加密与数字签名实验报告

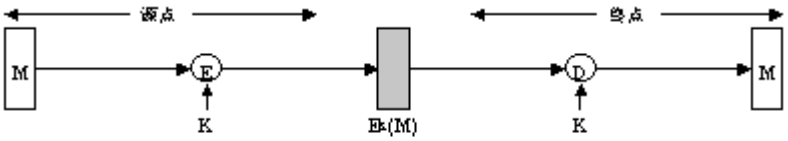
班级：　　学号：　　姓名：

一、实验名称

二、实验目的

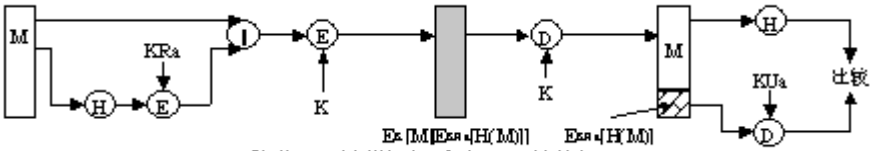
三、实验内容与要求

设计一个两个同学之间使用对称加密算法加密传送信息，验证数字签名方案



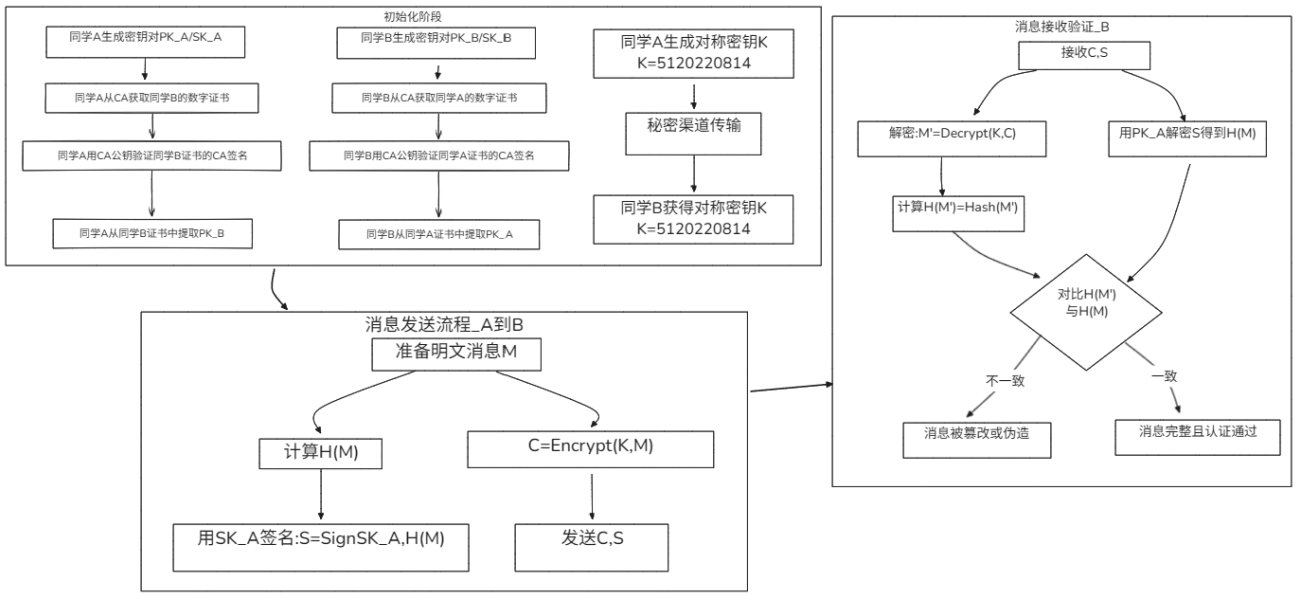
