作业六

题目：安全目标：用户 A 想利用互联网安全传输一个重要且很大(譬如 500M)的文件 m 给用户 B。

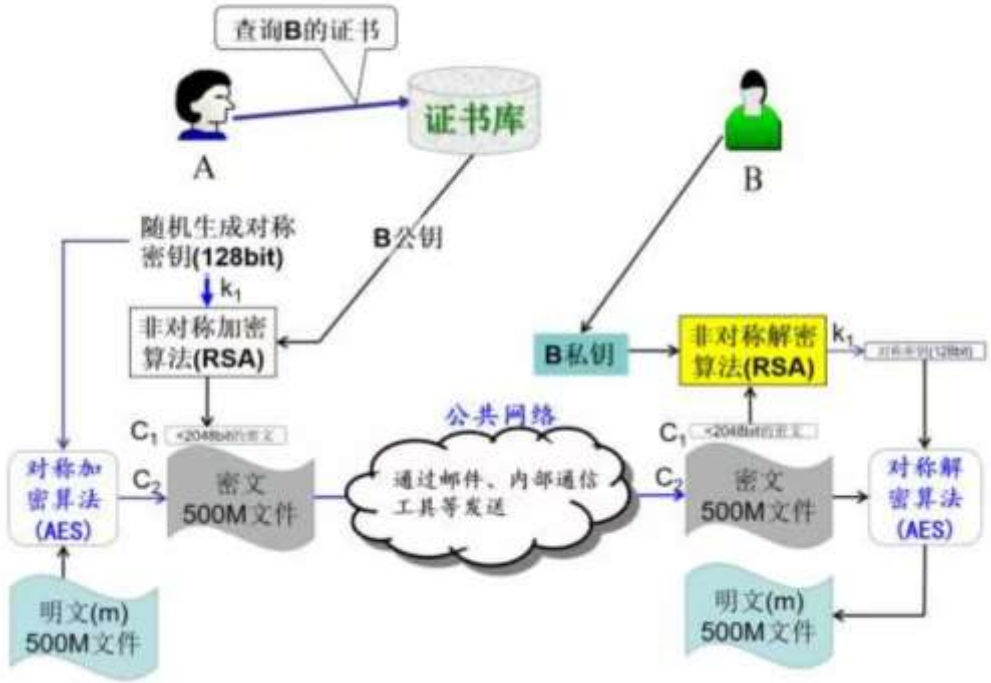
前提条件：用户 A 可以通过可信中心获得用户 B 的公钥证书。(提示:当然 B 拥有自己的私钥)

请回答一下问题：

1. **设计一个方案实现上述目标。**
2. **在上述目标中，如果增加了保证文件完整性的要求，那么上面方案需要增加那些改进。**
3. **用户 A 和 B 完成上述目标后，过了一段时间，又有另一个重要且很大的文件(譬如 200M)需要用户 A 安全发送给用户 B，为完成这个任务，接下来用户 A 和 B 需要如何做才能即满足安全需求又具有较高的效率?请写出具体步骤。**

答:

1. 方案如下图所示:



(1) 用户 A 向 CA 中心的证书库获取 B 的证书，验证证书的有效性，从证书中获取 B 的公钥。

（2） 用户 A 随机生成一个密钥 K_1(128 比特)，以 B 的公钥作为密钥使用非对称密码算法(例如 RSA)加密该密钥，生成密文 C_1。

（3） 以 K_1 作为密钥使用对称密码算法(例如 AES)加密大文件 m，生成密文 C_2。

（4） 用户 A 通过邮件或内部通信工具发送 C_1 和 C_2 到用户 B。

（5） 用户 B 以 B 的私钥作为密钥使用非对称密码算法(例如 RSA)解密 C_1，得到 K_1。

（6） 以 K_1 作为密钥使用对称密码算法(例如 AES)解密 C_2，得到大文件 m。

2. 改进方法：增加消息验证码（MAC）

在上述方案中，第（2）步修改为:随机生成密钥 K_1 和 K_2(均为 128 比特)，以 B 的公钥作为密钥使用非对称密码算法(譬如 RSA)加密 K_1 和 K_2 生成密文 C_1 和计算 C_3=MAC (m,K_2)。第（4）步中也传送 C_3 到用户 B。第（5）步中得到 K_1 和 K_2。第（6）步中计算 C_4=MAC(m,K_2)，如果 C_4=C_3，认证成功(保证文件的完整性)，否则，认证失败(不保证文件的完整性)。

注：根据密钥管理原则的责任分离原则，要产生一个新的密钥（K_2）用于 MAC。

3. 密钥要时常更新，不同的任务要采用不同的密钥

新的文件要传输，就要使用新的密钥加密文件，要高效生成密钥，就要在已有密钥(这密钥是安全的)基础上生成。方案很多(例如利用公钥密码技术实现密钥分发)，下面举例利用原有密钥实现密钥更新。

用户 A 和 B 利用已都掌握的 K_1 来生成，例如 K_2=Hash(K_1)，Hash 指哈希函数，K_2 作为新密钥。

好处：向 A、B 双方发布密钥更新通知，就可各自生成新密钥，效率高。由于原密钥是安全的，新生成的密钥也是安全的。由于 Hash 函数的单向性，即使新密钥泄露，也不影响原密钥的安全。