第一节作业

**1、SHA系列的压缩函数中，轮迭代之后，为什么要与输入链接变量（初始变量）模加?**

为了防止生日攻击。

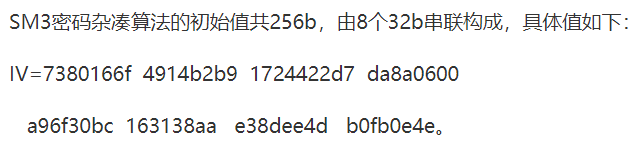
**2、调研国标GM/T 0004-2012。**

SM3是中华人民共和国政府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，相关标准为“GM/T 0004-2012 《SM3密码杂凑算法》”。2016年，成为中国国家密码标准（GB/T 32905-2016）。

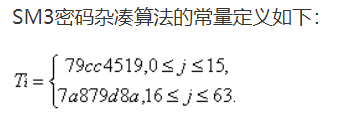
在商用密码体系中，SM3主要用于数字签名及验证、消息认证码生成及验证、随机数生成等，其算法公开。据国家密码管理局表示，其安全性及效率与SHA-256相当。

SM3密码杂凑算法采用Merkle-Damgard结构，消息分组长度为512b，摘要长度256b。压缩函数状态256b，共64步操作步骤。

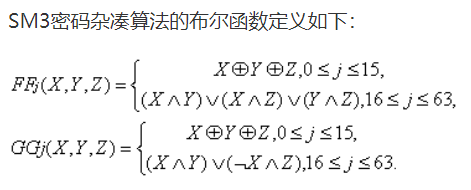
SM3密码杂凑算法的初始值：



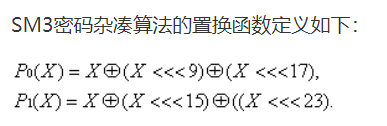
