**密码学基础实验**

# **一、实验原理**

## **1.1 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。

对称性：DES是对称的，也就是说它使用同一个密钥来加密和解密数据。与此相对的是RSA加密算法，是一种非对称加密算法

分组性：DES还是一种分组加密算法，该算法每次处理固定长度的数据段，称之为分组。DES分组的大小是64位，如果加密的数据长度不是64位的倍数，可以按照某种具体的规则来填充位。

“混乱和扩散”的原则：混乱的目的是为隐藏任何明文同密文、或者密钥之间的关系，而扩散的目的是使明文中的有效位和密钥一起组成尽可能多的密文。两者结合到一起就使得安全性变得相对较高。

DES算法具体通过对明文进行一系列的排列和替换操作来将其加密：过程的关键就是从给定的初始密钥中得到16个子密钥的函数。要加密一组明文，每个子密钥按照顺序（1-16）以一系列的位操作施加于数据上，每个子密钥一次，一共重复16次。每一次迭代称之为一轮。要对密文进行解密可以采用同样的步骤，只是子密钥是按照逆向的顺序（16-1）对密文进行处理。

## **1.2 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加密过程涉及到4种操作：字节替代（Sub Bytes）、行移位（Shift Rows）、列混淆（Mix Columns）和轮密钥加（Add Round Key）。解密过程分别为对应的逆操作。由于每一步操作都是可逆的，按照相反的顺序进行解密即可恢复明文。加解密中每轮的密钥分别由初始密钥扩展得到。算法中16字节的明文、密文和轮密钥都以一个4⨉4的矩阵表示。AES的具体加密解密流程，如图1.1所示。

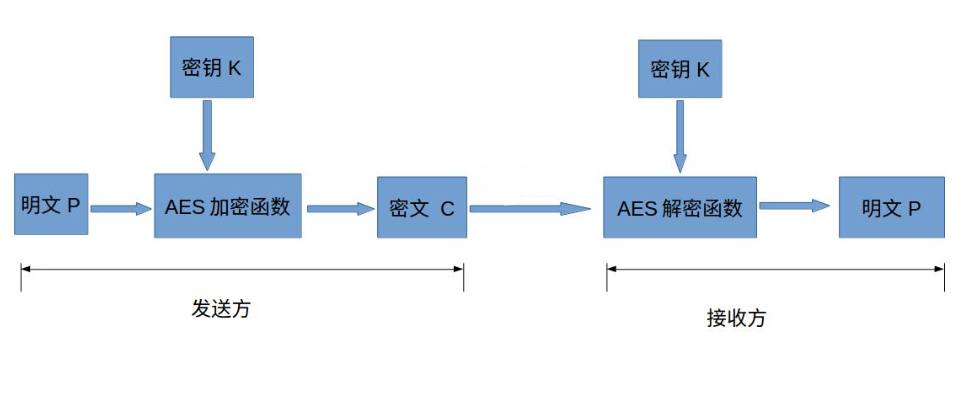


图 1.1 AES加密解密流程

下面简单介绍下各个部分的作用与意义：

**明文P**：

没有经过加密的数据。

**密钥K**

用来加密明文的密码，在对称加密算法中，加密与解密的密钥是相同的。密钥为接收方与发送方协商产生，但不可以直接在网络上传输，否则会导致密钥泄漏，通常是通过非对称加密算法加密密钥，然后再通过网络传输给对方，或者直接面对面商量密钥。密钥是绝对不可以泄漏的，否则会被攻击者还原密文，窃取机密数据。