(a)常规加密：保密和认证

方案原理



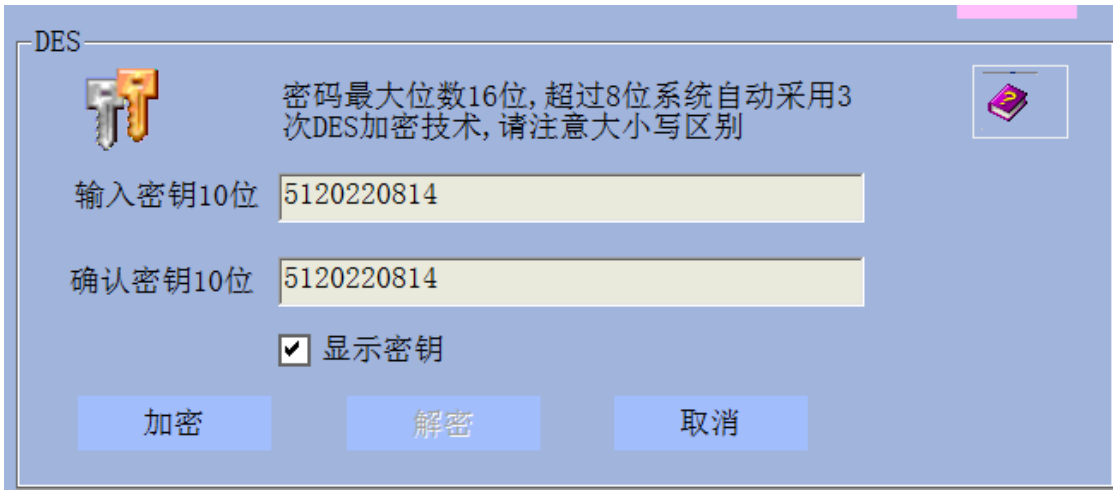
(d)散列及公开密钥加密：保密，认证和签名

框图：



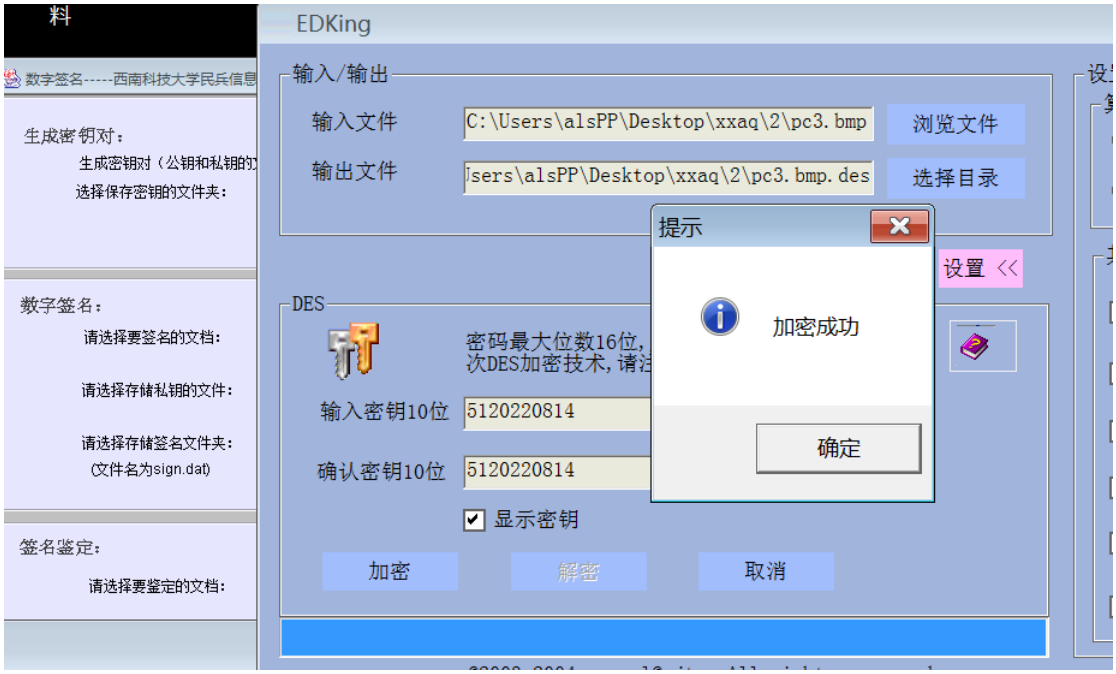
同学A和B分别在数字签名软件中生成各自的公私钥对(PK_A,SK_A,PK_B,SA_B)。