SM3密码杂凑算法的常量：



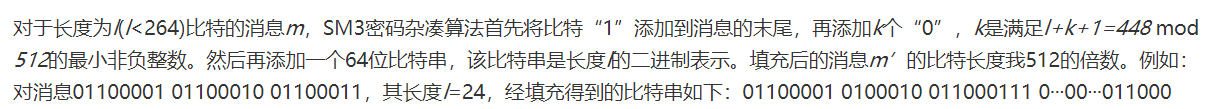
SM3密码杂凑算法的布尔函数：



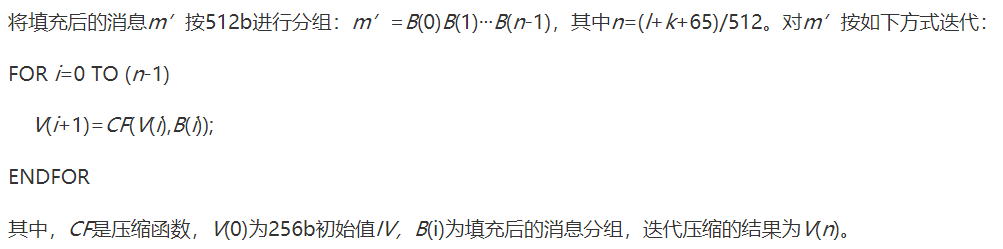
SM3密码杂凑算法的置换函数：



SM3密码杂凑算法的消息填充：



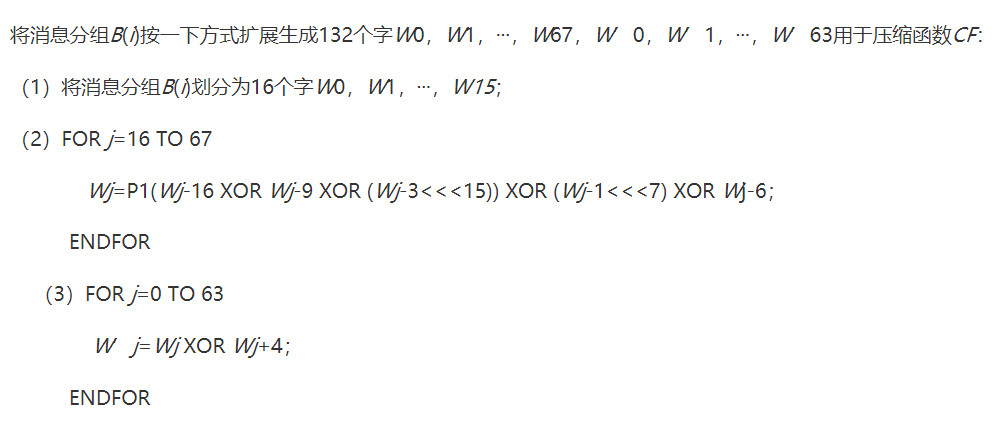
SM3密码杂凑算法的迭代压缩过程：



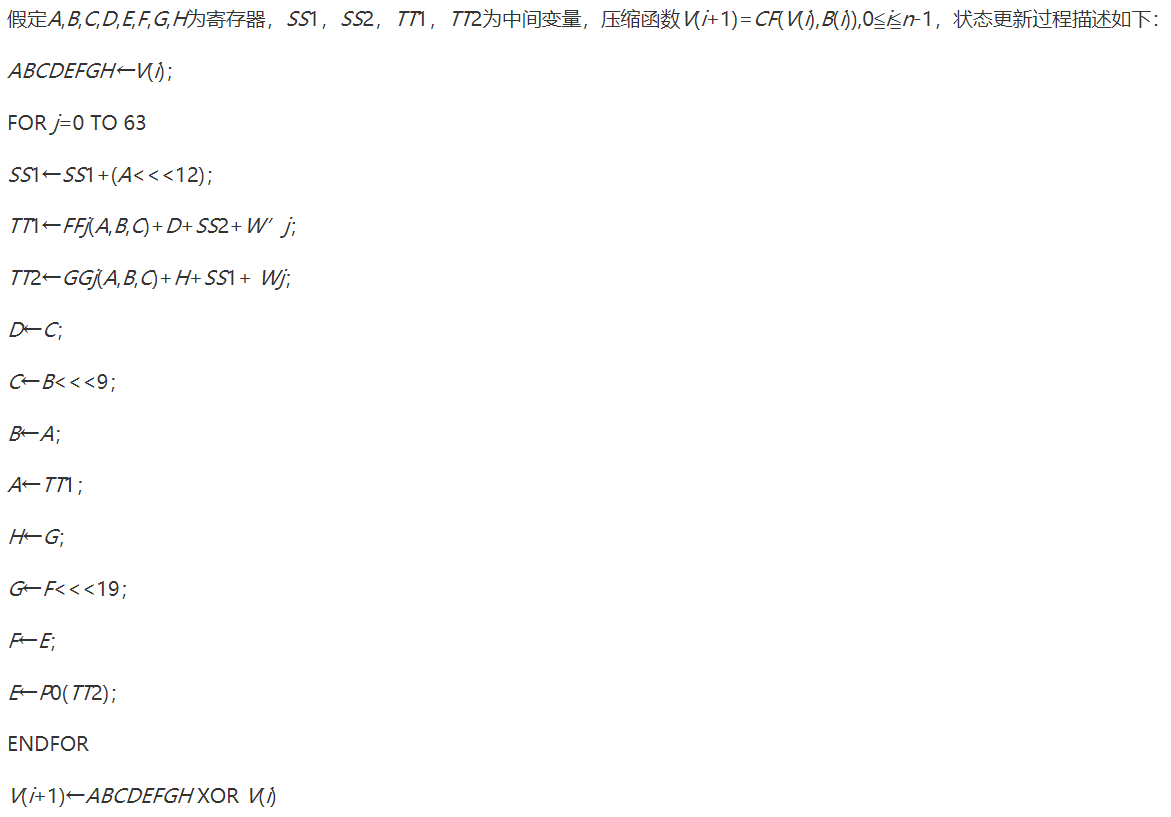
SM3密码杂凑算法的压缩函数：

SM3密码杂凑算法的压缩函数由消息扩展过程和状态更新过程组成，具体描述如下。

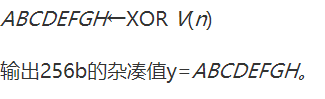
1、过程1消息扩展过程



2、过程2 状态更新过程：



3、过程3 杂凑值：



SM3密码杂凑算法的特点：

SM3密码杂凑算法压缩函数整体结构与SHA-256相似，但是增加了多种新的设计技术，包括增加16步全异或操作、消息双字介入、增加快速雪崩效应的P置换等。能够有效地避免高概率的局部碰撞，有效的抵抗强碰撞性的差分分析、若碰撞性的线性分析和比特追踪法等密码分析。

