输成本；高强度的公钥密码算法，复杂的密钥构成，提高试卷传输的机密性。

2.3 软件运行和系统要求

本系统运行在 PC 机上，使用 WINDOWS 操作系统，开发工具：Java，Eclipse。

CPU：Pentium 以上计算机 内存: 1G 以上。

操作系统版本：Windows XP /vista/Win7/Win10

三、系统使用

3.1 发送端与接收端会话密钥交换

首先是发送端产生随机变化会话密钥，用 RSA 算法进行加密，如图 3.1。

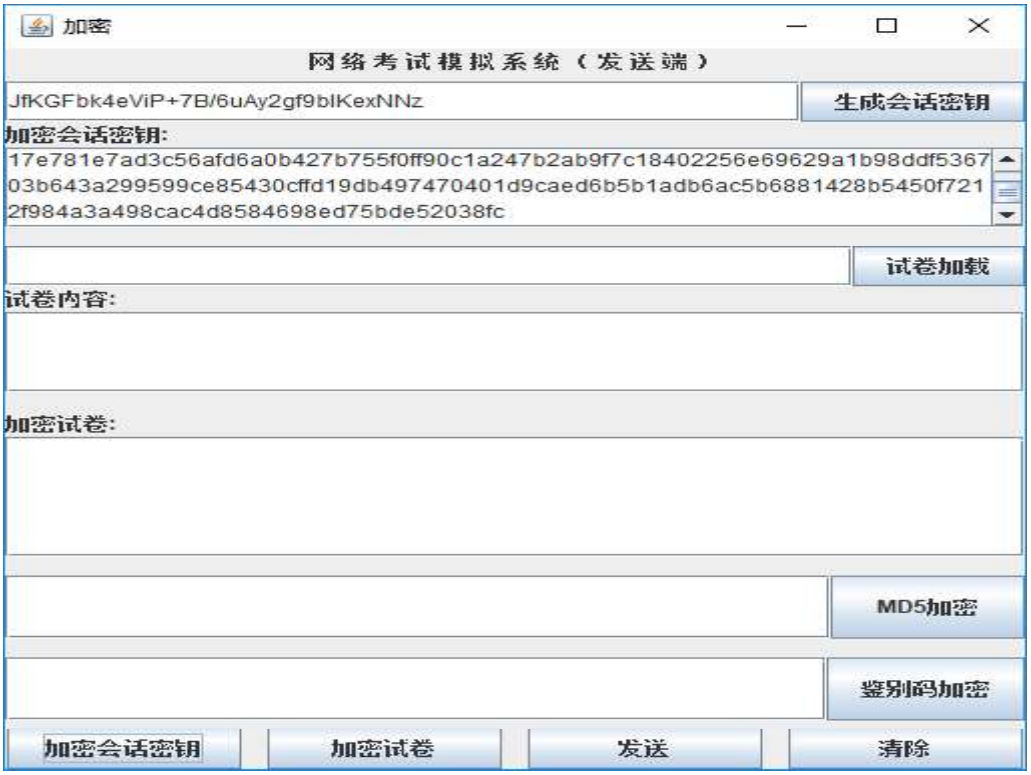

图 3.1 发送端加密会话密钥

然后是接收端收到会话密钥加密密文后进行解密获得会话密钥，如图 3.2。

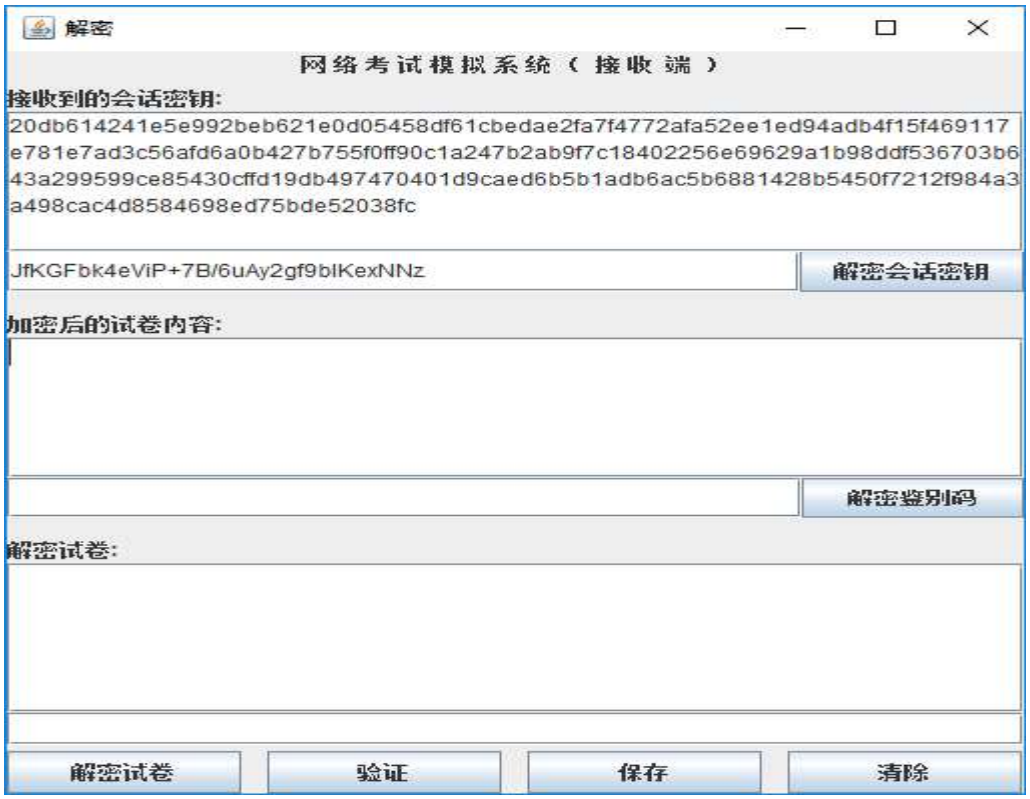

图 3.2 接收端解密会话密钥

3.2 发送端与接收端试卷传输

首先是发送端加载试卷获取试卷内容，并用会话密钥进行 DES 加密，同时对试卷进行 MD5 加密得到散列值 H，并对 H 用接收端公钥进行加密得到鉴别码，将鉴别码加在试卷密文前面得到扩展密文发送给接收端，如图 3.3 所示。

图 3.3 发送端试卷传输和鉴别码 H 加密

然后是接收端收到试卷加密密文并用会话密钥进行 DES 解密，在这里我们一定要先进行会话密钥的解密才可以再对试卷密文进行解密，如果顺序相反，则系统出错停止运行，并且用接收端的公钥解密获得鉴别码 H，如图 3.4。

