Java加密和数字签名1消息摘要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_644536.htm 本文主要谈一下密码学中的加密和数字签名，以及其在java中如何进行使用。对密码学有兴趣的伙伴，推荐看Bruce Schneier的著作：Applied Crypotography.在jdk1.5的发行版本中安全性方面有了很大的改进，也提供了对RSA算法的直接支持，现在我们从实例入手解决问题（本文仅是作为简单介绍）：一、密码学上常用的概念 1）消息摘要：这是一种与消息认证码结合使用以确保消息完整性的技术。主要使用单向散列函数算法，可用于检验消息的完整性，和通过散列密码直接以文本形式保存等，目前广泛使用的算法有MD4、MD5、SHA-1，jdk1.5对上面都提供了支持，在java中进行消息摘要很简单，java.security.MessageDigest提供了一个简易的操作方法： Java代码 /** *MessageDigestExample.java *Copyright 2005-2-16 */ import java.security.MessageDigest. /** *单一的消息摘要算法，不使用密码.可以用来对明文消息（如：密码）隐藏保存 */ public class MessageDigestExample{ public static void main(String[] args) throws Exception{ if(args.length!=1){ System.err.println("Usage:java MessageDigestExample text"). System.exit(1). } byte[] plainText=args[0].getBytes("UTF8"). //使用getInstance("算法")来获得消息摘要,这里使用SHA-1的160位算法 MessageDigest messageDigest=MessageDigest.getInstance("SHA-1"). System.out.println(" " messageDigest.getProvider().getInfo()). //开始使用算法 messageDigest.0update(plainText).

System.out.println(" Digest:"). //输出算法运算结果
System.out.println(new String(messageDigest.digest(),"UTF8")). }}
还可以通过消息认证码来进行加密实现，javax.crypto.Mac提供了一个解决方案，有兴趣者可以参考相关API文档，本文只是简单介绍什么是摘要算法。 编辑特别推荐: Java核心API需要掌握的程度 Java编程实例：Java版农历和阳历转换源码 Java认证辅导:非阻塞I/O简介 Tomcat内存溢出的三种情况及解决办法分析 Java输入数据流详解 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