信息安全技术之密码学实验指导书

2020.11.29

目录

[Java环境配置 3](#_Toc57491453)

[DES加解密 4](#_Toc57491454)

[AES加解密 5](#_Toc57491455)

[RSA加解密操作 6](#_Toc57491456)

[SHA256信息摘要算法 7](#_Toc57491457)

[RSA签名验证操作 8](#_Toc57491458)

[利用keytool生成证书 9](#_Toc57491459)

# Java环境配置

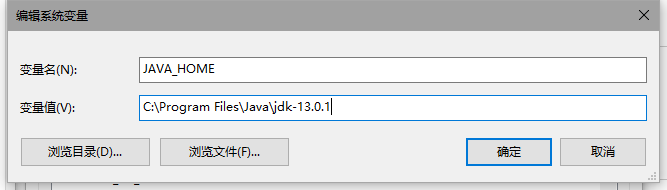
从ORACLE官网下载jdk安装包

从Oracle官网下载jdk (Java Development Kit)安装包进行安装

<https://www.oracle.com/technetwork/java/javase/downloads/index.html>

配置环境变量JAVA\_HOME为jdk默认安装目录

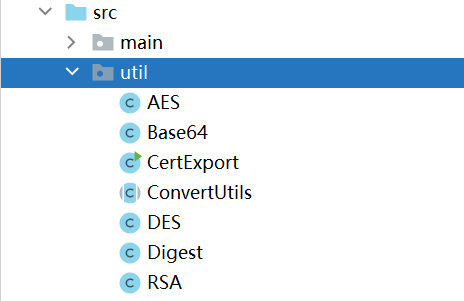
环境变量PATH中添加%JAVA\_HOME%\bin





打开控制台，分别输入java -version、javac -version查看是否有信息输出，有信息输出说明环境配置成功。

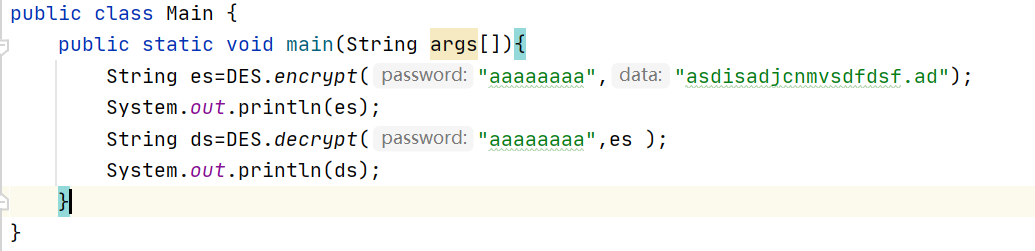
提供的源代码文件位于util包下，组织结构如下图所示：



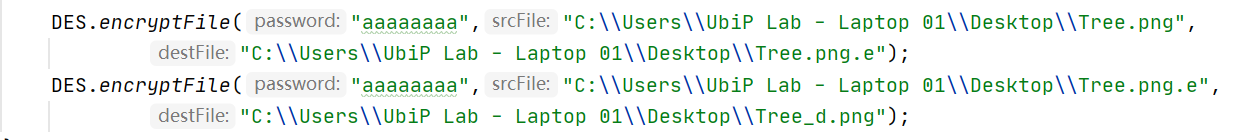
# DES加解密

DES全称为Data Encryption Standard，即数据加密标准，是一种使用密钥加密的块算法，1977年被美国联邦政府的国家标准局确定为联邦资料处理标准（FIPS），并授权在非密级政府通信中使用，随后该算法在国际上广泛流传开来。

DES加解密工具代码已给出，使用如下方式进行字符串的加解密操作:



