**题目名称：bbaes**

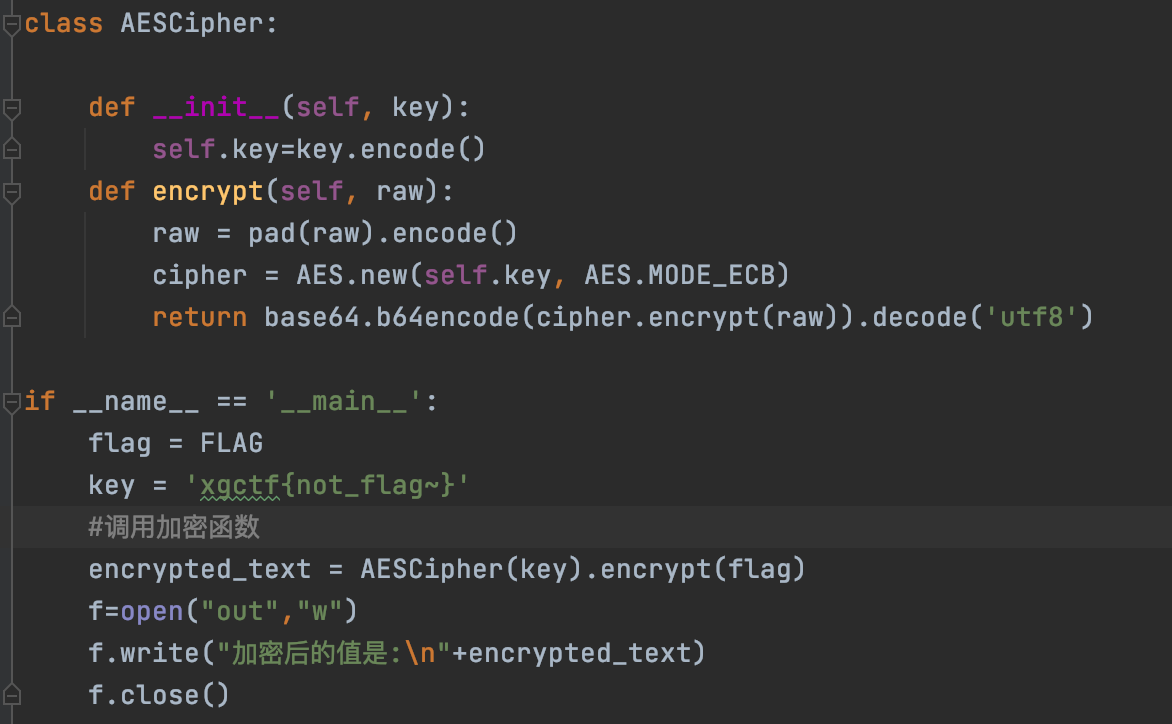
**类型：Crypto**

**介绍：**

本题是Crypto中的对称加密——AES

AES加密介绍：https://wiki.x10sec.org/crypto/blockcipher/aes-zh/

**解题步骤：**

**第一步：**分析题目附件，得到一个加密脚本和一个输出的密文结果。

flag传入AESCipher的encrypt函数中。

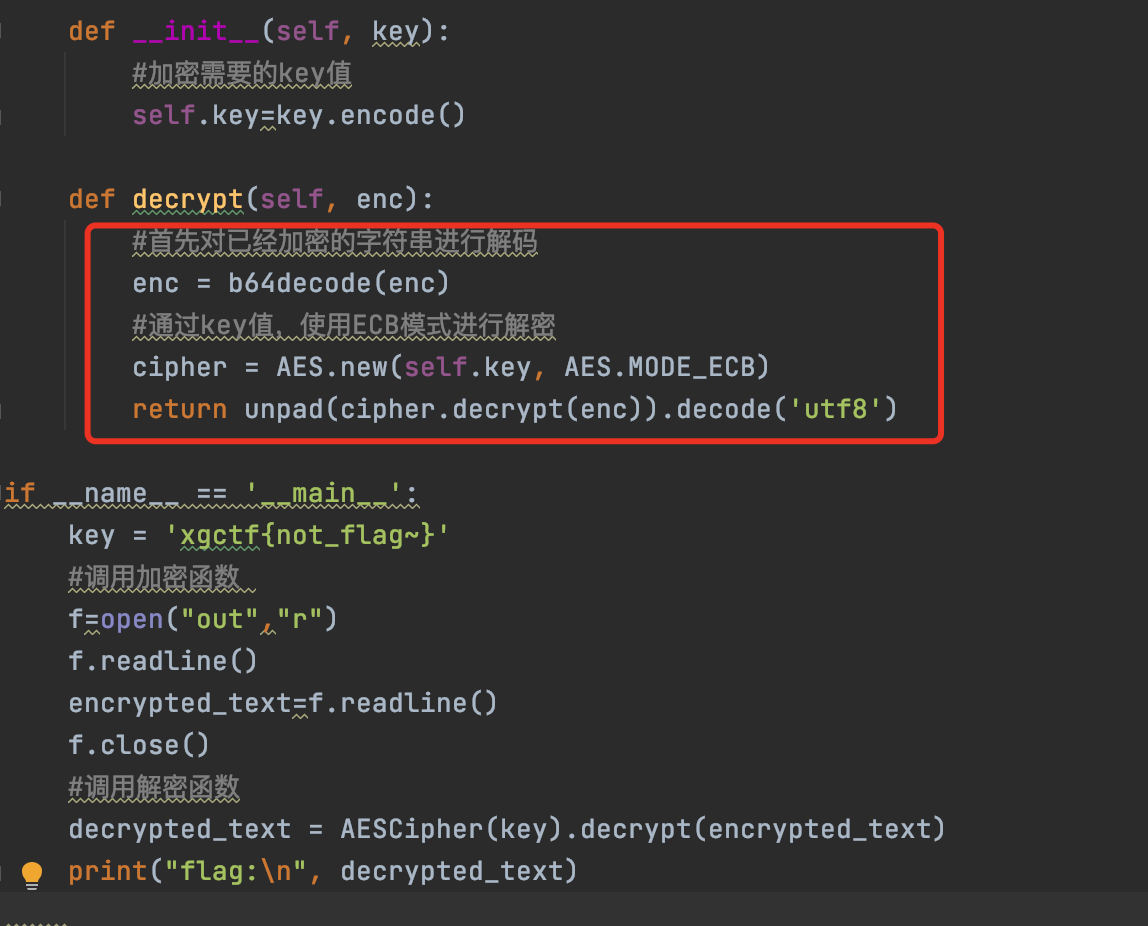
首先pad填充，然后调用python的AES库加密，ECB模式。

加密结果base64编码。写入out文件。

**第二步：**已知加密为AES ECB模式的加密，且在已知密钥的情况下，编写解密脚本即可。

因为pad是将flag明文填充后加密，解密不需要管填充的问题。

解密过程即base64解码后解AES即可。



**简要总结：**考查AES解密的python脚本编写