**RC4**

参考文章：<https://blog.csdn.net/iPlayForSG/article/details/123644676>

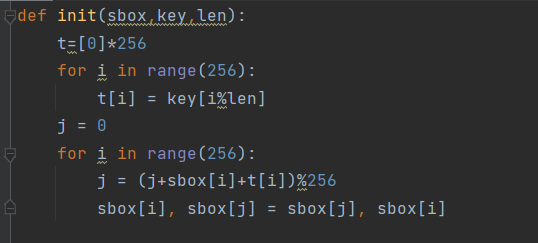
**简介：**

RC4（来自Rivest Cipher 4的缩写）是一种流加密算法，密钥长度可变。它的加解密使用相同的密钥，因此也属于对称加密算法。RC4是有线等效加密（WEP）中采用的加密算法，也曾经是TLS可采用的算法之一。其最重要的实现是初始化算法和伪随机子密码的生成。

RC4的实现是以字节流的方式依次加密明文中的每一个字节，解密的时候也是依次对密文中的每个字节解密。（只有异或操作和S盒，所以加解密的过程相同，这是其可逆性的原理）

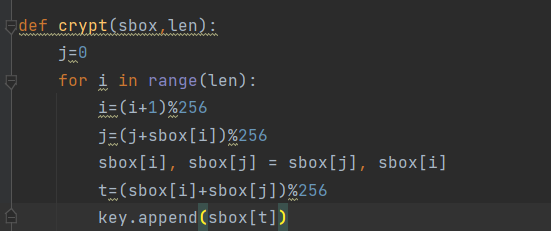
**初始化算法（KSA）**：

先来看看初始化算法，此处我们假设S盒的长度是256，密钥key的长度为len且key的内容由用户规定，其长度的可变范围不限（超过256的不要就行）



初始化算法的步骤为：  
1、初始化S盒为0-255  
2、扩展密钥长度，具体操作是：若key的长度小于256，则不断将其复制进临时数组t，直到t的长度刚好达到256（多的就不要了）  
3、根据t数组打乱S盒，使S盒近似为一个随机生成的、内含元素只有0-255的数组，在该算法中，i确保了S盒的每个元素都被处理过，而j确保了这种打乱的处理是近似于随机的

**伪随机子密码生成算法（PRGA)：**



该算法对data的每一位都进行了加密，具体操作是通过一定的算法找到了S盒中的某一元素，并与data当前字节异或，得到密文。  
值得注意的是，data保存为明文时，加密后得到密文；data保存为密文时，加密后得到明文。

**实现：**

