**S-AES**

**测试结果（共五关）**

**第一关：基本测试**

基本测试格式如下：

明文：16位二进制数

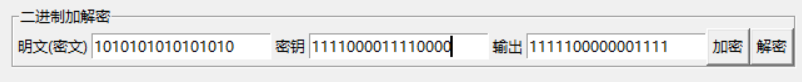
密文：16位二进制数

密钥：16位二进制数

**标准加密**

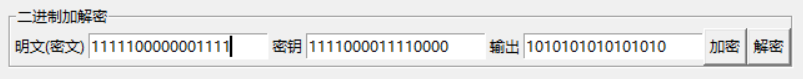
按照实验基本要求的输入格式，输入明文和密钥。

测试结果：



**标准解密**

按照实验基本要求的输入格式，将加密得到的密文和加密使用的密钥作为输入，看能否解密得到被加密的明文。

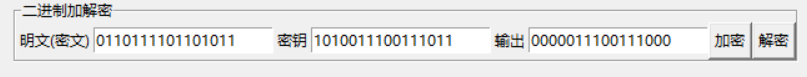


在基本加解密测试中，加密所用的密钥和明文能够与解密所用密钥与密文对应，说明基本加解密通过测试。

**第二关：交叉测试**

结果如下：

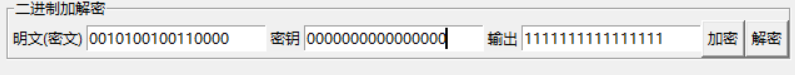
加密：

****

[](https://private-user-images.githubusercontent.com/170654582/380733961-eccea4d8-c290-46e4-9ce9-e90c2b9db278.png?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3MzA0NDAwMTYsIm5iZiI6MTczMDQzOTcxNiwicGF0aCI6Ii8xNzA2NTQ1ODIvMzgwNzMzOTYxLWVjY2VhNGQ4LWMyOTAtNDZlNC05Y2U5LWU5MGMyYjlkYjI3OC5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjQxMTAxJTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI0MTEwMVQwNTQxNTZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT05OGVhZDE1OWE4YzFiNjY0ZjA2MTRmYzYxMjNkYWUzYzI5YmY2ZGIzNjY1NmY3OTc0NTMzMTVhNTgxYzM3NmUzJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.6_zTnQCqF7M-U0B6Wn1jSY1wEzKMm6SplnaLkNb7NFE)

**使用相同的密钥和明文能够得出相同的加密结果，加密通过测试。**

**解密：**

****

[](https://private-user-images.githubusercontent.com/170654582/380734083-8a0187c2-7854-4b93-ac07-4ee36ed9d979.png?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3MzA0NDAwMTYsIm5iZiI6MTczMDQzOTcxNiwicGF0aCI6Ii8xNzA2NTQ1ODIvMzgwNzM0MDgzLThhMDE4N2MyLTc4NTQtNGI5My1hYzA3LTRlZTM2ZWQ5ZDk3OS5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjQxMTAxJTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI0MTEwMVQwNTQxNTZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT1jMTcyOWNlY2UwMzVkYjcyM2ViYzVmYTZjNGIwMmY0NjFkMDBmNDhmYWExNjNjZmFkNWZkNTU3Y2ZjMTE3MzIyJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.czkjfE0AHADtn5qcylf0TebKupktIojsKjmBcti7w2Q)

**使用相同的密钥和密文能够得出相同的解密结果，解密通过测试。**

**第三关：扩展功能**

考虑到向实用性扩展，加密算法的数据输入可以是ASII编码字符串(分组为2 Bytes)，对应地输出也可以是ACII字符串(很可能是乱码)。

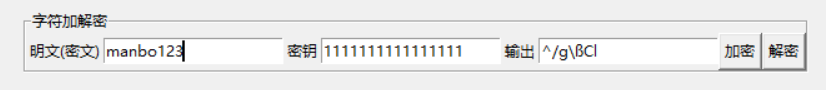
扩展功能测试输入格式如下：

明文：任意ASCII编码字符串

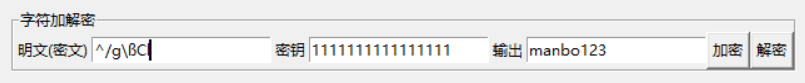
密钥：16bit二进制数

*注意:密钥应该为16bits 加密后极大可能出现乱码*

**以下是加密测试**



**以下是解密测试**



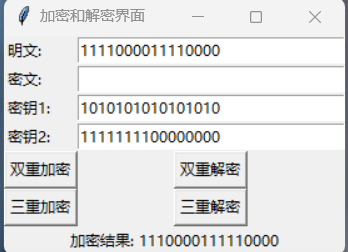
**第四关：多重加密**

**1.双重加解密的实现**

**双重加密**

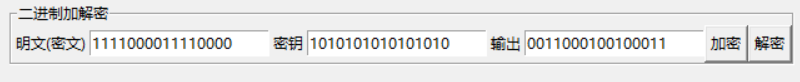
在完成基础的加解密功能之外，还完成了双重加密功能，使用两个16位的密钥，将密钥分为密钥1和密钥2，先使用key1加密明文，再使用key2加密密文，得到最终的加密结果 对此我们使用了下面的测试。

