作品类别： ☑软件设计 ☐硬件制作 ☐工程实践

密码学大作业设计报告

题目：基于 RSA 和 DES 的密钥及信息传输

2024 年 6 月 8 日

曾建钦 PB22030856

中国科学技术大学

网络空间安全学院 221 班

基本信息表
作品题目：基于 RSA 和 DES 的密钥及信息传输
作品类别：☑软件设计　☐硬件制作　☐工程实践
作品内容摘要：作品主要基于 RSA 和 DES 的算法，希望实现基本的 RSA 和 DES 加密算法，实现用 RSA 算法对 DES 密钥的加密，传输消息的 DES 加密，模拟密钥与消息安全传输和密钥与消息的 DES 解密
关键词（五个）：RSA，DES，对称加密密钥，非对称加密，对称加密

1.作品功能与性能说明

1) 实现对称加密密钥（DES 密钥）的模拟传输

功能：用 RSA 加密 DES 密钥，实现密钥的安全传输。

实现：使用 RSA 公钥加密 DES 密钥。

使用 RSA 私钥解密 DES 密钥。

功能：用 DES 加密文本和图片消息，实现消息的安全传输。

实现：使用 DES 密钥加密文本消息和图片消息。

使用 DES 密钥解密文本消息和图片消息。

2) 实现 RSA 的非对称加密

功能：生成公钥和私钥，对消息进行加密和解密。

实现：使用 Python 的 rsa 库生成一对密钥。

公钥用于加密消息，私钥用于解密消息。

3) 实现 DES 的对称加密

功能：生成 DES 密钥，对消息进行加密和解密。

实现：使用 Python 的 pyDes 库生成 DES 密钥。

DES 密钥用于加密和解密消息。

4) 实现简要的交互功能

2.设计与实现方案

期望通过 Python 环境来实现基本的 RSA 和 DES 的加密过程，主要采用 Python 两个库函数 rsa 和 pyDes 两来实现基本的功能，交互界面采用 tkinter 实现，传输信息以文本消息和图片消息进行示例。

2.1 实现原理

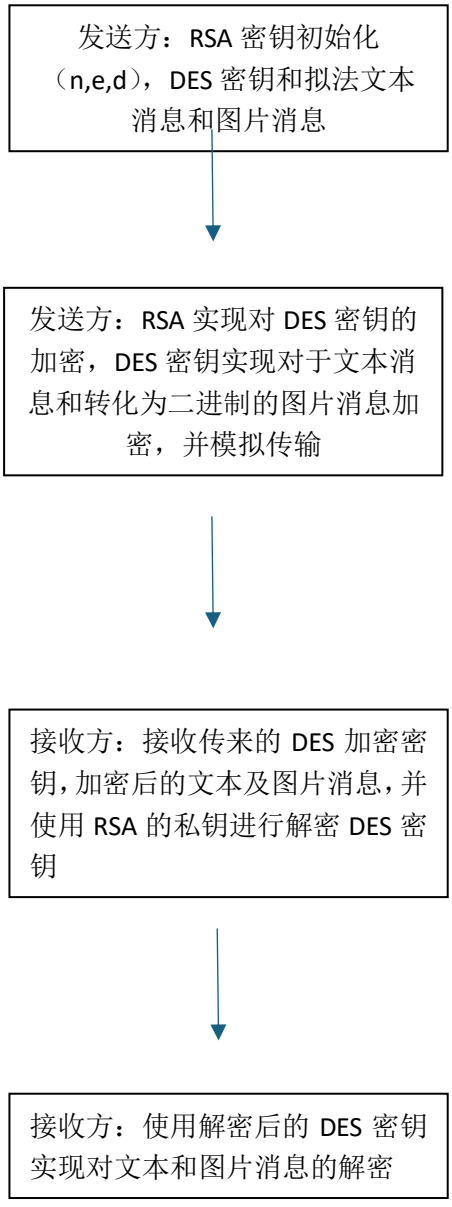
发送方：
RSA 密钥初始化（生成公钥和私钥）。
DES 密钥生成。

文本消息和图片消息的准备。

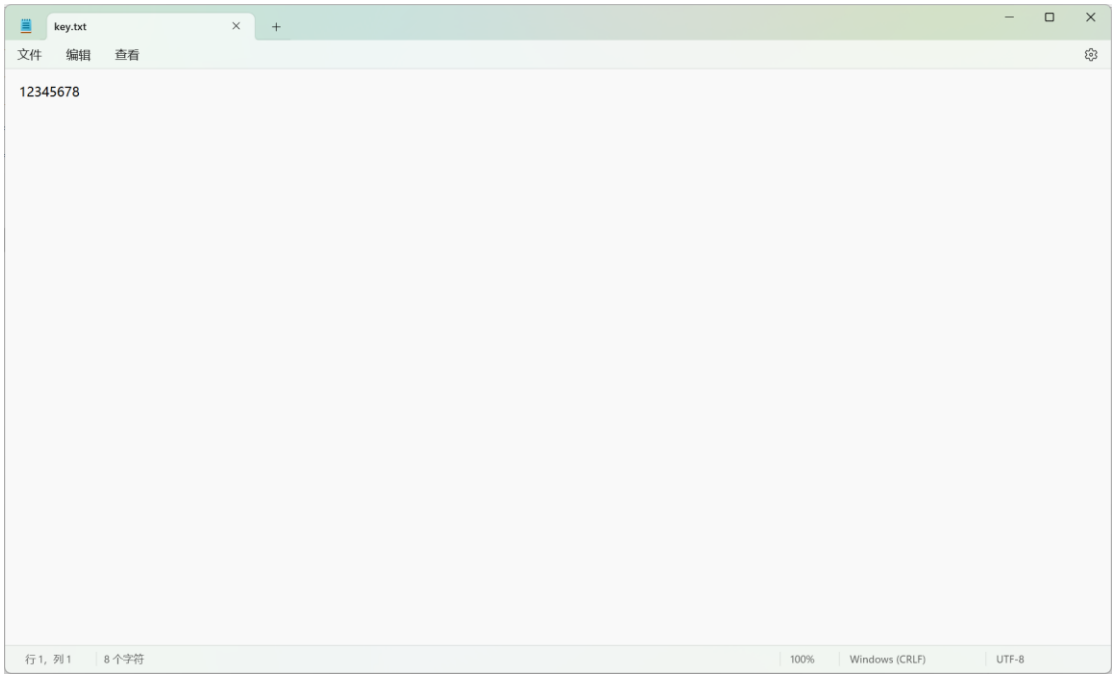
加密过程：
用 RSA 公钥加密 DES 密钥。
用 DES 密钥加密文本消息和图片消息。
模拟传输加密后的 DES 密钥和加密的消息。