同学 A 使用 DES 对称加密算法软件生成对称密钥 K=5120220814



同学 A 使用自己的私钥 SK_A 对消息摘要 H (M) 进行数字签名，得到签名 S = SK_A (H (M))。

同学 A 使用对称密钥 K 对消息 M 进行对称加密，得到加密后的消息 C

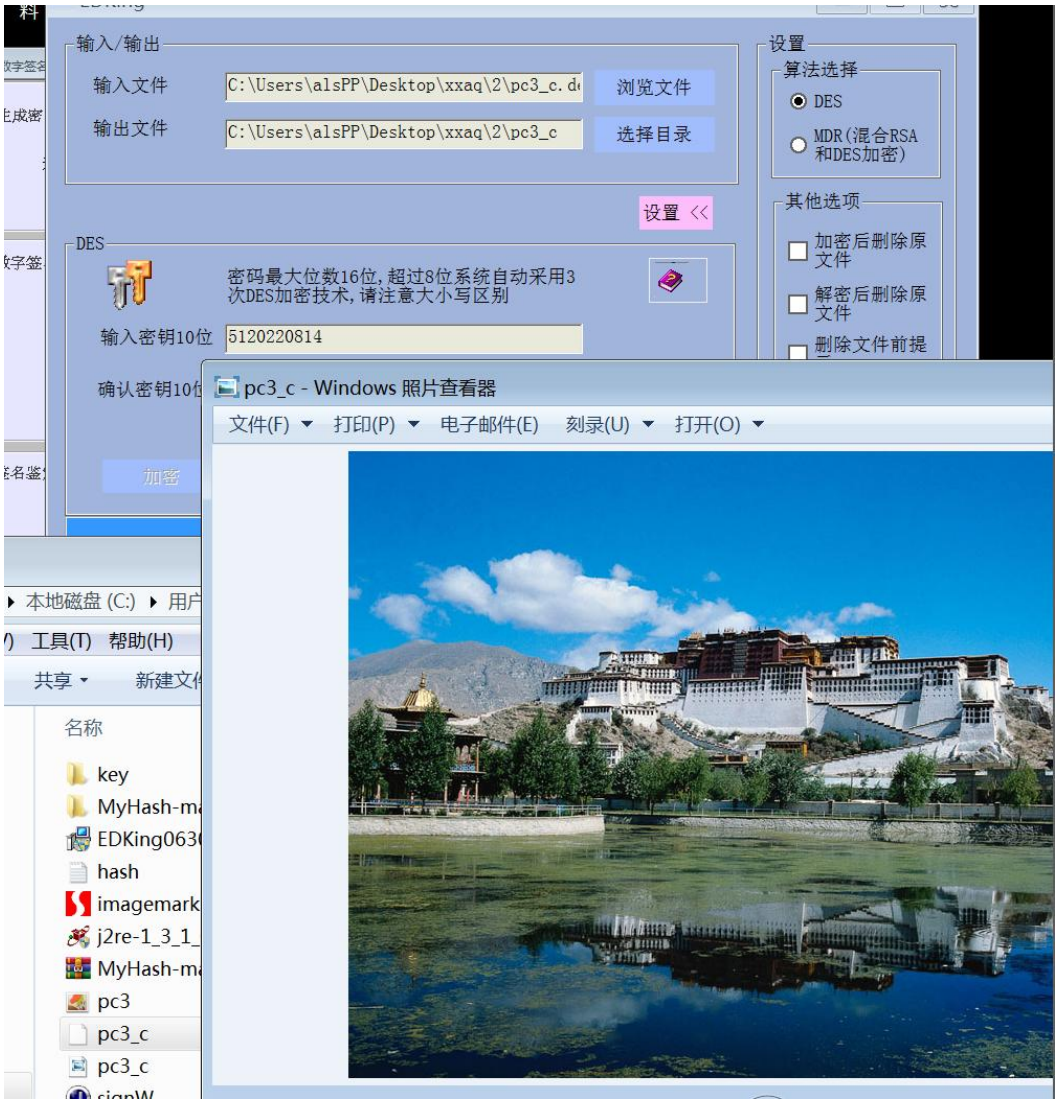


加密后消息不可见（明文）

同学 A 将加密信息 C、数字签名 S 发送给同学 B

同学 B 接收到同学 A 发送的加密消息 C、数字签名 S。

同学 B 使对称密钥 K 对加密消息 C 进行解密，得到原始消息 M' = D_K (C)，



同学 B 使用同学 A 的公钥 PK_A 对数字签名 S 进行验证，即计算 H (M')，并将其与用 PK_A 解密签名 S 得到的消息摘要 H（M）进行对比。

若两者一致，则验证数字签名成功，说明消息来自同学 A 且未被篡改；

若不一致，则说明消息可能被篡改或并非来自同学 A。

四、实验过程

实验的详细步骤，过程

五、实验结果分析

六、思考与心得体会