1．是非判断题

(1)哈希函数的定义中的“任意消息长度”是指实际中存在的任意消息长度，而不是理论上的任意消息长度。（ V ）

(2)关于哈希函数的特性，具有抗强碰撞性的哈希函数一定具有抗弱碰撞性。（ V ）

(3)哈希函数可以将“任意消息长度”的消息经过变换得到固定长度的输出，也就是说，无论采用何种哈希函数，所得哈希值的长度总是相同的。（ X ）

注：不同的哈希函数所得哈希值不同

(4)哈希函数的安全性是指根据已知的哈希值不能推出相应的消息原文。（ X ）

注：主要是防止碰撞的出现

(5)MD5、SHA1、SHA256 这三个算法所输出的哈希值长度是不同的，并且它们的分组长度也是不相同的。（ X ） 注：都是 512 位

(6)SHA-256 和 SHA-512 输入消息的最大长度是相同的。（ X ）注：$2^{64}-1$ 和 $2^{128}-1$

(7)SHA 系列算法有多个，其输出的散列值长度是不相同的，其散列值长度越长，其安全性就越高。（ V ）

(8)基于 hash 消息认证码的输出长度与消息的长度无关，而与选用的 hash 函数有关。（ V ）

(9)基于 hash 消息认证码 HMAC 的安全强度是由嵌入散列函数的安全强度决定的。（ V ）

(10)消息认证码 MAC 的生成过程使用到密钥,所以,消息认证码 MAC 也是一种保密技术。（ X ） 注：密钥用来确定消息的来源

2．选择题

(1)下面哪一项***不是***hash 函数的等价提法。（ A ）

A. 压缩信息函数 B. 哈希函数 C. 单向散列函数 D. 杂凑函数

(2)下面哪个***不是***hash 函数具有的特性。（ B ）

A. 单向性 B. 可逆性 C. 压缩性 D. 抗碰撞性

(3)现代密码学中很多应用包含散列运算，而下面应用中***不包含***散列运算的是（ A ）。

A. 消息机密性 B. 消息完整性 C. 消息认证码 D. 数字签名

(4)散列（哈希）技术主要解决信息安全存在的（ B ）问题。

A. 保密性 B. 完整性 C. 可用性 D. 不可否认性

(5)在众多 Hash 算法中，SHA 被称为安全的哈希函数，其中 SHA-1 生成消息的哈希值长度是（ C ）。

A. 64 位 B. 128 位 C. 160 位 D. 256 位

(6)下面哪一项***不是***hash 函数的应用（ C ）。

A. 文件校验 B. 数字签名 C. 数据加密 D. 安全存储口令

(7) SHA-1 算法是以（ D ）位分组来处理输入信息的。

A. 64 B. 128 C. 256 D. 512

(8) SHA-1 算法可接受输入消息的最大长度是（ C ）比特。

A. 任意 B. 2^{64} C. $2^{64}-1$ D. $512*(2^{64}-1)$

注：填充前留有 64 位存放信息的长度

(9)分组加密算法（如 AES）与散列函数算法（如 SHA）的实现过程最大的***不同***是（ D ）。

A. 分组　　B. 迭代　　C. 非线性　　D. 可逆

(10)生日攻击是针对下面哪种密码算法的分析方法。（ D ）

A. DES　　B. AES　　C. RC4　　D. SHA-1

(11)设 hash 函数的输出长度为 n 比特，则安全的 hash 函数寻找碰撞的复杂度应该为（ D ）。

A. O(n)　　B. $O(2^n)$　　C. $O(2^{n-1})$　　D. $O(2^{n/2})$

注：见书 P180

(12)消息认证码(MAC)的主要作用是实现（ B ）。

A．消息的保密性　B．消息的完整性　C．消息的可用性　D．消息的不可否认性

(13)国家商用密码管理办公室制定了一系列密码标准，其中（ C ）是哈希函数。

A. SM1　　B. SM2　　C. SM3　　D. SM4

3．填空题

(1)Hash 函数就是把任意有限长度消息的输入，通过散列算法，变换成固定长度二进制的输出，该输出称为__哈希值或杂凑值__。

(2)Hash 函数的单向特性是指_对于给定的哈希值 h，要找到一个消息 M，使得 M 的哈希值等于 h 在计算上是不可行的_。

(3)Hash 函数的抗碰撞性是指_不同的消息 M1 和消息 M2，使得 M1 的哈希值与 M2 的哈希值相等在计算上是不可行的__。

(4)Hash 函数迭代使用一个压缩函数，压缩函数有两个输入：一个是前一次迭代的 n 位输出，称为链接变量，另一个来源于消息的_一个分组_，并产生一个 n 位的输出。第一次迭代输入的链接变量又称为_初始值_，由算法在开始时指定，最后一次迭代的输出即为___消息哈希值__。