使用如下方式进行文件的加解密操作：

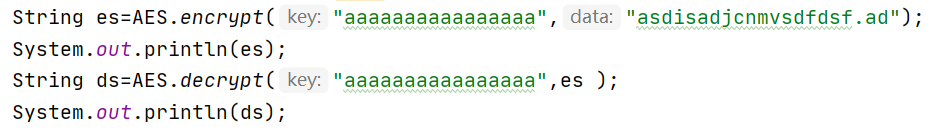


对实验结果进行截图，尝试对不同类型的文件，如视频、音频等进行加解密处理。

# AES加解密

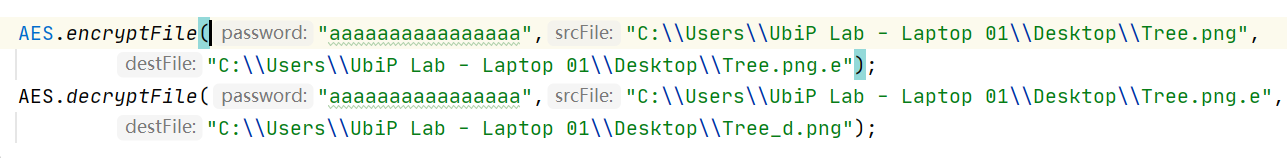
AES全称为Advanced Encryption Standard，是美国联邦政府采用的一种区块加密标准，用来替代原先的DES。

AES加解密工具代码已给出，使用如下方式进行字符串加解密操作：



注意，这里的密钥必须为16字节(128位)。

使用如下方式对文件进行加解密：



对运行结果进行截图，对实验结果进行截图，尝试对不同类型的文件，如视频、音频等进行加解密处理。

# RSA加解密操作

RSA加密算法，是世界上第一个非对称加密算法，也是数论的第一个实际应用。它的算法如下：

1.找两个非常大的质数p和q（通常p和q都有155十进制位或都有512十进制位）并计算n=pq，k=(p-1)(q-1)。

2.将明文编码成整数M，保证M不小于0但是小于n。

3.任取一个整数e，保证e和k互质，而且e不小于0但是小于k。加密钥匙（称作公钥）是(e, n)。

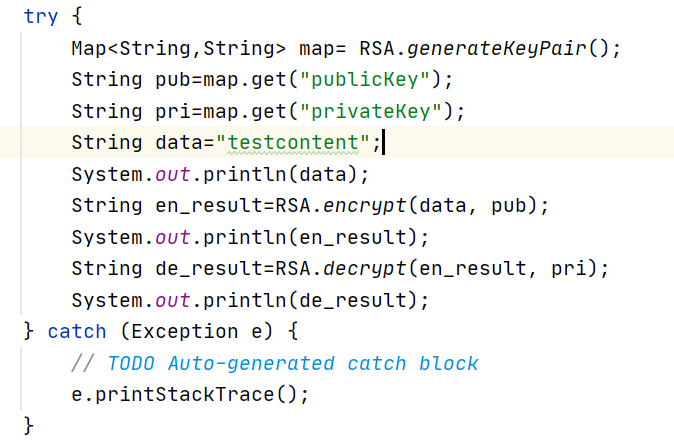
4.找到一个整数d，使得ed除以k的余数是1（只要e和n满足上面条件，d肯定存在）。解密钥匙（称作密钥）是(d, n)。

加密过程： 加密后的编码C等于M的e次方除以n所得的余数。

解密过程： 解密后的编码N等于C的d次方除以n所得的余数。

只要e、d和n满足上面给定的条件。M等于N。

通过如下方式对字符串进行加解密：



对实验结果进行截图，比较RSA加解密操作与前文中对称加密算法加解密操作的不同。

# SHA256信息摘要算法

SHA256是SHA-2下细分出的一种算法，产生的输出是一个256-bit 的报文摘要。能够计算出一段信息的摘要，也即数字签名。利用数字签名可以知道消息是否被更改过，可以认证消息是否是确实来自意定的信源，还可以使信源不能否认曾将发送的消息。

Java中提供了多个信息摘要算法，在工程中引入java.security.MessageDigest

对一个字符串提取信息摘要的方法如下:

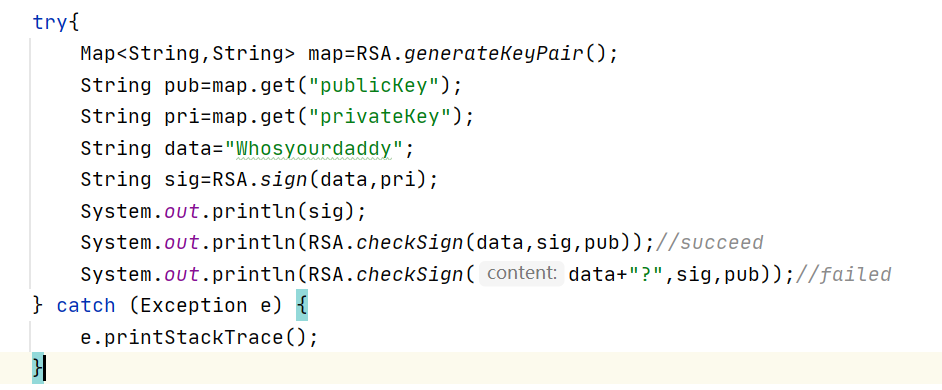


对实验结果进行截图，对输入信息进行微小更改并比较信息摘要结果(例如abcdefghijklmnopqrstuvwxyz与abcdefghijklmnopqrstuvwxyx)。

