

Java加密和数字签名4数字签名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_644533.htm 数字签名：数字签名，它是确定交换消息的通信方身份的第一个级别。上面A通过使用公钥加密数据后发给B，B利用私钥解密就得到了需要的数据，问题来了，由于都是使用公钥加密，那么如何检验是A发过来的消息呢？上面也提到了一点，私钥是唯一的，那么A就可以利用A自己的私钥进行加密，然后B再利用A的公钥来解密，就可以了；数字签名的原理就基于此，而通常为了证明发送数据的真实性，通过利用消息摘要获得简短的消息内容，然后再利用私钥进行加密散列数据和消息一起发送。java中为数字签名提供了良好的支持，java.security.Signature类提供了

消息签名：Java代码 `/** *DigitalSignature2Example.java
*Copyright 2005-2-16 */ import java.security.Signature. import
java.security.KeyPairGenerator. import java.security.KeyPair. import
java.security.SignatureException. /** *数字签名，使用RSA私钥对
对消息摘要签名，然后使用公验证 测试 */ public class
DigitalSignature2Example{ public static void main(String[] args)
throws Exception{ if(args.length!=1){ System.err.println("Usage:java
DigitalSignature2Example 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`