如何有效防止Java程序源码被人偷窥？[3] PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/244/2021_2022__E5_A6_82_E4_BD_95_E6_9C_89_E6_c104_244674.htm 为简单计，在本文中我们将用DES算法加密和解密字节码。下面是用JCE加密和解密数据必须遵循的基本步骤： 步骤1：生成一个安全密匙。在加密或解密任何数据之前需要有一个密匙。密匙是随同被加密的应用一起发布的一小段数据，Listing 3显示了如何生成一个密匙。 【Listing 3：生成一个密匙】以下是引用片段：// DES算法要求有一个可信任的随机数源 SecureRandom sr = new SecureRandom(). // 为我们选择的DES算法生成一个KeyGenerator对象 KeyGenerator kg = KeyGenerator.getInstance("DES"). kg.init(sr). // 生成密匙 SecretKey key = kg.generateKey(). // 获取密匙数据 byte rawKeyData[] = key.getEncoded(). /* 接下来就可以用密匙进行加密或解密，或者把它保存 为文件供以后使用 */ doSomething(rawKeyData). 步骤2：加密数据。得到密匙之后，接下来就可以用它加密数据。除了解密的ClassLoader之外，一般还要有一个加密待发布应用的独立程序(见Listing 4)。 【Listing 4：用密匙加密原始数据】 以下是引用片段：// DES算法要求有一个可信任的随机数源 SecureRandom sr = new SecureRandom(). byte rawKeyData[] = /* 用某种方法获得密匙数据 */. // 从原始密匙数据创建DESKeySpec对象 DESKeySpec dks = new DESKeySpec(rawKeyData). // 创建一个密匙工厂，然后用它把DESKeySpec转换成 // 一个SecretKey对象 SecretKeyFactory keyFactory = SecretKeyFactory.getInstance(

"DES"). SecretKey key = keyFactory.generateSecret(dks). // Cipher对象实际完成加密操作 Cipher cipher = Cipher.getInstance("DES"). // 用密匙初始化Cipher对象 cipher.init(Cipher.ENCRYPT_MODE, key, sr). // 现在，获取数据并加密 byte data[] = /* 用某种方法获取数据 */ // 正式执行加密操作 byte encryptedData[] = cipher.doFinal(data). // 进一步处理加密后的数据 doSomething(encryptedData). 步骤3：解密数据。运行经过加密的应用时，ClassLoader分析并解密类文件。操作步骤如Listing 5所示。 【Listing 5：用密匙解密数据】 // DES算法要求有一个可信任的随机数源 SecureRandom sr = new SecureRandom(). byte rawKeyData[] = /* 用某种方法获取原始密匙数据 */. // 从原始密匙数据创建一个DESKeySpec对象 DESKeySpec dks = new DESKeySpec(rawKeyData). // 创建一个密匙工厂，然后用它把DESKeySpec对象转换成 // 一个SecretKey对象 SecretKeyFactory keyFactory = SecretKeyFactory.getInstance("DES"). SecretKey key = keyFactory.generateSecret(dks). // Cipher对象实际完成解密操作 Cipher cipher = Cipher.getInstance("DES"). // 用密匙初始化Cipher对象 cipher.init(Cipher.DECRYPT_MODE, key, sr). // 现在，获取数据并解密 byte encryptedData[] = /* 获得经过加密的数据 */ // 正式执行解密操作 byte decryptedData[] = cipher.doFinal(encryptedData). // 进一步处理解密后的数据 doSomething(decryptedData). 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