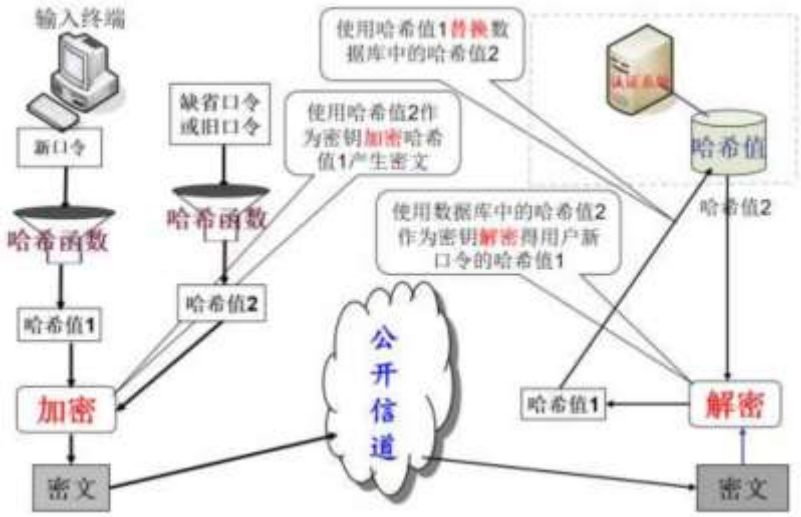
作业五

题目：在一个广域网的应用环境，用户使用用户名和口令的方式登录远程服务器，服务器管理员给每个用户设置一个初始口令，请利用哈希函教实现以下安全功能：

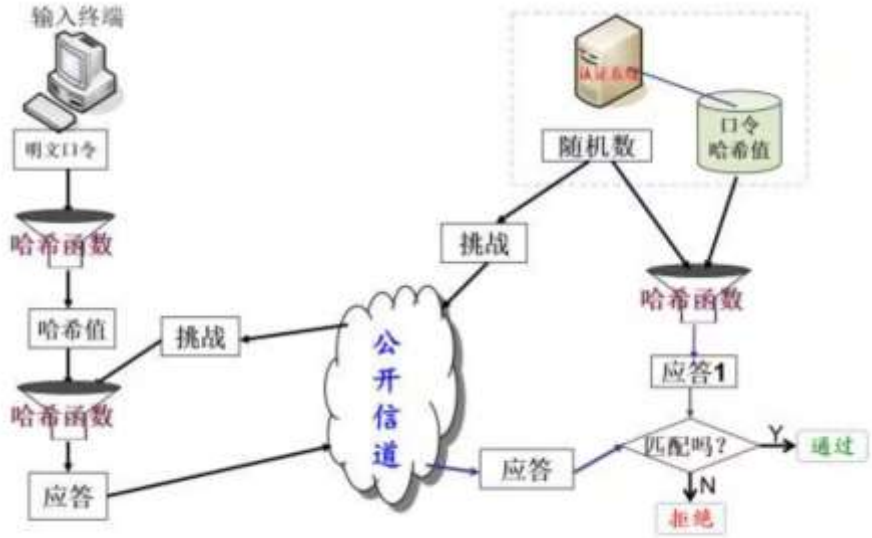
1. **用户口令相关信息在广域网上安全传输（也就是说，即使攻击者窃取了用户网上传输的信息，也分析不出用户的口令）。**
2. **服务器的管理员不知道用户的口令。**

请设计一个方案(至少包括新口令的设定和口令的验证)实现上述的安全功能并分析其安全性。

新口令设置:



远程口令认证:



安全分析:

(1) 在远程认证过程中，攻击者能得到应答信息(口令和随机数的哈希值)，根据 Hash 函数的特性，攻击者即使得到“挑战”(随机数)也不能分析出口令的哈希值，更不可能分析到口令。每次远程口令认证都要使用不同的“挑战”(随机数)，目的是防止攻击者的重放攻击。所以，用户口令相关信息(应答信息)在广域网上传输并不能泄露口令的哈希值，更不可能泄露口令。

(2) 当用户选用新口令，并使用初始口令哈希值作为密钥加密新口令的哈希值，攻击者截获到密文，因为不知道初始口令，也就得不到加密密钥，就不能解密从而得不到新口令的哈希值,当然攻击者更不可能分析到新口令。管理员知道初始口令，从而能得到新口令的哈希值，根据 Hash 函数的特性，管理员不能得到新口令。