES**