

Java非对称加密的源代码(RSA)计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/646/2021_2022_Java_E9_9D_9E_E5_AF_B9_c97_646075.htm 鉴于rsa加密的重要性和相关源代码的匮乏，经过整理特此贴出。需要下载bcprov-jdk14-123.jar。下载地址

: www.bouncycastle.org/latest_releases.html

```
import
javax.crypto.Cipher. import java.security.*. import
java.security.spec.RSAPublicKeySpec. import
java.security.spec.RSAPrivateKeySpec. import
java.security.spec.InvalidKeySpecException. import
java.security.interfaces.RSAPrivateKey. import
java.security.interfaces.RSAPublicKey. import java.io.*. import
java.math.BigInteger. /** * RSA 工具类。提供加密，解密，生成
密钥对等方法。 * 需要到http://www.bouncycastle.org下
载bcprov-jdk14-123.jar。 * */ public class RSAUtil { /** * 生成密
钥对 * @return KeyPair * @throws EncryptException */ public static
KeyPair generateKeyPair() throws EncryptException { try {
KeyPairGenerator keyPairGen =
KeyPairGenerator.getInstance("RSA", new
org.bouncycastle.jce.provider.BouncyCastleProvider()). final int
KEY_SIZE = 1024.//没什么好说的了，这个值关系到块加密的
大小，可以更改，但是不要太大，否则效率会低
keyPairGen.initialize(KEY_SIZE, new SecureRandom()). KeyPair
keyPair = keyPairGen.genKeyPair(). return keyPair. } catch
(Exception e) { throw new EncryptException(e.getMessage()). } }
```

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