

# 对称加密算法 - Java加密与安全 - 飞扬学院

## Java加密与安全

---

### 对称加密算法

使用同一个密钥进行加密和解密

常用算法：DES / AES / IDEA等

密钥长度由算法设计决定，AES的密钥长度是128 / 192 / 256

使用256位加密需要修改JDK的policy文件

使用对称加密算法需要指定：算法名称 / 工作模式(ECB, CBC, PCBC...) / 填充模式(NoPadding, PKCS5Padding, PKCS7Padding...)

### 练习

[下载练习](#) ( 推荐使用Eclipse插件直接导入工程 )