接收方：
接收并用 RSA 私钥解密 DES 密钥。
用解密后的 DES 密钥解密文本消息和图片消息。

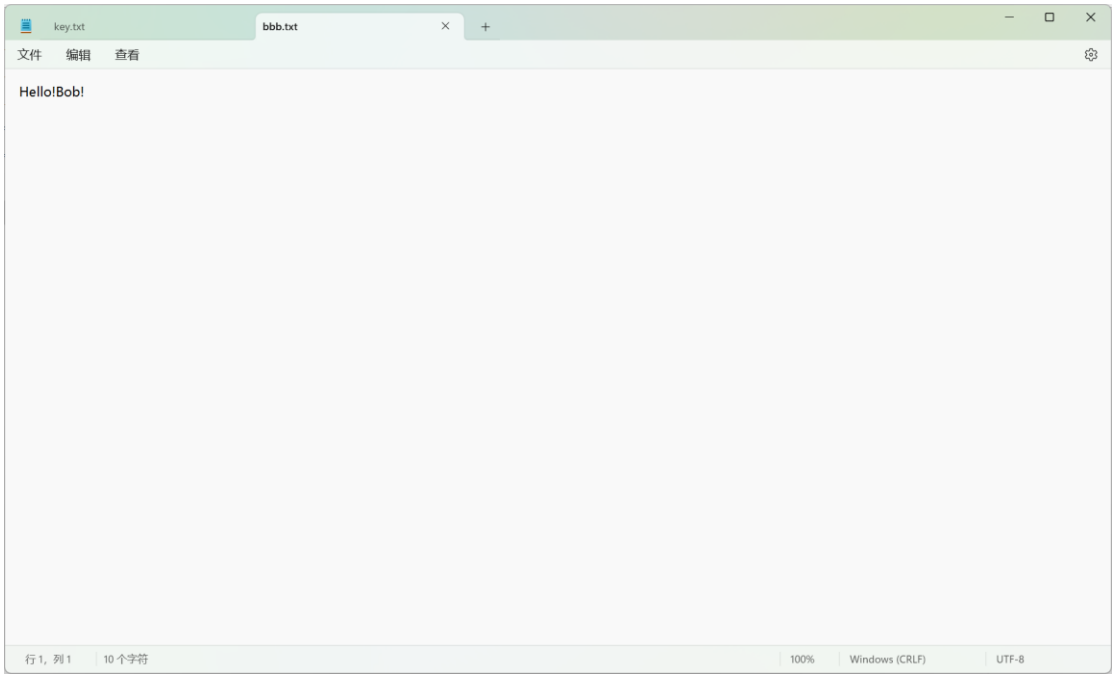
软件基本流程如下：



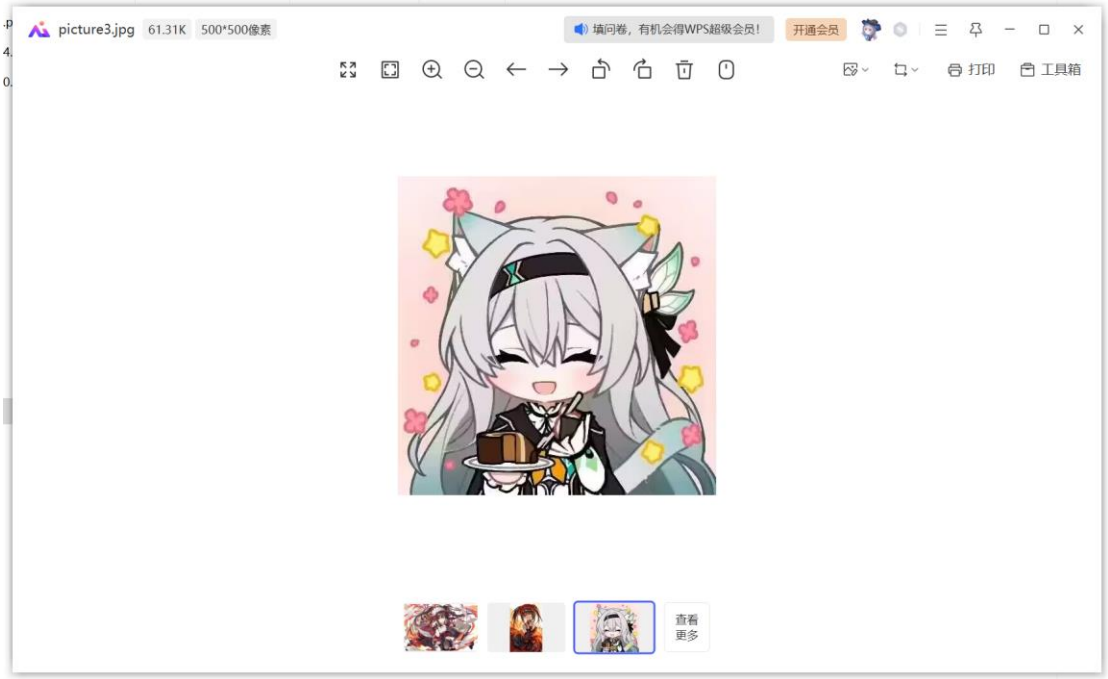
2.2 运行结果



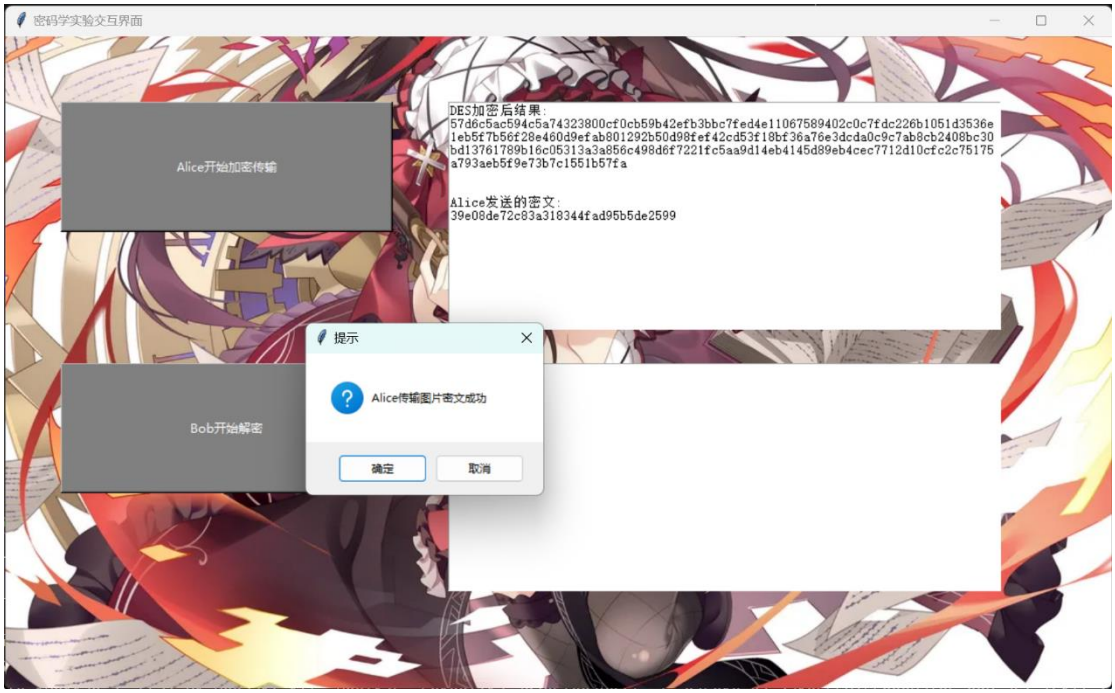
上图为需传输的 DES 密钥



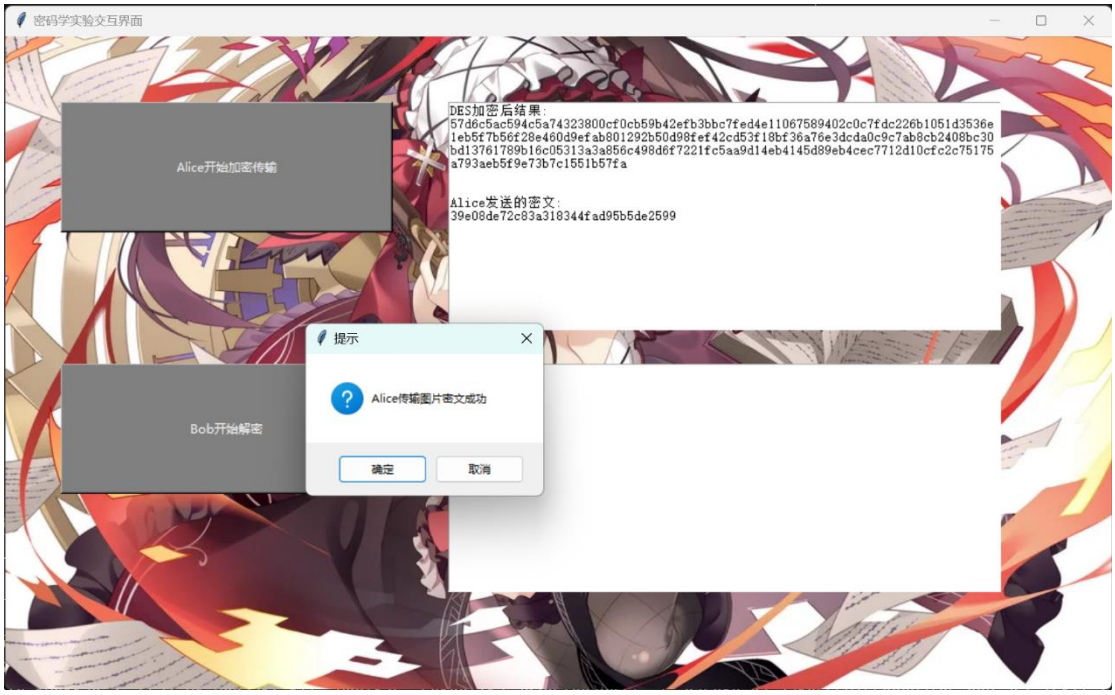
上图为文本消息



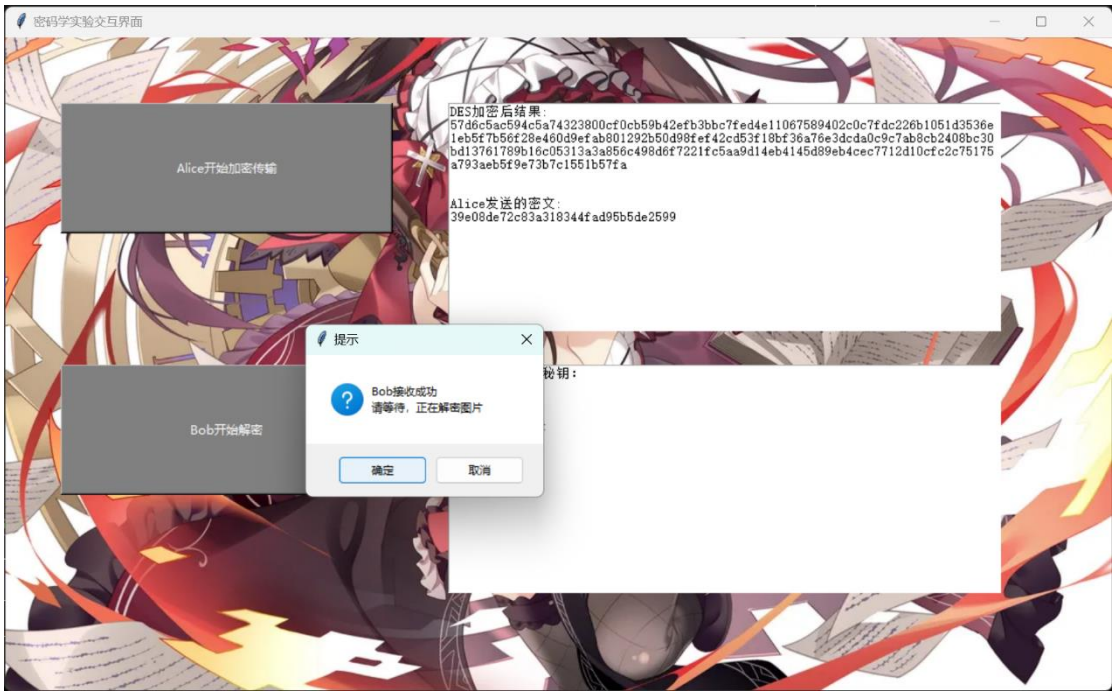
上图为图片消息



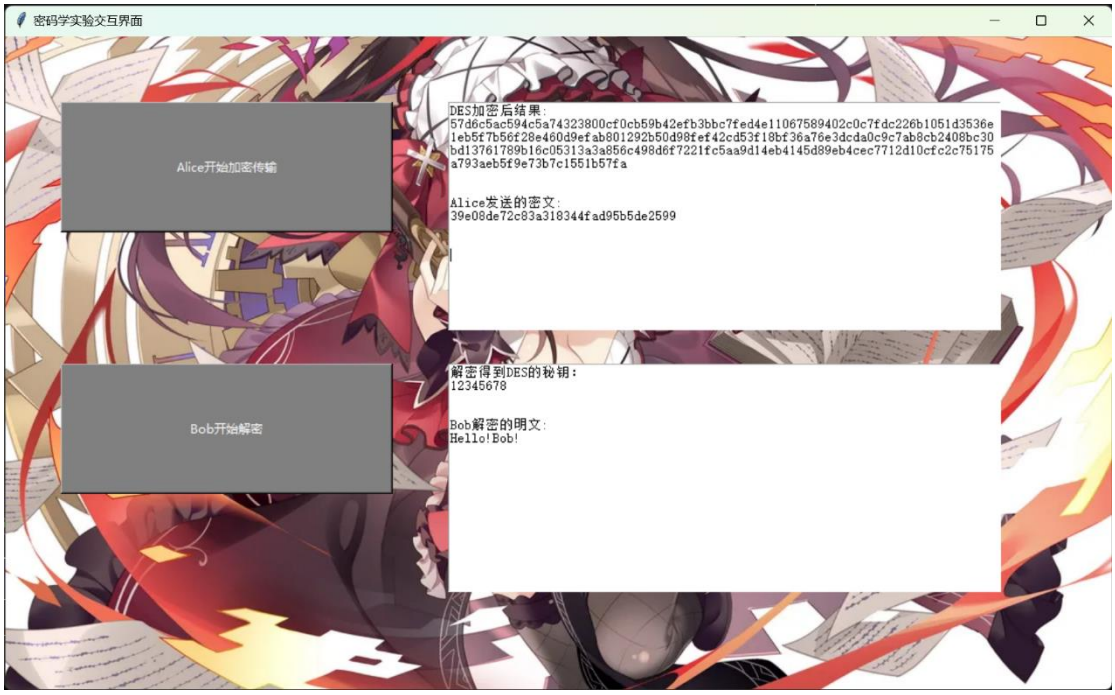
上图模拟发送方的操作过程，即实现了 DES 密钥的加密和对文本、图片消息的加密

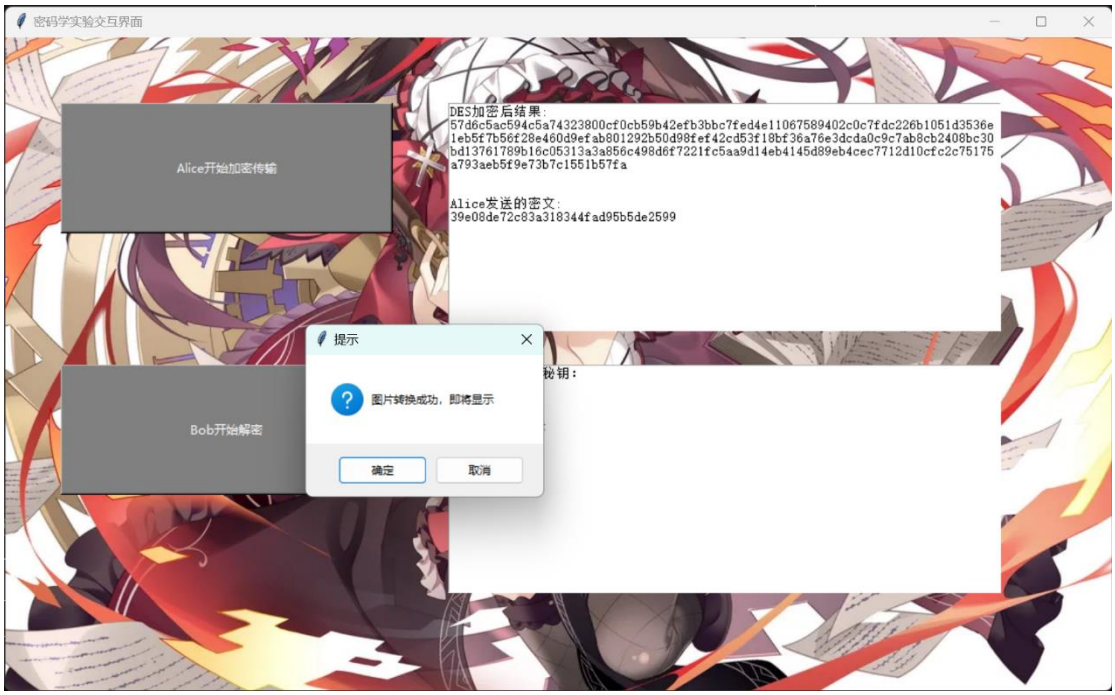


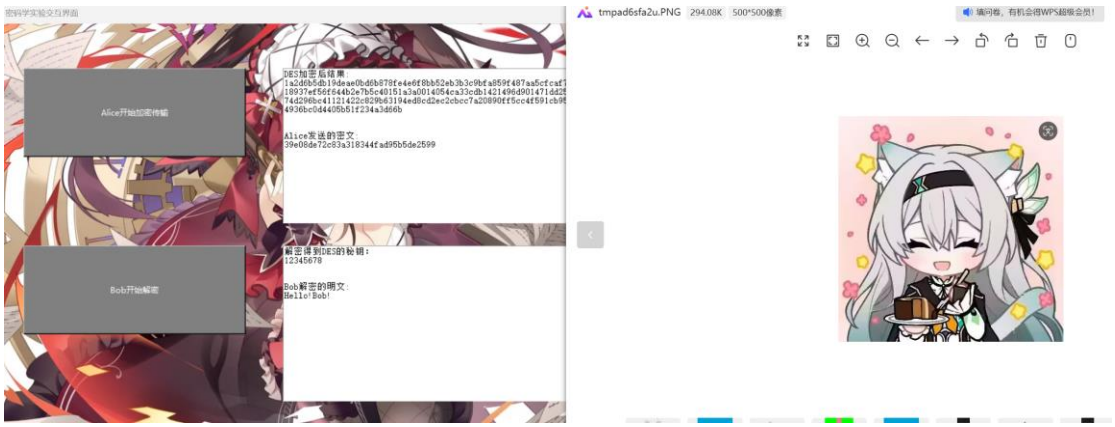
上图模拟发送方的传输过程



