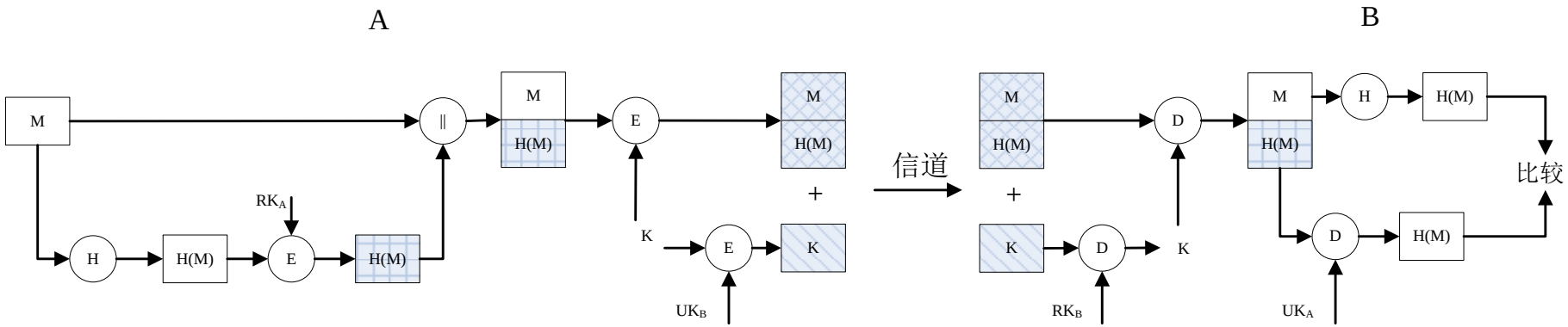
大作业



说明：（1）M 表示明文，H 表示 Hash 函数，E 表示加密算法，D 表示解密算法，RK_A 表示发送方 A 的私钥，UK_A 表示发送方 A 的公钥，RK_B 表示发送方 B 的私钥，UK_B 表示发送方 B 的公钥，||表示组合。

（2）阴影部分表示加密后的结果。

要求：（1）对称加密算法包含 DES 和 AES，在程序中可选；密钥可选或根据种子产生；

（2）Hash 算法包含 SHA 和 MD5，在程序中可选；

（3）非对称加密算法 RSA，程序中能够产生不同的私钥和公钥对；密钥长度不得小于 200 位；

（4）图示过程在一个程序中完成；

（5）采用 eclipse 4.8M5 或 visual studio2012 平台开发；

（6）需要有可视化界面；提交的程序包括源码和编译后的可执行文件（release 版本）

时间：课程上完之后，考试之前，每位同学提交源码和编译后的可执行代码（发布版）。