Java加密和数字签名2私钥加密Java认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_Java_E5_8A_A0_E5_AF_86_c104_644535.htm 私钥加密： 消息摘要只能检查消息的完整性，但是单向的，对明文消息并不能加密，要加密明文的消息的话，就要使用其他的算法，要确保机密性，我们需要使用私钥密码术来交换私有消息。 这种最好理解，使用对称算法。比如：A用一个密钥对一个文件加密，而B读取这个文件的话，则需要和A一样的密钥，双方共享一个私钥（而在web环境下，私钥在传递时容易被侦听）： 使用私钥加密的话，首先需要一个密钥，可用javax.crypto.KeyGenerator产生一个密钥（java.security.Key），然后传递给一个加密工具（javax.crypto.Cipher）， 该工具再使用相应的算法来进行加密，主要对称算法有：DES（实际密钥只用到56 位）， AES（支持三种密钥长度：128、192、256位）， 通常首先128位，其他的还有DESede等，jdk1.5种也提供了对对称算法的支持，以下例子使用AES算法来加密： Java代码 /** *PrivateExmaple.java *Copyright 2005-2-16 */ import javax.crypto.Cipher. import javax.crypto.KeyGenerator. import java.security.Key. /** *私加密，保证消息机密性 */ public class PrivateExample{ public static void main(String[] args) throws Exception{ if(args.length!=1){ System.err.println("Usage:java PrivateExample 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com