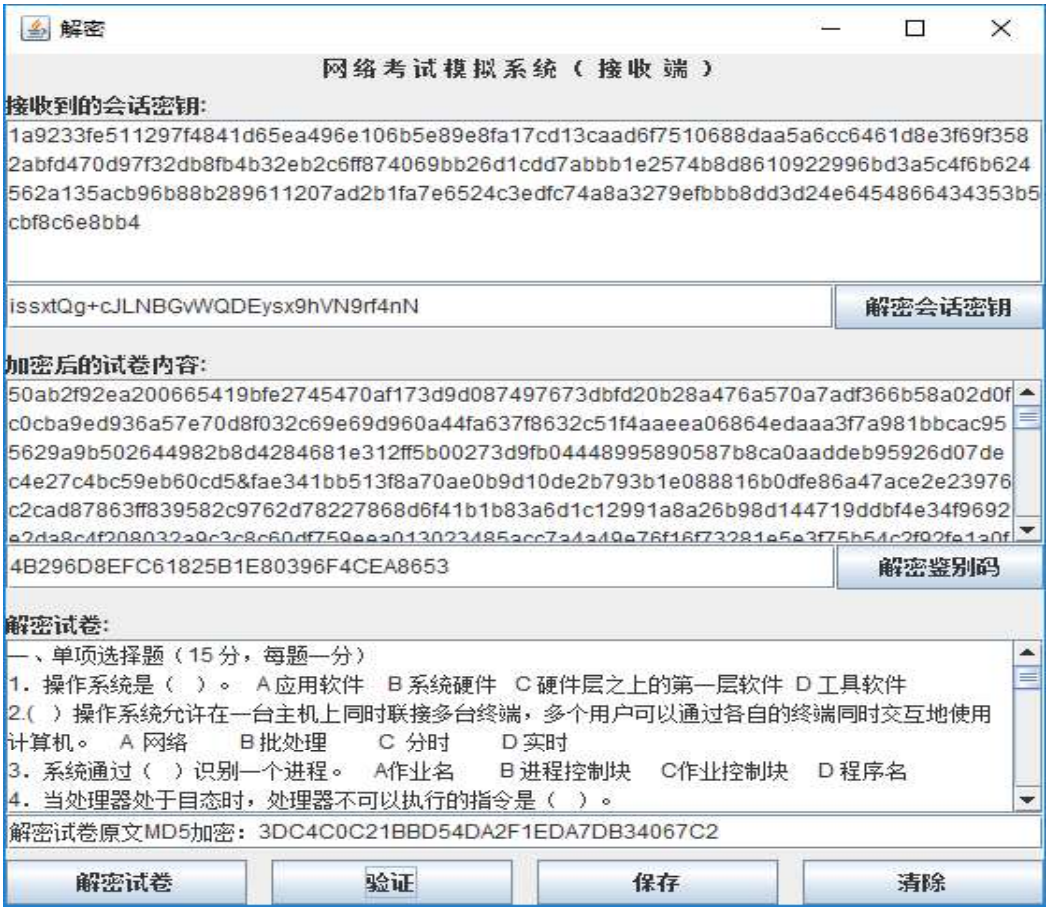

图 3.4 接收端解密试卷和鉴别码 H

3.3 接收端消息摘要验证并存储试卷

先是会话密钥的交换使用 RSA 算法，体现非对称加密；其次是试卷传输使用 DES 算法，体现对称加密；然后 RSA 解密得到 H 以及对试卷进行 MD5 运算得到 H(X)，将 H 和 H(X)进行比较验证；最后进行试卷保存，混合加密传输完成，如图 3.5；如图 