上图模拟接收方的接收过程，即实现 DES 密钥的解密和加密后的文本、图片消息的解密


密码学实验交互界面
Alice开始加密传输
Bob开始解密
DES加密后结果:
57d6c5ac594c5a74323800cf0cb59b42efb3bbc7fed4e11067589402c0c7fdc226b1051d3536e
1eb5f7b56f28e460d9efab801292b50d98fef42cd53f18bf36a76e3dcda0c9c7ab8cb2408bc30
bd13761789b16c05313a3a856c498d6f7221fc5aa9d14eb4145d89eb4cec7712d10cfc2c75175
a793aeb5f9e73b7c1551b57fa
Alice发送的密文:
39e08de72c83a318344fad95b5de2599
解密得到DES的秘钥:
12345678
Bob解密的明文:
Hello!Bob!


密码学实验交互界面
Alice开始加密传输
Bob开始解密
DES加密后结果:
57d6c5ac594c5a74323800cf0cb59b42efb3bbc7fed4e11067589402c0c7fdc226b1051d3536e
1eb5f7b56f28e460d9efab801292b50d98fef42cd53f18bf36a76e3dcda0c9c7ab8cb2408bc30
bd13761789b16c05313a3a856c498d6f7221fc5aa9d14eb4145d89eb4cec7712d10cfc2c75175
a793aeb5f9e73b7c1551b57fa
Alice发送的密文:
39e08de72c83a318344fad95b5de2599
提示
图片转换成功，即将显示
确定
取消
秘钥:



以上图片展示接收方的结果

3. 系统测试与结果

测试环境：
硬件：Inter Core i7 13700H，16GB
软件：Windows 11， Python 3.12， Pycharm2023

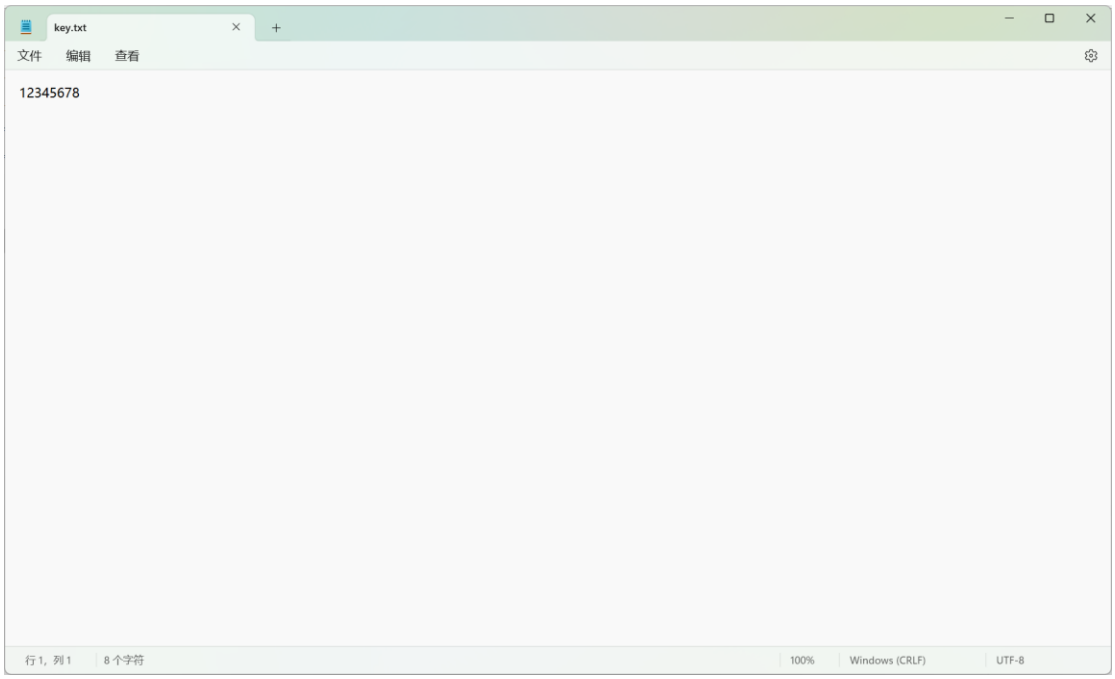
3.1 测试方案

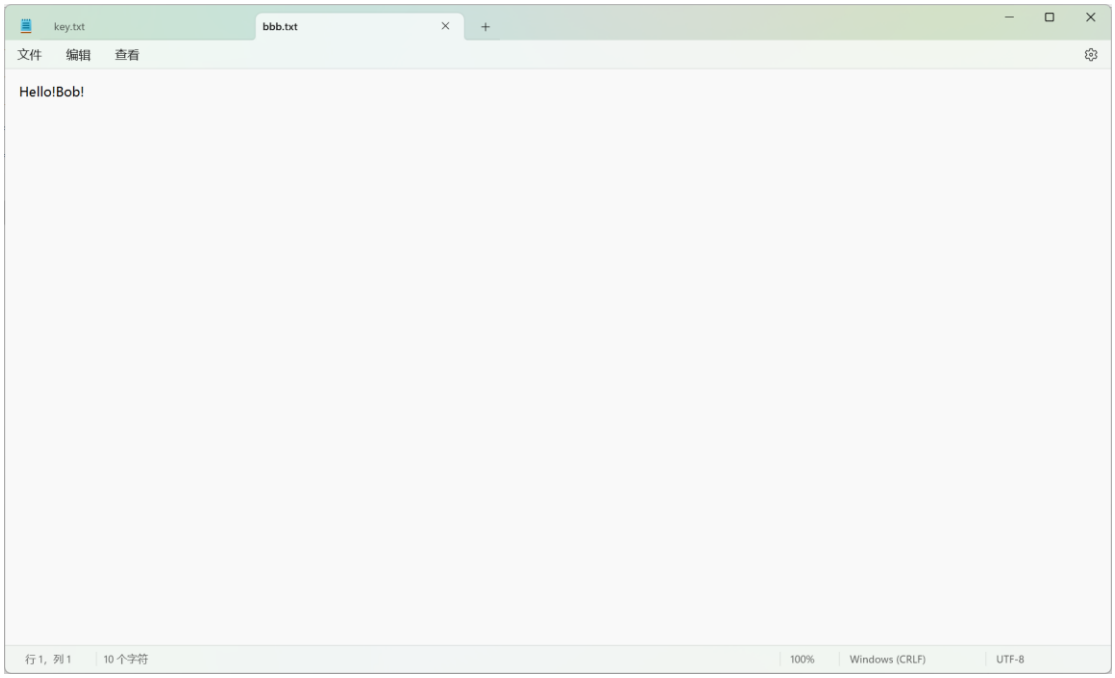
功能测试：
测试 RSA 和 DES 的加密解密功能。
验证消息传输的完整性和正确性。

