

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。

加密

网络考试模拟系统（发送端）

JfKGFbk4eViP+7B/6uAy2gf9bIKexNNz

生成会话密钥

加密会话密钥:

17e781e7ad3c56afd6a0b427b755f0ff90c1a247b2ab9f7c18402256e69629a1b98ddf5367
03b643a299599ce85430cfd19db497470401d9caed6b5b1adb6ac5b6881428b5450f721
2f984a3a498cac4d8584698ed75bde52038fc

试卷加载

试卷内容:

加密试卷:

MD5加密

鉴别码加密

加密会话密钥 加密试卷 发送 清除

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。

网络考试模拟系统（发送端）	
issxtQg+cJLNBGWQDEysx9hVN9rf4nN	生成会话密钥
加密会话密钥:	
582abfd470d97f32db8fb4b32eb2c6ff874069bb26d1cdd7abbb1e2574b8d8610922996bd3a5c4f6 b624562a135acb96b88b289611207ad2b1fa7e6524c3edfc74a8a3279efbbb8dd3d24e64548664 34353b5cbf8c6e8bb4	
C:\Users\龙的哈士奇\Desktop\shijuan.txt	试卷加载
试卷内容:	
一、单项选择题（15 分，每题一分） 1. 操作系统是（ ）。 A 应用软件 B 系统硬件 C 硬件层之上的第一层软件 D 工具软件 2.（ ）操作系统允许在一台主机上同时联接多台终端，多个用户可以通过各自的终端同时交互地使用计算机。 A 网络操作系统 B 批处理操作系统 C 分时操作系统 D 实时操作系统	
加密试卷:	
fae341bb513f8a70ae0b9d10de2b793b1e088816b0dfe86a47ace2e23976c2cad87863ff839582c9 762d78227868d6f41b1b83a6d1c12991a8a26b98d144719ddb4e34f9692e2da8c4f208032a9c3c 8c60df759eea013023485acc7a4a49e76f16f73281e5e3f75b54c2f92fe1a0fef1de063c28385fc794 2e4d334d3ec141fa956d70e6c093e3dc8937d14b1c28e4beac30404ae6a5ddb6a4d49da9387a32 eb7a2940f37af617ab531b64f538054c3596a6554a6f9b4464e3c6b5760f22c5f4e92742d2ff82179	
4B296D8EFC61825B1E80396F4CEA8653	MD5加密
7a0f500b50a02d01c0c0a9e0930a37e70601032c09e09d900a44a03710032c311 4aaeea06864edaaa3f7a981bbcac955629a9b502644982b8d4284681e312ff5b 00273d9fb04448995890587b8ca0aaddeb95926d07dec4e27c4bc59eb60cd5	鉴别码加密
加密会话密钥	加密试卷
发送	清除

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。

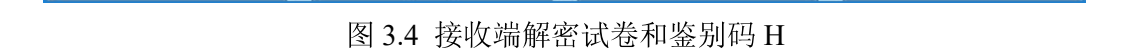


图 3.5 试卷保存

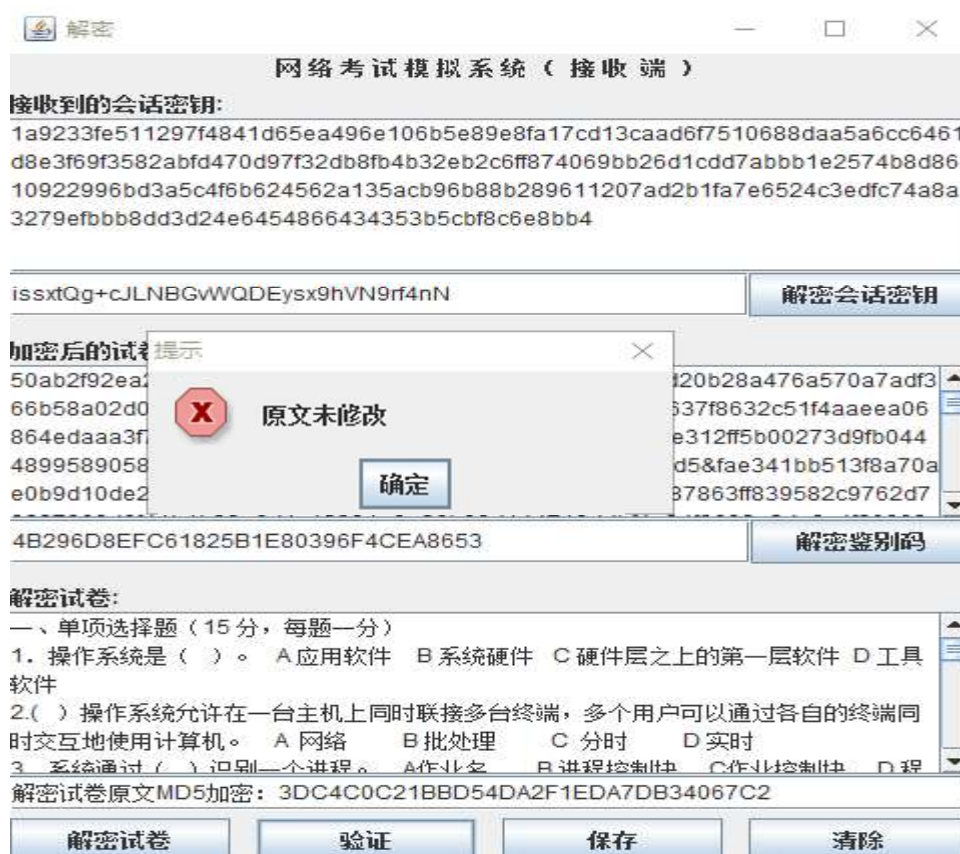


图 3.6 H 与 H(X)比较验证



图 3.7 试卷内容比较