(5)SHA-1 算法的输入是最大长度小于_2^{64}_比特的消息，输出为_160_比特的消息摘要。

(6)SHA-1 的算法核心是一个包含_4_轮组成的，每轮由__20_个步骤组成，每轮使用的步函数相同，不同轮中步函数包含不同的_非线性函数_，每一步函数的输入也不相同，除了寄存器 A、B、C、D 和 E 外，还有_额外常数__和__子消息分组__。

(7)与以往攻击者的目标不同，散列函数的攻击不是恢复原始的明文，而是寻找__碰撞_的过程，最常用的攻击方法是__生日攻击___。

(8)消息认证码的作用是_验证信息的来源是真实的__和_验证消息的完整性__。

(9)MD5、SHA-1、SHA-256 的消息分组长度为__512__比特，SHA-384、SHA-512 的消息分组长度为__1024_比特。

4．思考题

(1)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入到远程的服务器上，服务器的管理员给每个用户设置一个初始口令，请利用哈希函数的技术实现以下安全需求：

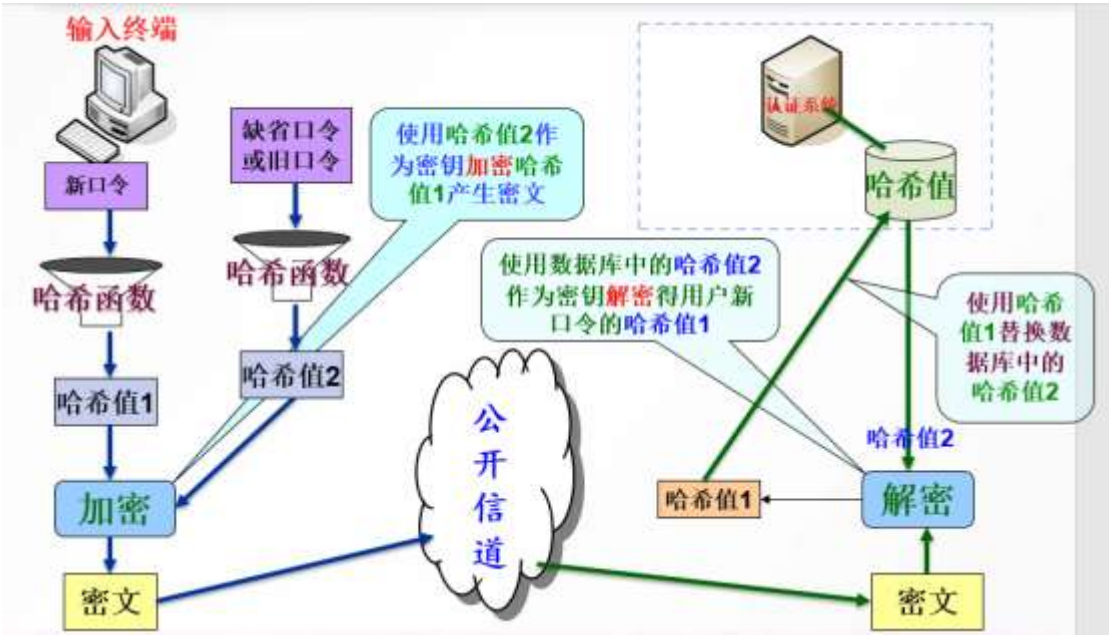
（ⅰ）用户口令在广域网上安全传输（也就是说，即使攻击者窃取用户网上传输的信息，也分析不出口令）。

