**密码学第九次作业**

1.【Hash函数基础知识】

（1）Hash函数首要实现的安全目标是保护，它的输入长度，输出长度。

（2）Hash函数应用广泛。Hash函数常用于构造、、。此外，在密码学中还常将Hash函数应用于数字签名，请写出数字签名往往需要用到Hash函数的原因。

**原因：由于现代密码学使用的都是公钥密码技术, 而且这种非对称算法的运算速度较慢, 所以对消息在传 输前都要进行一定的压缩计算。**

（3）以下三项是密码学Hash函数最常见的安全性需求：

I.抗攻击（性）：；

II.抗攻击（性）：；

III.抗攻击（性）：。

请填写上述内容，并画出以上安全特性（安全性需求）之间的联系图。

（4）从穷举攻击的角度攻击位的Hash值。对于原像攻击和第二原像攻击，攻击者的平均尝试次数为。对于碰撞攻击，攻击者往往采用生日攻击，将平均尝试次数降为，请简述攻击者通过生日悖论进行碰撞攻击，在不知道密钥的前提下伪造消息签名的过程。

（5）构造Hash函数的方法很多。请至少写出3种构造（安全的）Hash函数的方法并各给出一个例子。

2.【迭代型Hash函数基础知识】

（1）迭代型Hash函数根据提出该概念的作者名又称结构Hash函数。在MD5、SHA1、SHA2、SHA3、SM3中，原名为算法的没有采用该结构，而是采用了结构。

（2）请画出迭代型Hash函数的结构图并写出其递归定义。

（3）如果压缩函数具有抗碰撞能力，那么迭代Hash函数也具有抗碰撞能力。请简述：接受任意长输入的Hash函数为什么不可能是无碰撞的？

（4）MD5的输入长度，分组长度为，输出长度为。SHA1的输入长度，分组长度为，输出长度为。

（5）迭代型Hash函数往往需要填充，MD5、SHA1、SHA512的填充与附加消息长度值的方式类似。请简述它们的附加填充位、附加长度值的具体步骤及区别。

3.【MAC基础知识】：

（1）消息认证码MAC是一种技术，是指消息被一的公开函数作用后产生的、用作认证符的、固定长度的数值，也称为密码校验和。消息认证码的函数形式是，其中，为；为。

（2）常见的构造MAC的方式有：、、用伪随机函数构造MAC等。

（3）对于位密钥，位明文输入的MAC：

I.请描述对密钥的穷举攻击方法。

II.综合考虑对密钥或对消息的穷举攻击，MAC算法的穷举攻击所需的代价为。

III.一般认为MD5算法是不安全的Hash算法，但HMAC-MD5仍被认为是安全的，请简述原因。

**注意：**

以上作业请使用**pdf**文档格式提交，于**2023年5月19日（星期五）23:59**之前在OJ系统上提交，并将作业命名为“**学号\_姓名\_密码学第九次作业**”。如“21371234\_张三\_密码学第九次作业”。