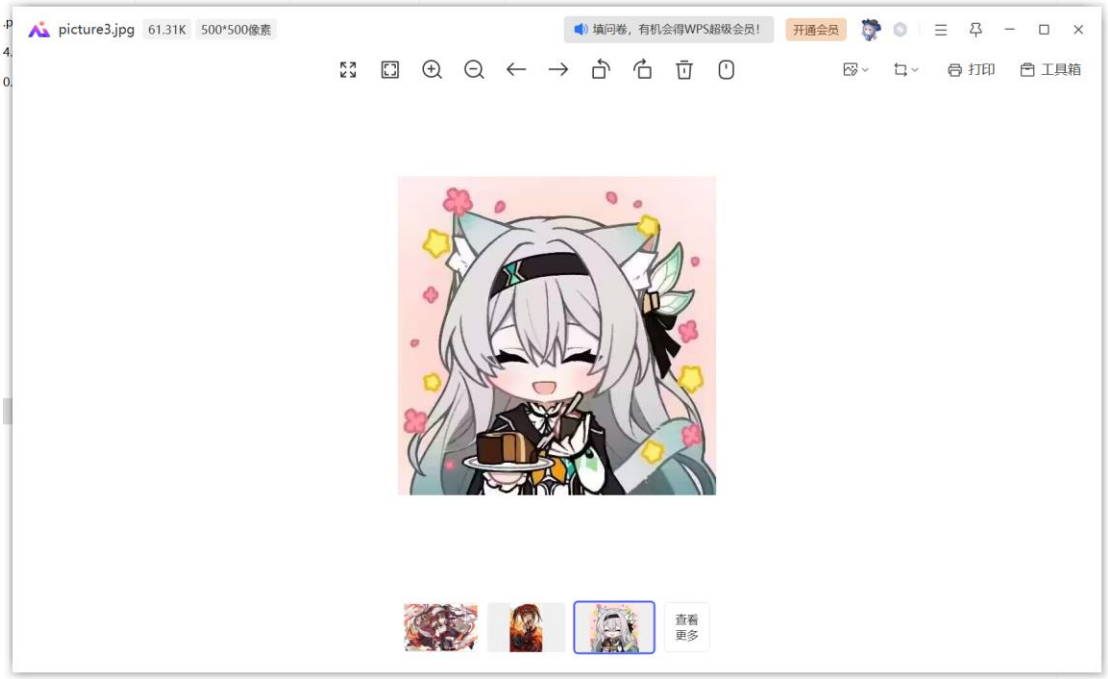
性能测试：
采用 python 的 time 库函数。
测试加密解密的时间和资源消耗。
使用不同大小的消息进行测试。

3.2 功能测试

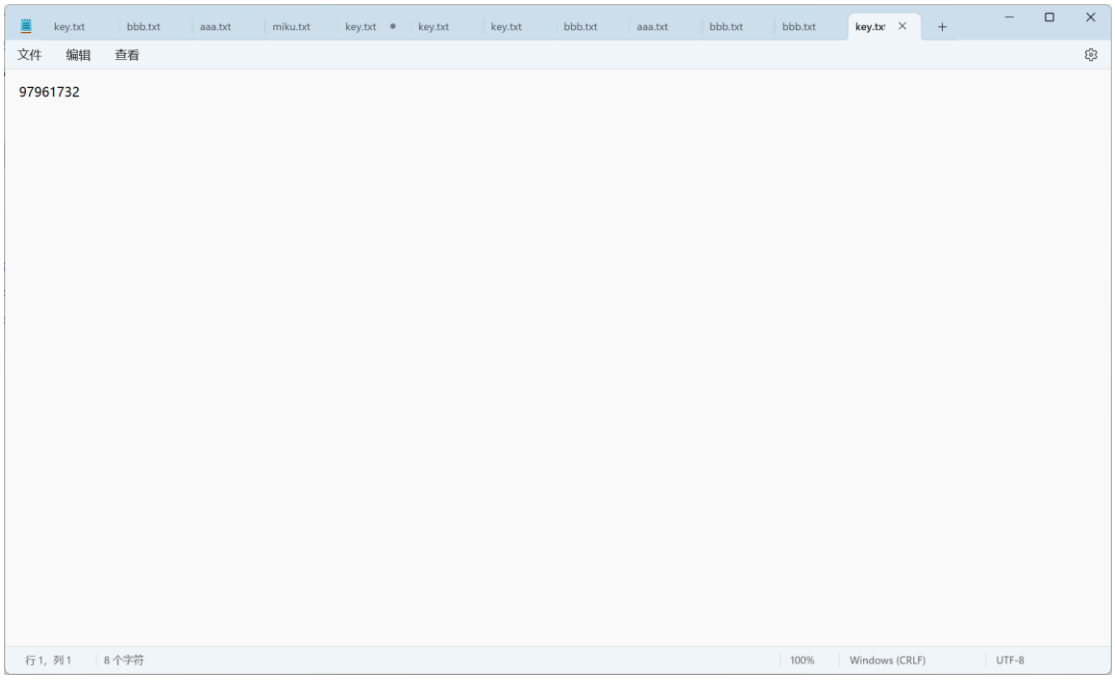
输入三个不同 DES 密钥、文本和图片消息，并测试解密结果的正确性
1.