（ⅱ）管理员也不知道用户的口令。

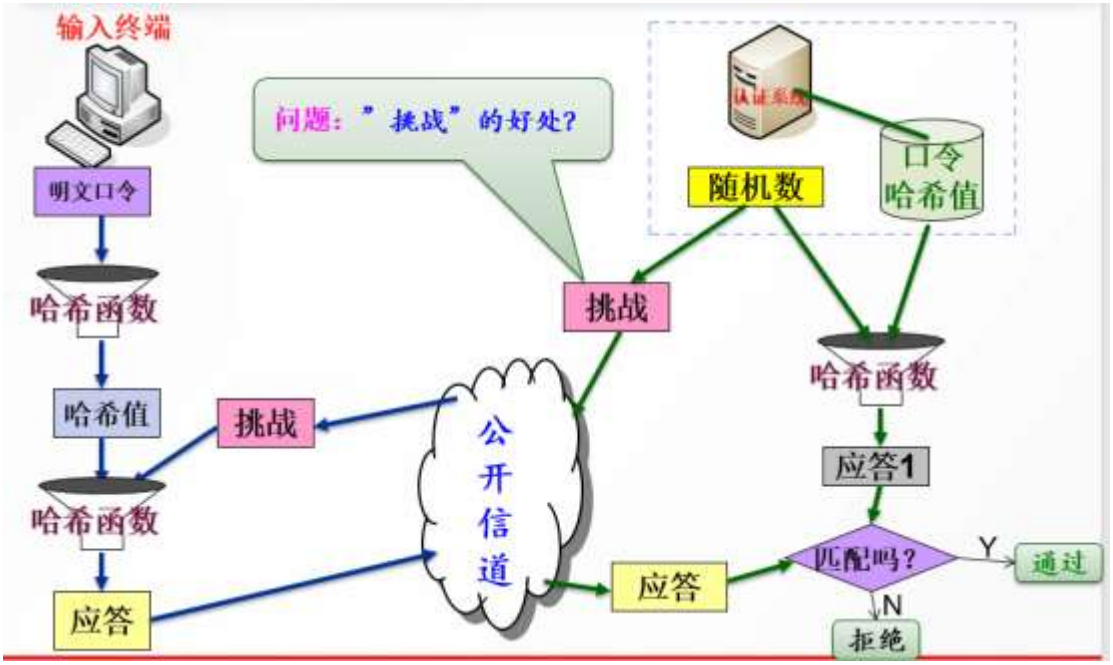
请设计一个方案满足上述的安全需求并分析其安全性。

提示：通常方案包括两部分，首先，用户根据管理员给定的初始口令，设定只有自己知道的新口令；然后，实现用户使用新口令认证自己的身份。

（ｉ）用户设置自己的口令



（ii）口令认证过程



(2) **SM3** 是我国采用的一种密码散列函数标准，由国家密码管理局于 2010 年 12 月 17 日发布，请简要描述 sm3 算法的实现过程。

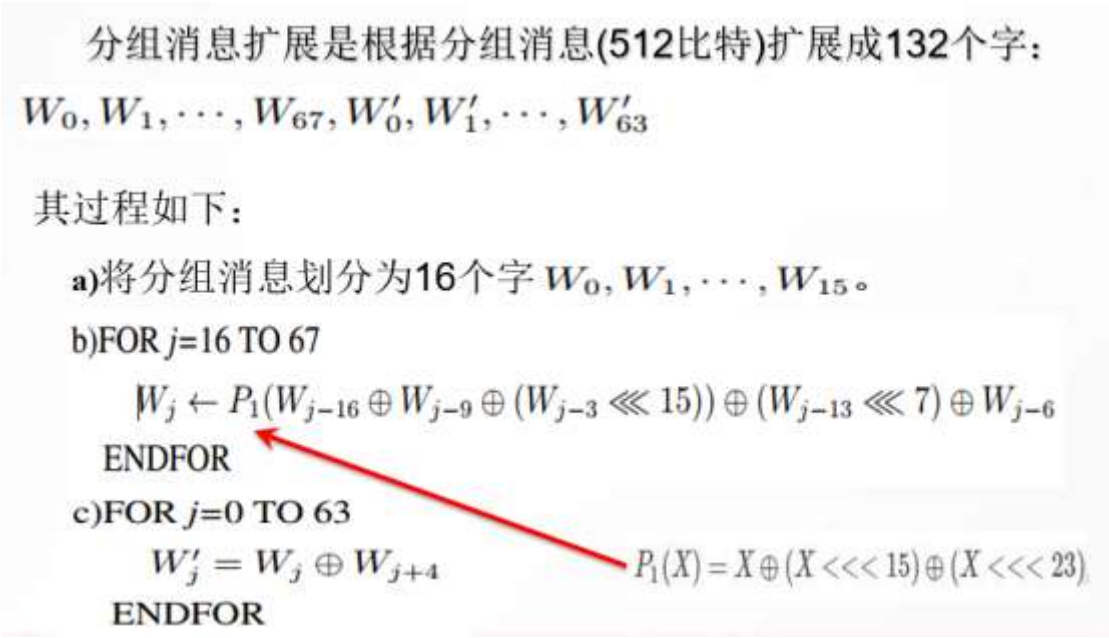
SM3 是我国采用的一种密码散列函数标准，由国家密码管理局于 2010 年 12 月 17 日