**AES加密函数**

设AES加密函数为E，则 C = E(K, P),其中P为明文，K为密钥，C为密文。也就是说，把明文P和密钥K作为加密函数的参数输入，则加密函数E会输出密文C。

**密文C**

经加密函数处理后的数据

**AES解密函数**

设AES解密函数为D，则 P = D(K, C),其中C为密文，K为密钥，P为明文。也就是说，把密文C和密钥K作为解密函数的参数输入，则解密函数会输出明文P。

## **1.3 RSA加解密**

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：

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)。

将明文编码成整数M，保证M不小于0但是小于n。

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)。

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。

# **二、实验环境**

## **2.1 硬件**

Dell G3579笔记本电脑。

## **2.2 软件**

运行系统：Windows 10 Pro N for Workstations

开发工具：VSCode

编程语言：java

**三、实验结果**

**3.1 DES加解密实验**

**3.1.1 加解密字符串“abcdef”**

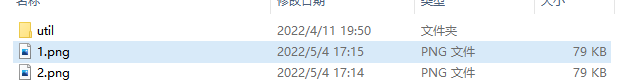
代码：



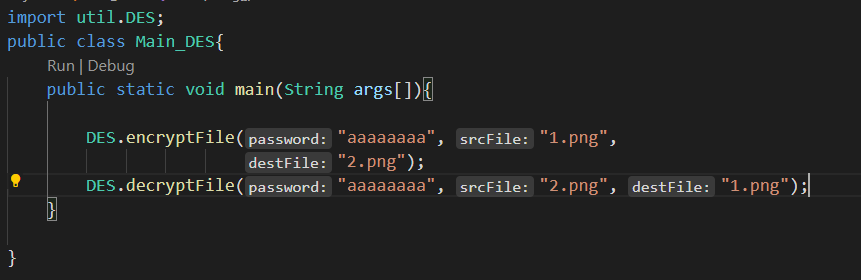
运行结果：



**3.1.2 加解密图片**



代码：



原始图片：



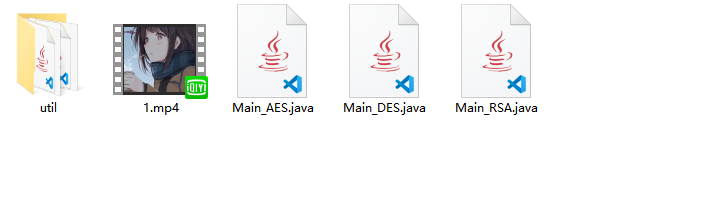
加密后：



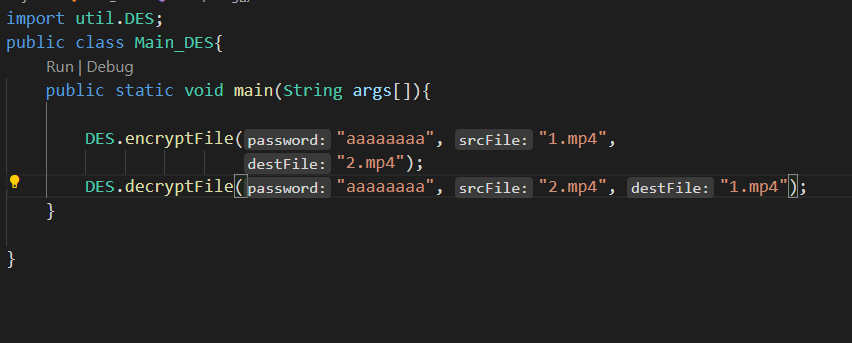
解密后：



**3.1.3 加解密视频**



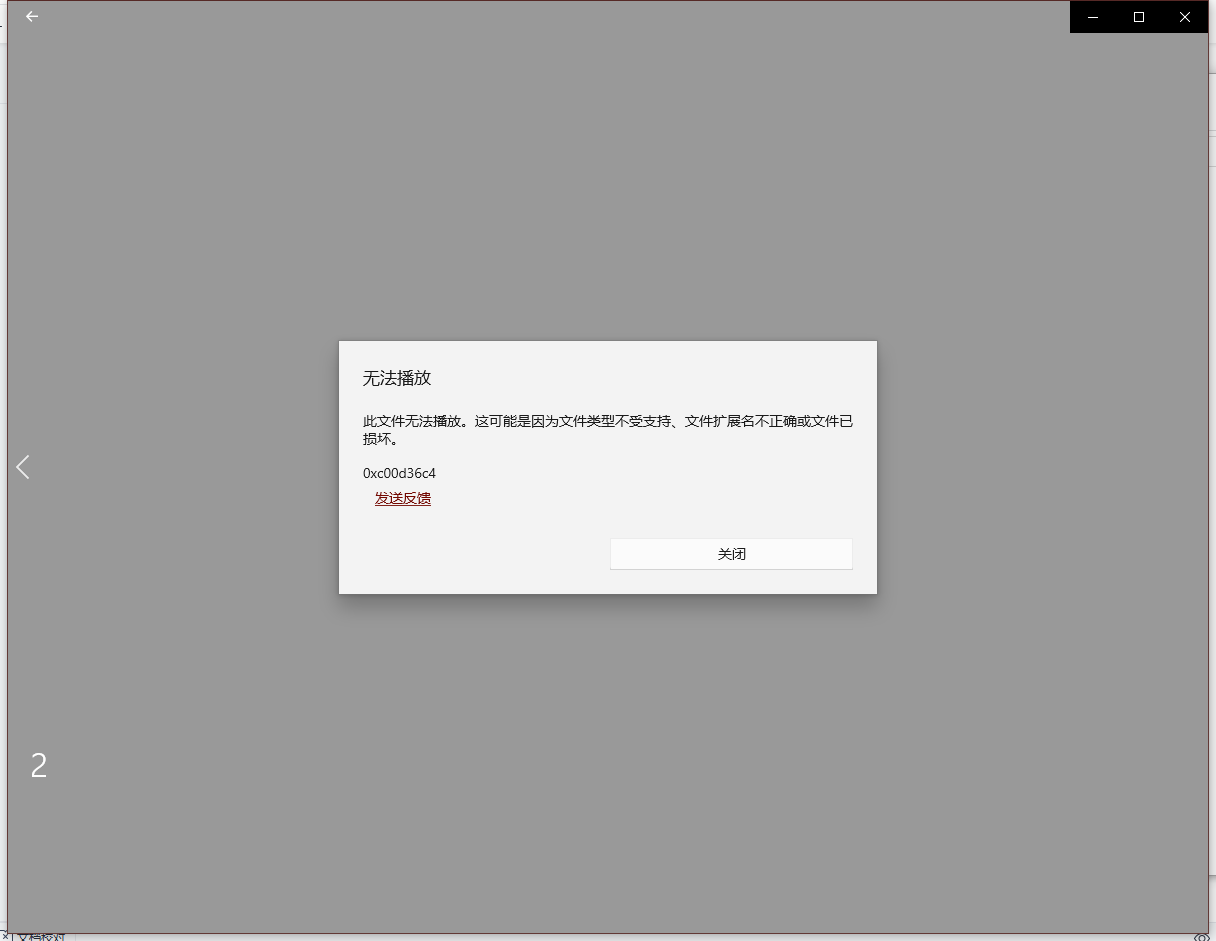
代码：



加密前：



加密后：



