**密码学原理**

**实验三：公钥加密**

学号： 姓名：

**实验目的**：本实验旨在让学生掌握运用密码学工具生成RSA密钥，进行非对称加解密，并分析相同因子RSA公钥理解RSA的安全性。

1. **公钥加密**
2. 使用密码学工具实现混合加密过程

要求：生成RSA密钥对（公钥1和私钥1），用公钥1加密对称密钥并采用对称加密方法加密图片，用私钥1解密对称密钥，然后解密图片。（你可以使用实验二中的对称加密方案）

1. **相同因子公钥分析**
2. 通过分析RSA公钥的因子得到私钥并破解加密信息

要求：分析附件中给出的两个公钥（公钥1、公钥2，均为pem格式）中大整数的公共因子，得到公钥1的私钥，并用私钥解密对称密钥，再解密对称加密的图片。

* 1. 对称加密方法为密钥长度128位的AES-CBC，对明文采用[PKCS #7](https://datatracker.ietf.org/doc/html/rfc2315#section-10.3)填充，128位IV放在密文开头。
  2. 对称加密的明文为RGBA四通道图像中的所有像素，为使密文图片尺寸合法，对密文进行了填充，以四字节（一个像素）为单位，与[PKCS #7](https://datatracker.ietf.org/doc/html/rfc2315#section-10.3)类似，即如果密文图像最后一个像素转换为四字节整数的值为k（大端序），说明密文图像的后k个像素是padding。由此填充方法产生的密文图片比明文图片多一行像素。
  3. 对称加密产生的密文图片为enc1.png
  4. 128位对称密钥先进行Base64编码，再使用公钥1加密，加密方法为RSA-OAEP，密文的Base64编码在下面给出。

|  |
| --- |
| **公钥1：**  -----BEGIN PUBLIC KEY-----  MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAuz20BUTcqVDjzEOKiJF9  66LbQB/59lnXTj/SmiD07mV1XE03BLrWfi7jFh/iq5ZPzVXfbNPjHiojO9WRhWzr  wiQGZNVZ7qFoO/PzXOT8OyHyOMcrb6ogtCyFvDOeximr3M/ICmliU2JxbLSfteZj  AplHJVgs5bJ5LTW7eSy1x2Z5aOsHjesK3rkLi1yB2jM0MeaNIB/Enb82bBMKzAam  vN6tY8bQbEoRbTnlX6PUfkU9w7XsWLMa3QbpIH9mNam1Qz4ynCjWXcDo6KzYotUf  TgGlIIOOJKsAqgOgSHqTz83e8bBizPwJg+CxBzP4Ha8C9phc41i2GiEgDf4J1J0R  0BZDcJEgZIlI+B5tlvJTy/uQyvmEP+hyMD8d83RdzLYy9h8u0MNHjJygY/Kktftp  wPtZPThpMOWWbOMM72a8Y2usz5rKTBAe+bN5QyELCErc/aQB0ABUSsNf4XxaQWbz  gJdb3hEvUkas0PfHui8UB6Yuaa7RmEE6EPIELx2WF2BGw1AG8vg5mi3I+HYxpk9W  mxy2gj63UPqr1f0u7+fnig7ANlyyPYG3LLUfhBT/d9VH0W644lqF8eZo0INEHfQf  +g4qvVVSTWfuC84ky5gTnWMbzB0iqVsZD3xw4wfSrSKyK6QFNESNdOo+1E0nz83I  cQAFD+zSSMLgodHCgA9GlGECAwEAAQ==  -----END PUBLIC KEY-----  **公钥2：**  -----BEGIN PUBLIC KEY-----  MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAymf92H5ljvvfTE8QjuOd  xv7YPOxXC05VceuSjtZN1aDb/4gqpWxDyMzRrPS8VRQTxkqWia4nd//zj+dheHNv  6+Emb3f00IyC2bcAFvDgQmnQB0sJZf2UI3mbMfLdnsIYW2YCbvxEiFYmUUOnh6xP  AnYFtZuvh9EDpyUwT95thQS23UEO2M1y5Q9SRUZo4EeQGb6/iqB6Q5FYabRqbsXe  Ckqxk1ENkPpuLkiQCtra++bICj4WbfVCOiiYpaN/faVud6qMHxsCxxkk+2p7kcs3  ZsCSEmLBzFNmzT32pMK9pq/rAXyXbGh4ECDuTdk1va/cCxIr5Ongven4oe4qGdnj  OCD9xPNfQZDSpYMaBcn1UveM9Rrv/GYaC9AgMnVvG5PaQOYKJzETU2gJm4rdPp/M  Hc9CvN30B6X9ewsLYIaA8ES/DRIqMG4GKAgMz0siROwLXMSkLXg1u4+mLeQzBQP5  TPJ5qwAwKJc6uPPoXo9ZmFnFW4THCoEJ+caax9M0Urg4+B6ids73C2u8A6xqVXld  ng0pAdt5exZqckhPWaWajFt4mmbUmlot7GU9PxV+NDhCn4YDmhBKQRin4lkuLilM  0/WmvnVxD7IhgXbDYrP7E1j/IO9VZQOGkntVT/BtvhJLQauF6J2bxyct9GD6Ahg4  BBKL1/FPLaDsmzWqbNiJKp8CAwEAAQ==  -----END PUBLIC KEY-----  **使用公钥1加密的对称密钥：**   |