# Challenge 16

本题要求使用随机密钥进行AES-CBC加密，

内容格式如下：

"comment1=cooking%20MCs;userdata=" + userdata + ";comment2=%20like%20a%20pound%20of%20bacon"

其中userdata为可控制的输入,但不允许存在';'及'='；

目标是为提交的信息添加";admin=true;"标签

server16.jar为模拟的服务端程序，当收到解密后包含admin=true标签则输出admit,并退出；否则输出fail并退出。提交的字符串已默认保存在服务端。

atk16.jar为攻击者程序，当收到服务端返回成功攻击的信息时，输出success并退出。

为了便于观察，server16.jar在加密时将输出密文（以数值形式）和明文（字符串形式），解密时将输出解密后的字符串。

运行时需要先打开服务端，之后开启攻击程序，具体过程可通过服务端输出观察。