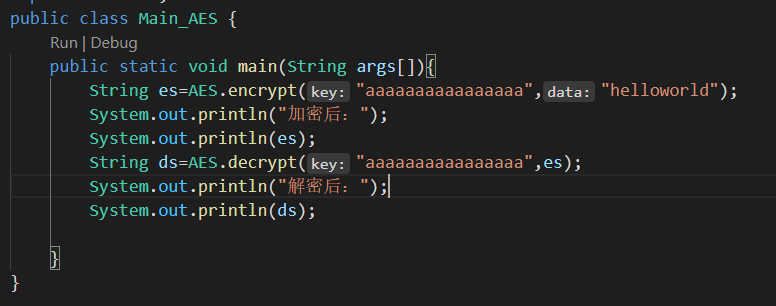
解密后：



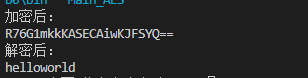
**3.2 AES加解密实验**

**3.2.1 加解密字符串“helloworld”**

代码

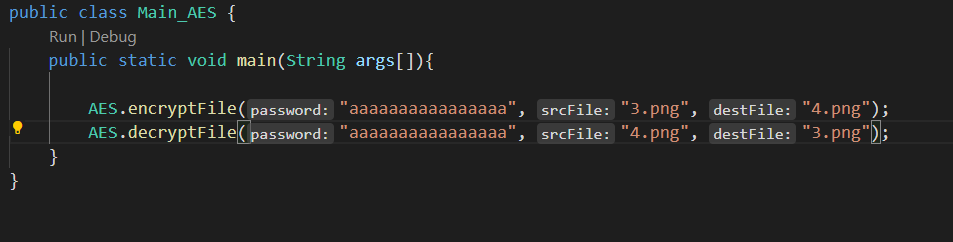


运行结果：



**3.2.2 加解密图片**

代码：



原始图片：



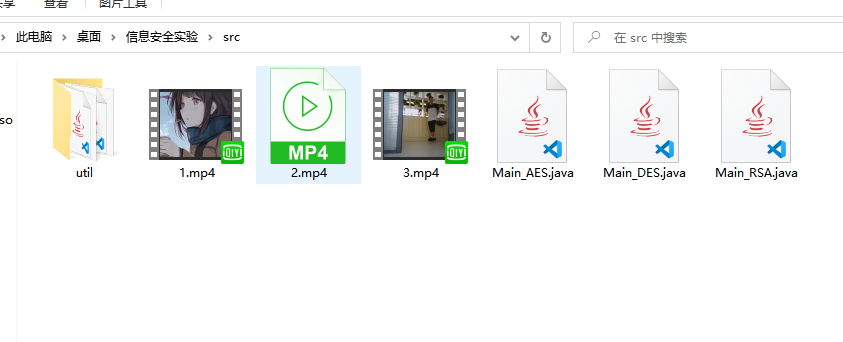
加密后：



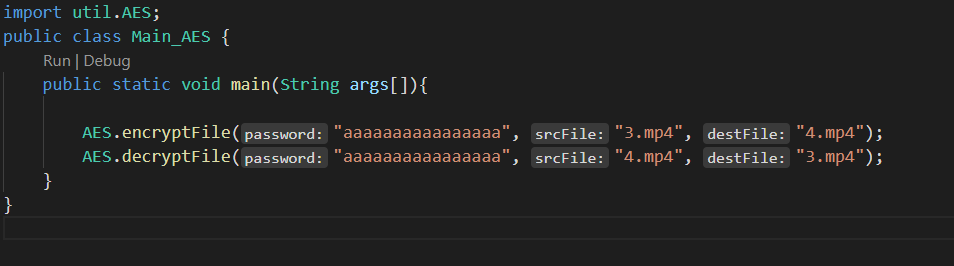
解密后：



**3.2.3 加解密视频**



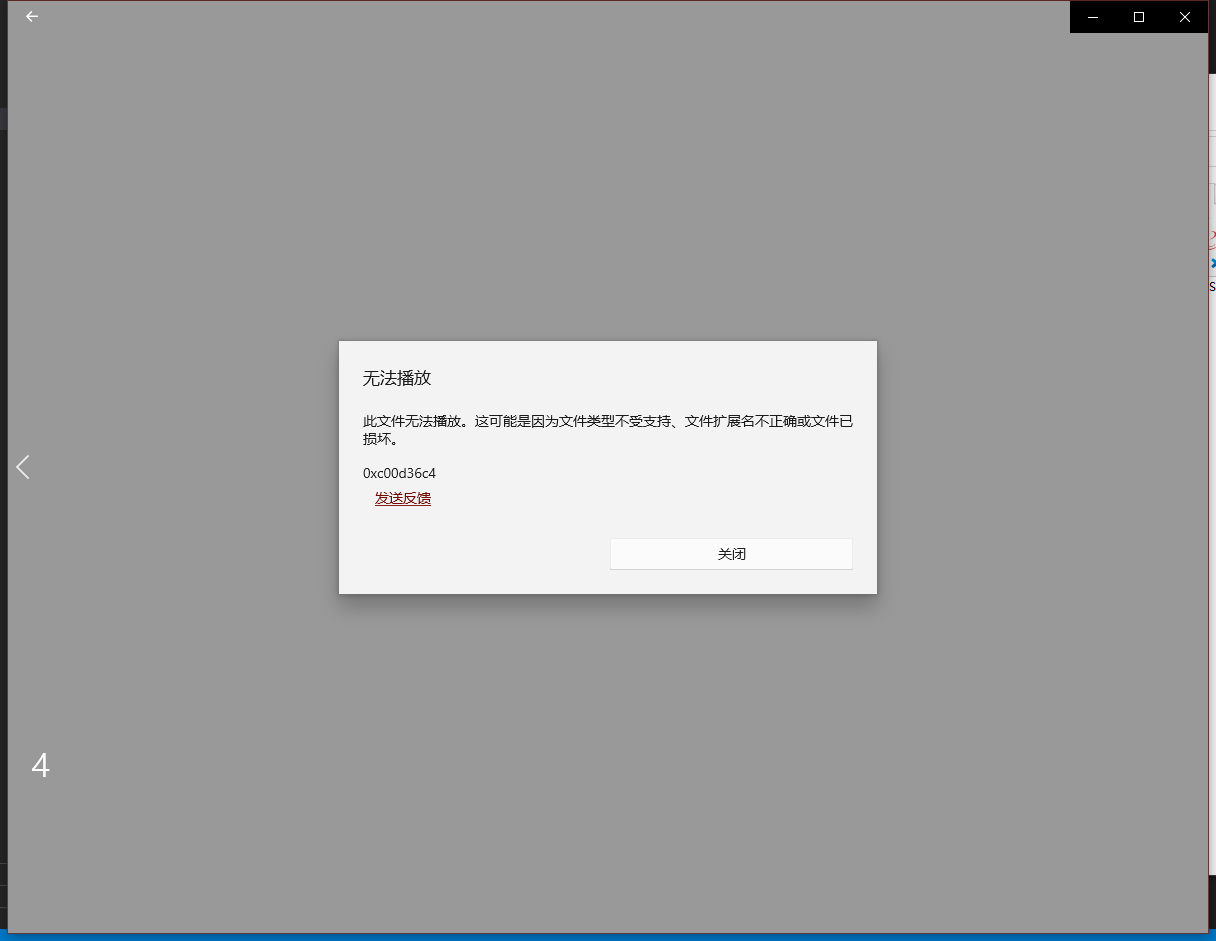
代码：



加密前：



加密后：



解密后：



**3.3 RSA 加解密实验**

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。