# RSA签名验证操作

RSA算法与hash算法结合可进行签名操作，明文信息与其hash值共同使用RSA私钥进行签名，任一持有RSA公钥者可对签名进行验证。

使用如下方式进行签名与验签操作：

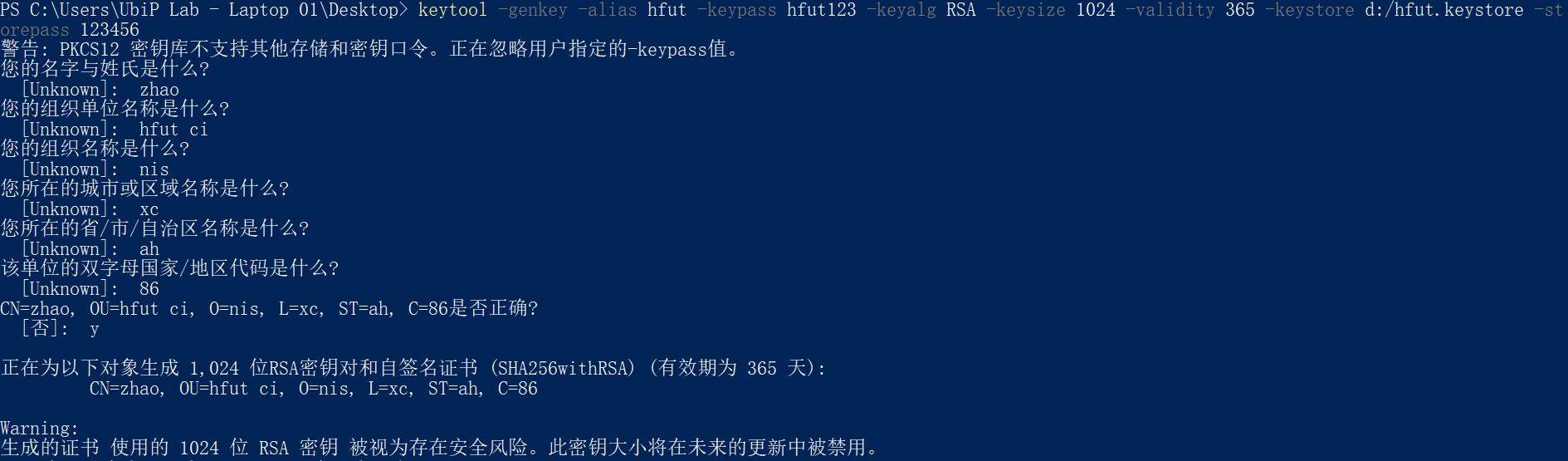


对实验结果进行截图。

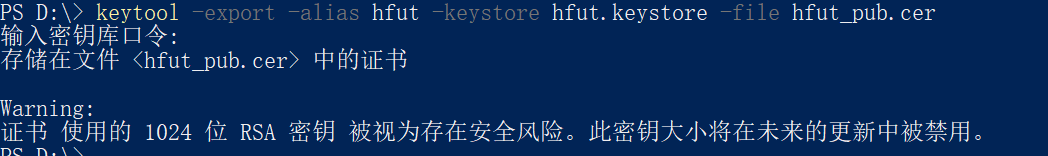
# 利用keytool生成证书

keytool 是一个密钥和证书管理工具。它使用户能够管理自己的公钥/私钥对及相关证书，用于（通过数字签名）自我认证（用户向别的用户/服务认证自己）或数据完整性以及认证服务。它还允许用户储存他们的通信对等者的公钥（以证书形式）。

使用以下命令生成keystore：



切换至keystore目录下，使用以下命令导出证书文件：



双击打开可观察到如下信息：