3.6，H 与 H(X)比较得 H=H(X)，因此原文未修改；经过散列值比较原文未修改，则对文档进行保存，保存后再次比较两个文档的内容，是一样的，如图 3.7。

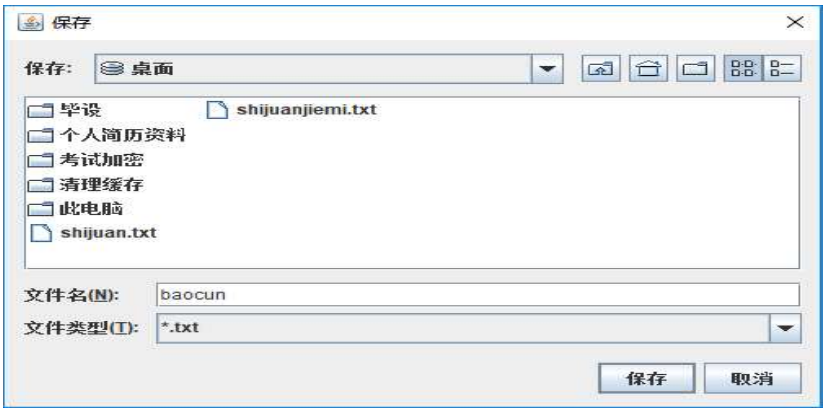

图 3.5 试卷保存

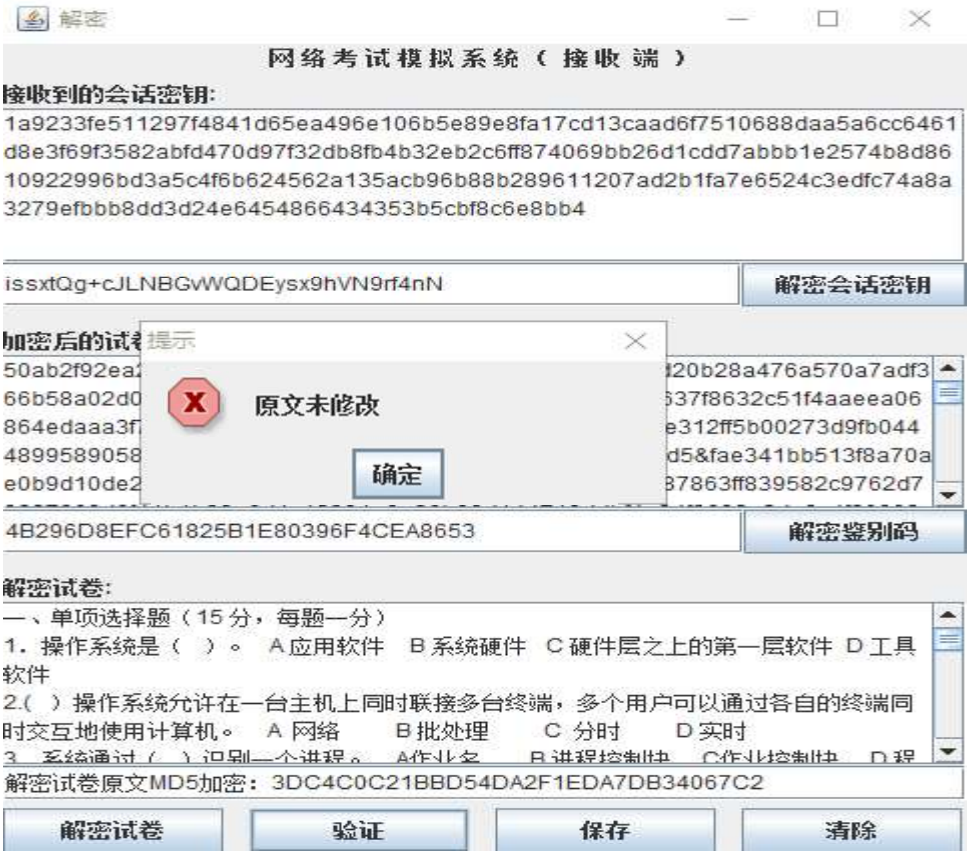

图 3.6 H 与 H(X)比较验证

图 3.7 试卷内容比较