Java加密和数字签名3公钥加密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_644534.htm 公钥加密： 上面提到，私钥加密需要一个共享的密钥，那么如何传递密钥呢？web环境下，直接传递的话很容易被侦听到，幸好有了公钥加密的出现。公钥加密也叫不对称加密，不对称算法使用一对密钥对，一个公钥，一个私钥，使用公钥加密的数据，只有私钥能解开（可用于加密）；同时，使用私钥加密的数据，只有公钥能解开（签名）。但是速度很慢（比私钥加密慢100到1000倍），公钥的主要算法有RSA，还包括Blowfish，Diffie-Helman等，jdk1.5 种提供了对RSA的支持，是一个改进的地方： Java代码 /** *PublicExample.java *Copyright 2005-2-16 */ import java.security.Key. import javax.crypto.Cipher. import java.security.KeyPairGenerator. import java.security.KeyPair. /** * 一个简单的公加密例子,Cipher类使用KeyPairGenerator生成的公和私 */ public class PublicExample{ public static void main(String[] args) throws Exception{ if(args.length!=1){ System.err.println("Usage:java PublicExample 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