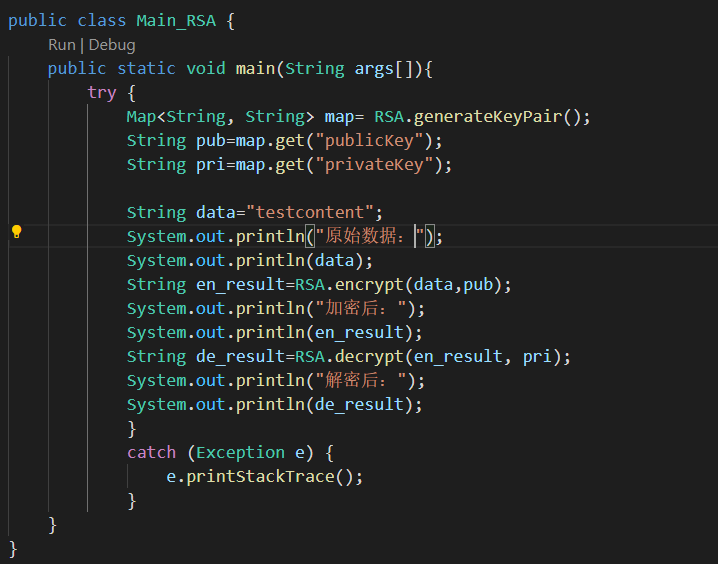
3.任取一个整数 e，保证 e 和 k 互质，而且 e 不小于 0 但是小于 k。加密钥匙（称作公钥）是(e, n)。

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)。

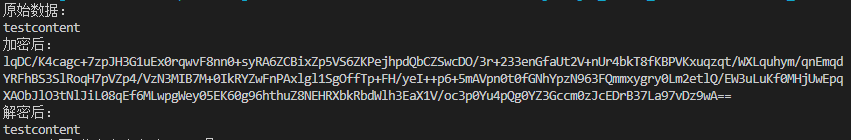
加密过程： 加密后的编码 C 等于 M 的 e 次方除以 n 所得的余数。

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。

**3.3.1 代码**



**3.3.2 运行结果**



非对称加密算法（如RSA）同前文所述DES、AES等对称加密算法不同的是，对称加密算法的加密与解密密钥相同，而非对称加密算法的加密密钥与解密密钥不同。众所周知，RSA加密算法基于一个十分简单的数论事实：将两个大素数相乘十分容易，但想要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。