发布，其主要用于数字签名及验证、消息认证码生成及验证、随机数生成等，其算法公开，据国家密码管理局表示，其安全性及效率与 SHA-256 相当。

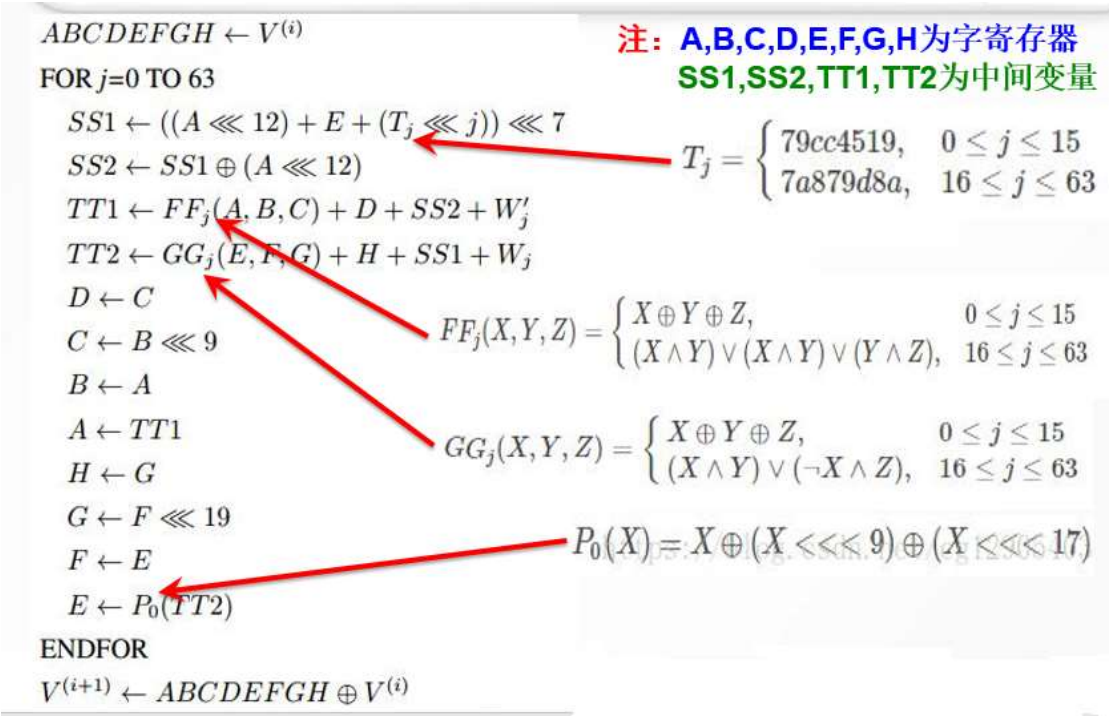
对长度为 L(< 2^{64}) 比特的消息 m， SM3 杂凑算法经过填充和迭代压缩，生成杂凑值，杂凑值长度为 256 比特。

SM3 算法的消息分组长度为 512 比特，如果不满足 512 比特分组，需要填充，其填充方法同 SHA-1 填充方法完全一致。

分组数据的扩展：



算法实现过程：



注：V^0= 7380166f 4914b2b9 172442d7 da8a0600 a96f30bc 163138aa e38dee4d b0fb0e4e