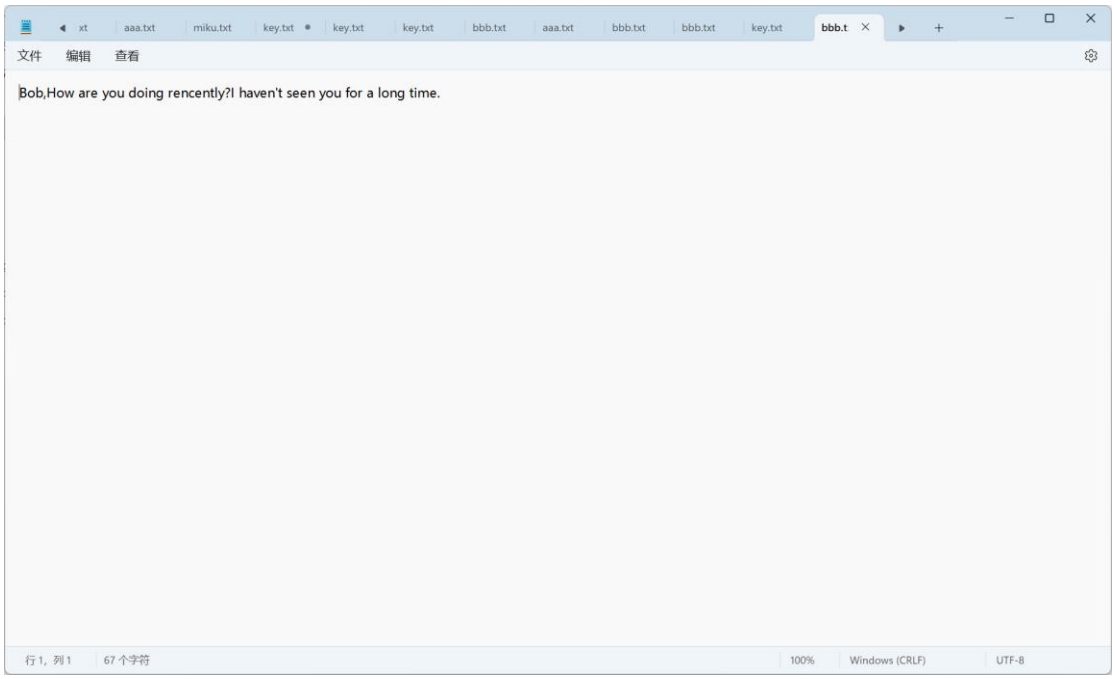

key.txt
文件 编辑 查看
12345678
行 1，列 1
8 个字符
100%
Windows (CRLF)
UTF-8

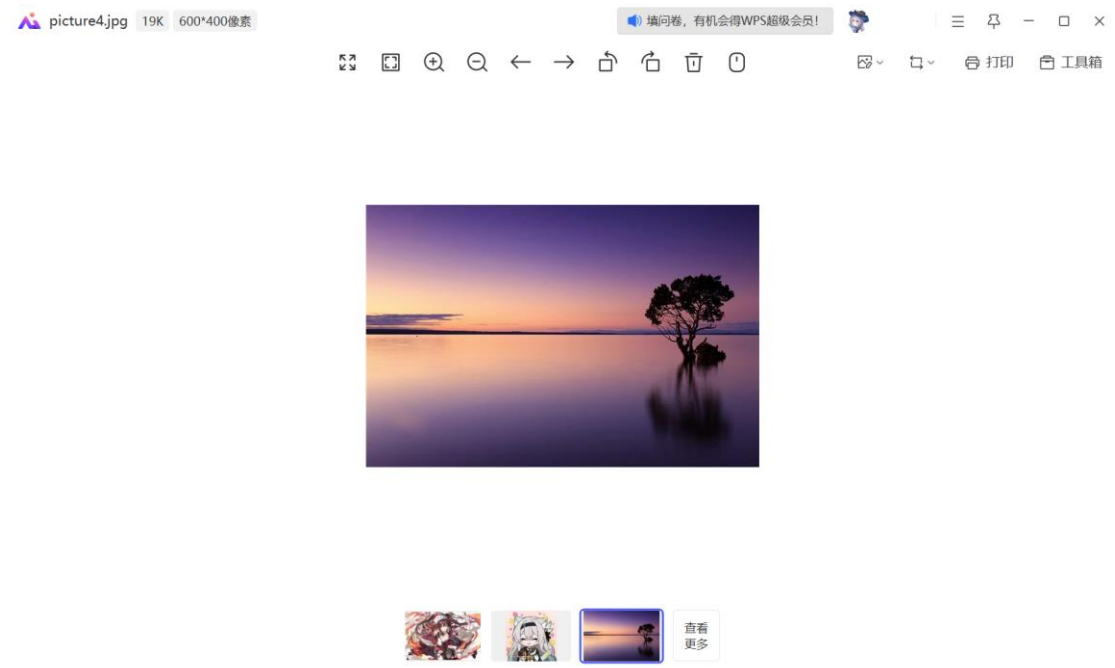

key.txt
bbb.txt
文件 编辑 查看
Hello!Bob!
行 1，列 1
10 个字符
100%
Windows (CRLF)
UTF-8


picture3.jpg 61.31K 500*500像素
填问卷，有机会得WPS超级会员！
开通会员
打印
工具箱
查看
更多

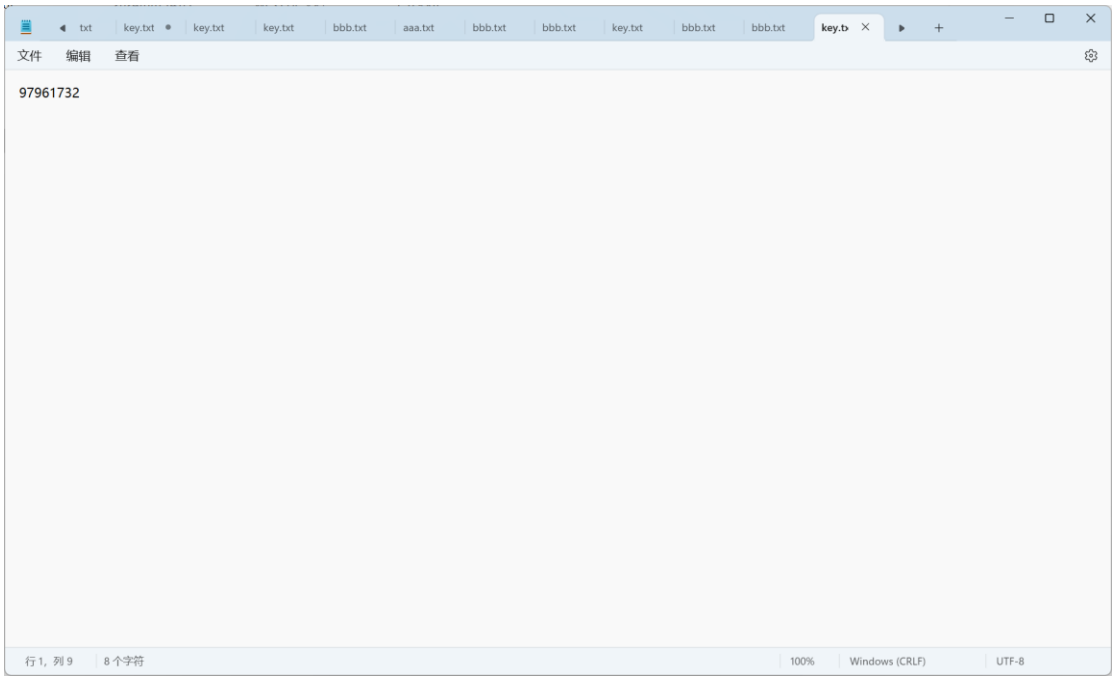
2.