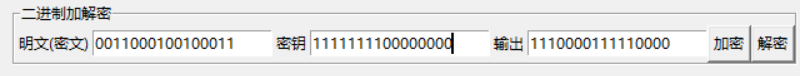
测试结果如下：



**这里我们按照双重加密的步骤使用AES分别进行两次加密，如果得到相同结果，则测试成功。**

分别进行两次加密结果如下



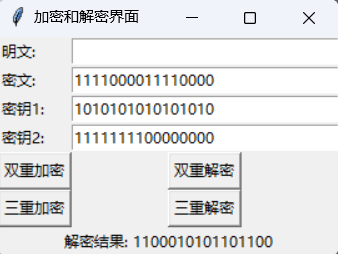


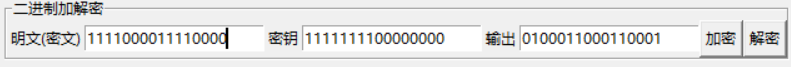
**由于进行双重加密和分别进行两次加密得到了相同的密文，因此测试成功。**

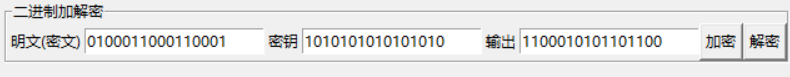
**双重解密**

按照实验基本要求的输入格式，将加密得到的密文和加密使用的密钥作为输入，看能否解密得到被加密的明文。

测试结果如下：







**在双重解密测试中，加密所用的密钥和明文能够与解密所用密钥与密文对应，说明双重解密通过测试。**

**2.中间相遇攻击**

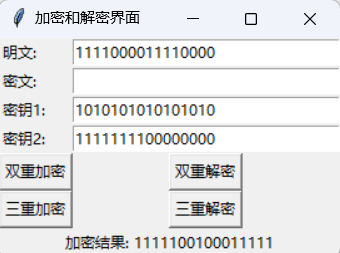
**3.三重加解密的实现**

与双重加解密类似：这里我们按照32bits密钥key（k1+k2）的模式进行三重加密，key=key1+key2+key3(key1)，依次使用key1、key2、key3对明文、中间态、第二次加密得到的中间态进行加密，得到密文，解密过程则相反。

对此我们使用了下面的测试来进行验证：

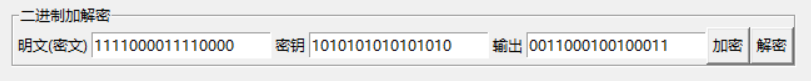
**三重加密：**

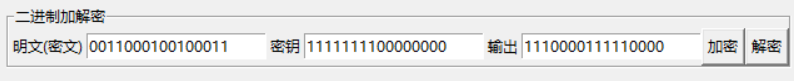
测试结果如下

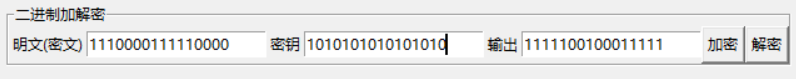


这里我们按照三重加密的步骤使用AES分别进行三次加密，如果得到相同结果，则测试成功。

分别进行三次加密结果如下





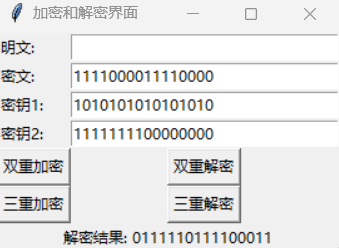


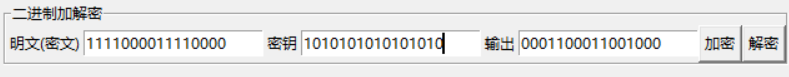
**由于进行三重加密和分别进行三次加密得到了相同的密文，因此测试成功。**

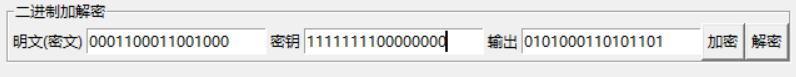
**三重解密：**

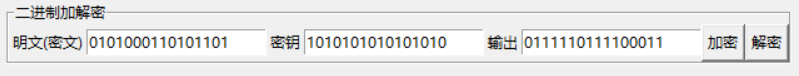
按照实验基本要求的输入格式，将加密得到的密文和加密使用的密钥作为输入，看能否解密得到被加密的明文。

测试结果如下





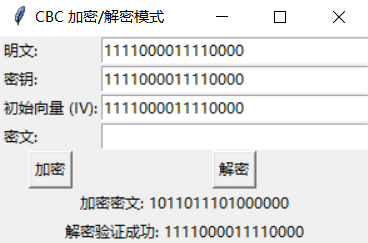


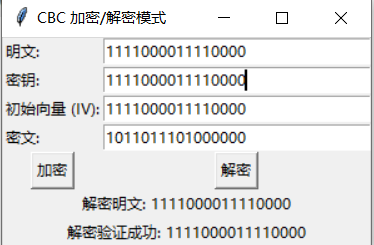


**在三重解密测试中，加密所用的密钥和明文能够与解密所用密钥与密文对应，说明三重解密通过测试。**

**第五关：工作模式**

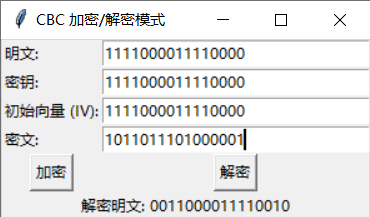
CBC模式下进行加解密，测试结果如下：





加解密测试成功

篡改密文后解密：



明密文不一致，测试成功