Java常用的加密解密数字签名等API PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/273/2021_2022_Java_E5_B8_B8_E7_94_A8_c104_273299.htm 常用API java.security.KeyPairGenerator 密钥生成器类 public static KeyPairGenerator getInstance(String algorithm) throws NoSuchAlgorithmException 以指定的算法返回一个KeyPairGenerator 对象 参数: algorithm 算法名. 如:"DSA","RSA" public void initialize(int keysize) 以指定的长度初始化KeyPairGenerator对象,如果没有初始化系统以1024长度默认设置 参数:keysize 算法位长.其范围必须在 512 到 1024 之间，且必须为 64 的倍数 public void initialize(int keysize, SecureRandom random) 以指定的长度初始化和随机发生器初始化KeyPairGenerator对象 参数:keysize 算法位长.其范围必须在 512 到 1024 之间，且必须为 64 的倍数 random 一个随机位的来源(对于initialize(int keysize)使用了默认随机器 public abstract KeyPair generateKeyPair() 产生新密钥对 java.security.KeyPair 密钥对类 public PrivateKey getPrivate() 返回私钥 public PublicKey getPublic() 返回公钥 java.security.Signature 签名类 public static Signature getInstance(String algorithm) throws NoSuchAlgorithmException 返回一个指定算法的Signature对象 参数 algorithm 如:"DSA" public final void initSign(PrivateKey privateKey) throws InvalidKeyException 用指定的私钥初始化 参数:privateKey 所进行签名时用的私钥 public final void 0update(byte data) throws SignatureException public final void 0update(byte[] data) throws SignatureException public final void

0update(byte[] data, int off, int len) throws SignatureException 添加要签名的信息 public final byte[] sign() throws SignatureException 返回签名的数组,前提是initSign和0update public final void initVerify(PublicKey publicKey) throws InvalidKeyException 用指定的公钥初始化 参数:publicKey 验证时用的公钥 public final boolean verify(byte[] signature) throws SignatureException 验证签名是否有效,前提是已经initVerify初始化 参数: signature 签名数组 