

RSA签名算法 - Java加密与安全 - 飞扬学院

Java加密与安全

RSA签名算法

数字签名

用发送方的私钥对原始数据进行签名

只有用发送方公钥才能通过签名验证

防止伪造发送方

防止抵赖发送过信息

防止信息在传输过程中被修改

常用算法：MD5withRSA / SHA1withRSA / SHA256withRSA

练习

[下载练习](#)（推荐使用Eclipse插件直接导入工程）