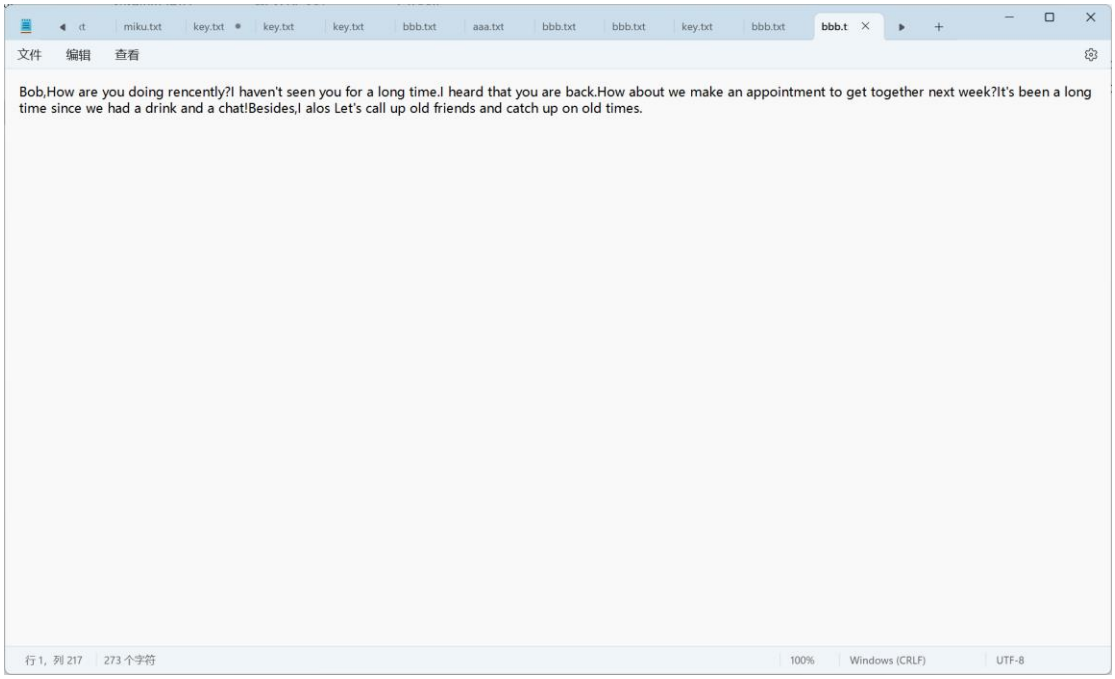

key.txt
bbb.txt
aaa.txt
miku.txt
key.txt
key.txt
key.txt
bbb.txt
aaa.txt
bbb.txt
bbb.txt
key.txt
文件
编辑
查看
97961732
行 1，列 1
8 个字符
100%
Windows (CRLF)
UTF-8


xt
aaa.txt
miku.txt
key.txt
key.txt
key.txt
bbb.txt
aaa.txt
bbb.txt
bbb.txt
key.txt
bbb.t
文件
编辑
查看
Bob,How are you doing rencently?I haven't seen you for a long time.
行 1，列 1
67 个字符
100%
Windows (CRLF)
UTF-8


picture4.jpg
19K
600*400像素
填问卷，有机会得WPS超级会员！
打印
工具箱
查看
更多

3.


key.txt
key.txt
key.txt
bbb.txt
aaa.txt
bbb.txt
bbb.txt
key.txt
bbb.txt
bbb.txt
key.t
文件
编辑
查看
97961732
行 1，列 9
8 个字符
100%
Windows (CRLF)
UTF-8


miku.txt
key.txt
key.txt
key.txt
bbb.txt
aaa.txt
bbb.txt
bbb.txt
key.txt
bbb.txt
bbb.t
文件
编辑
查看
Bob,How are you doing rencently?I haven't seen you for a long time.I heard that you are back.How about we make an appointment to get together next week?It's been a long time since we had a drink and a chat!Besides,I alos Let's call up old friends and catch up on old times.
行 1，列 217
273 个字符
100%
Windows (CRLF)
UTF-8

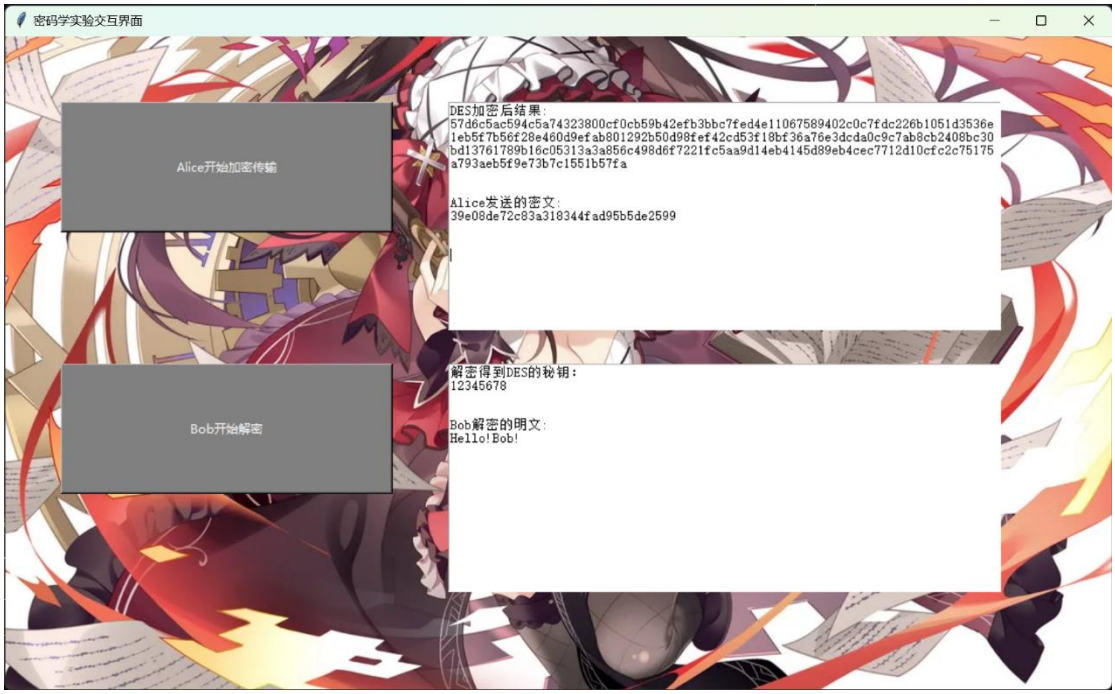
3.3 性能测试

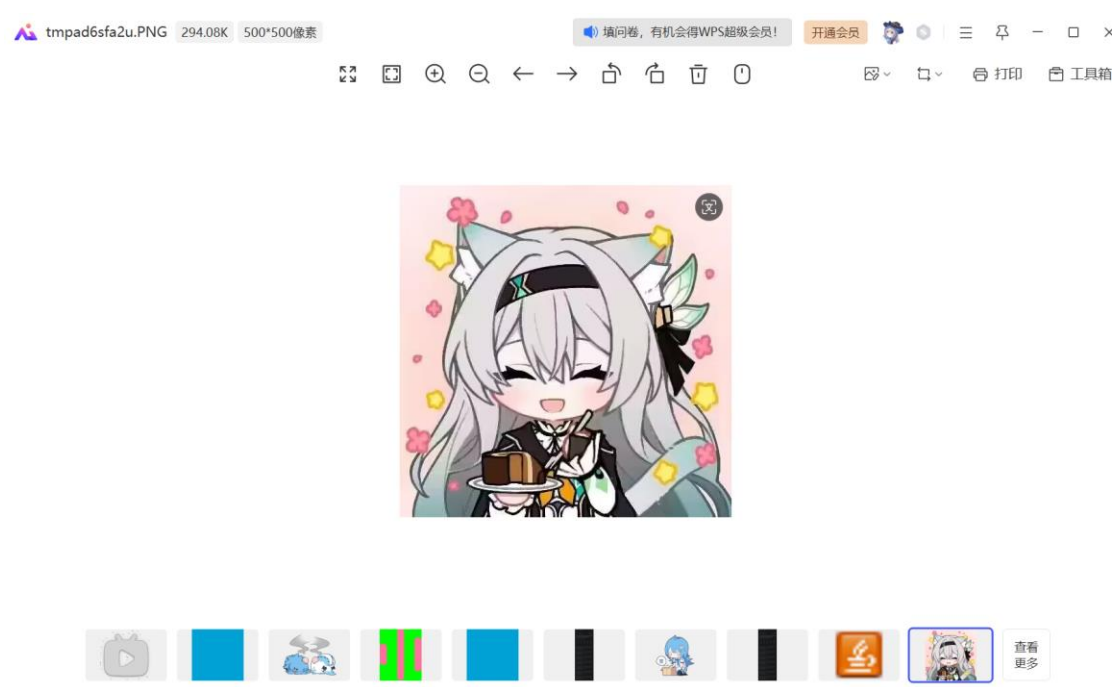
时间复杂度分析：
RSA 加密和解密的时间复杂度主要由大整数的幂模运算决定，通常为 $O(n^3)$
DES 的时间复杂度为线性，即$O(n)$，其中 n 为数据块的大小。

DES 密钥：12345678
文本和消息大小为：63KB

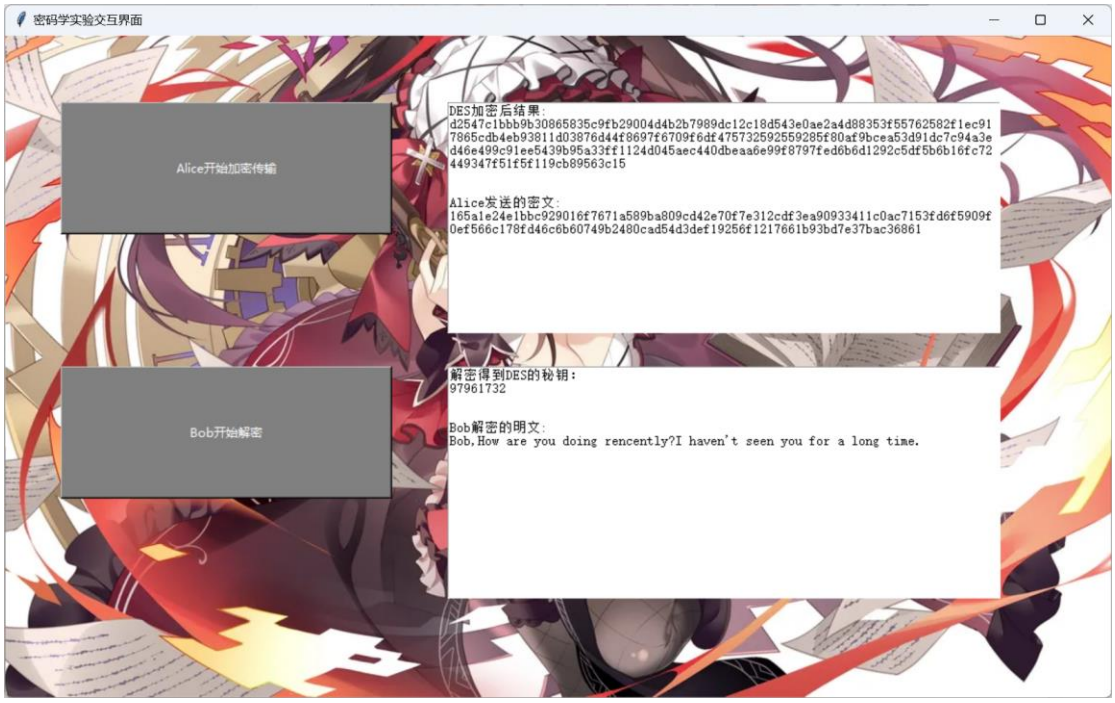
3.4 测试数据与结果

功能测试：
1.


密码学实验交互界面
Alice开始加密传输
Bob开始解密
DES加密后结果:
57d6c5ac594c5a74323800cf0cb59b42efb3bbc7fed4e11067589402c0c7fdc226b1051d3536e
1eb5f7b56f28e460d9efab801292b50d98fef42cd53f18bf36a76e3dcda0c9c7ab8cb2408bc30
bd13761789b16c05313a3a856c498d6f7221fc5aa9d14eb4145d89eb4cec7712d10cfc2c75175
a793aeb5f9e73b7c1551b57fa
Alice发送的密文:
39e08de72c83a318344fad95b5de2599
解密得到DES的秘钥:
12345678
Bob解密的明文:
Hello!Bob!


tmpad6sfa2u.PNG
294.08K
500*500像素
填问卷，有机会得WPS超级会员!
开通会员
打印
工具箱
查看更多

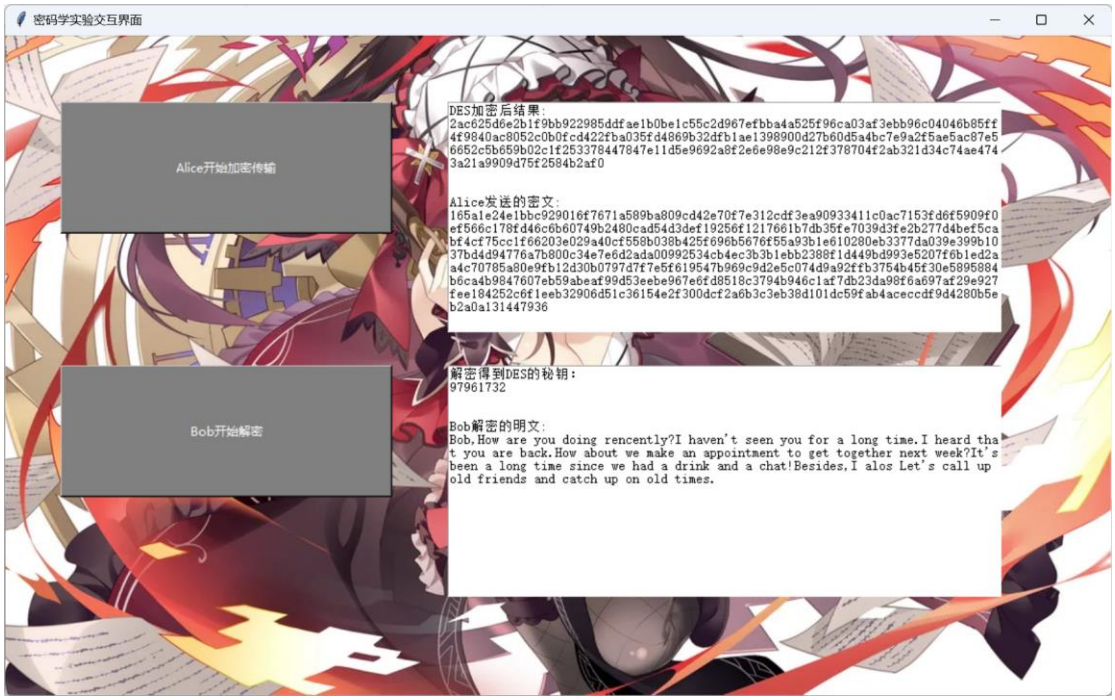
2.


密码学实验交互界面
Alice开始加密传输
Bob开始解密
DES加密后结果:
d2547c1bbb9b30865835c9fb29004d4b2b7989dc12c18d543e0ae2a4d88353f55762582f1ec91
7865cdb4eb93811d03876d44f8697f6709f6df475732592559285f80af9bcea53d91dc7c94a3e
d46e499c91ee5439b95a33ff1124d045aec440dbeaa6e99f8797fed6b6d1292c5df5b6b16fc72
449347f51f5f119cb89563c15
Alice发送的密文:
165a1e24e1bbc929016f7671a589ba809cd42e70f7e312cdf3ea90933411c0ac7153fd6f5909f
0ef566c178fd46c6b60749b2480cad54d3def19256f1217661b93bd7e37bac36861
解密得到DES的秘钥:
97961732
Bob解密的明文:
Bob,How are you doing rencently?I haven't seen you for a long time.


tmpbzy_dv55.PNG
155.72K
600*400像素
填问卷，有机会得WPS超级会员!
开通会员
打印
工具箱


查看
更多

3.



性能测试：
DES 密钥加密花费时间：0.01100 秒
文本和图片消息加密花费时间：22.1984 秒
DES 密钥解密花费时间：0.02000 秒
文本和图片消息解密花费时间：19.0050 秒
根据结果，花费时间在合理范围之内

4. 应用前景

本作品将 RSA 和 DES 算法相结合来实现消息之间的传输，这种混合密码的思路有助于提高消息传输的安全性和消息传输的效率，将 RSA 和 DES 结合使用的混合加密方式，可以在确保安全性的同时提高传输效率。这种方式适用于各种需要高安全性和高效率的消息传输场景，如金融交易、军事通信等。

5. 结论

本作品实现了 RSA 和 DES 混合加密，用于安全的密钥和消息传输。测试结果表明，该方法能够有效提高系统的安全性和传输效率。未来可以进一步优化算法，提高加密解密速度，并探讨更多的应用场景。