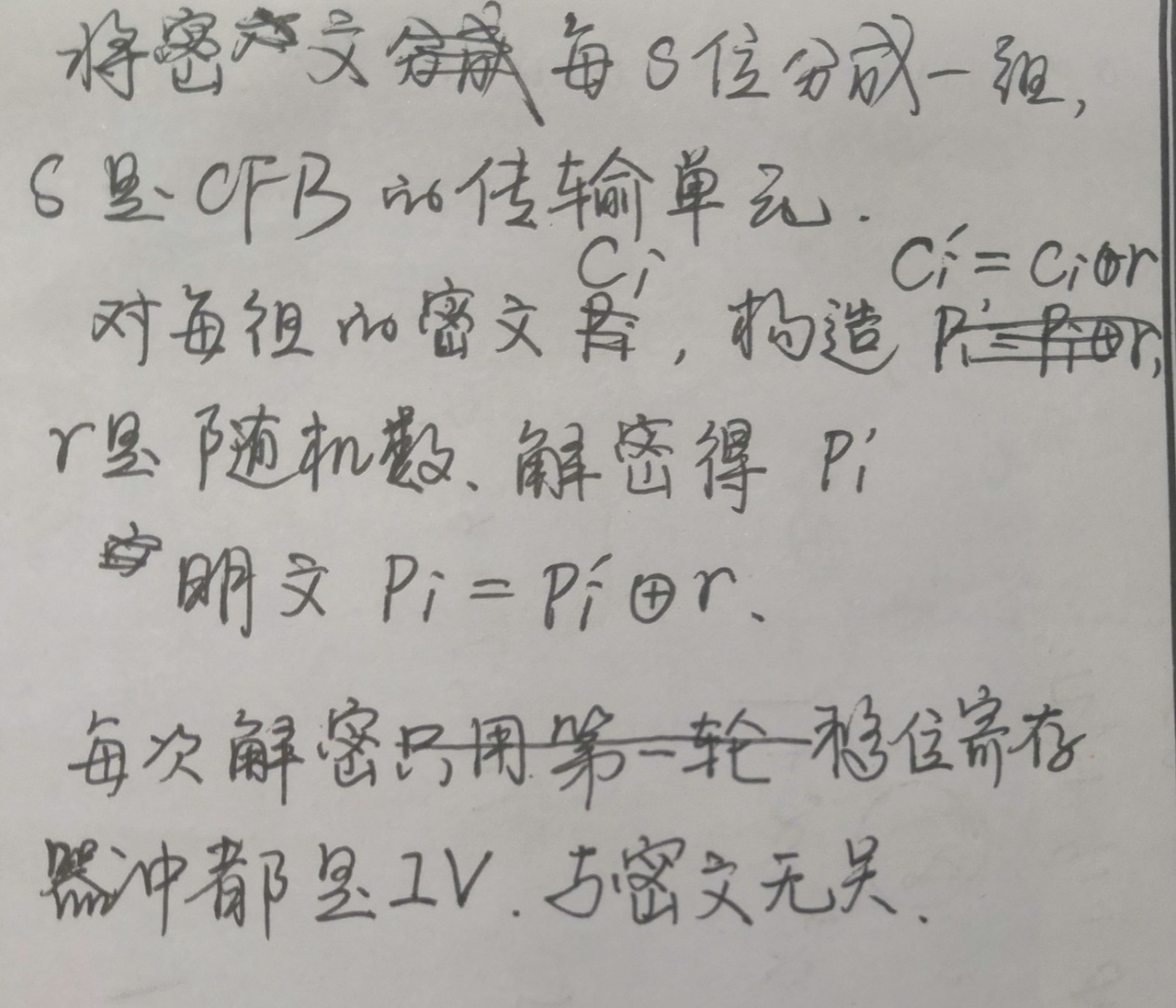
SM3密码杂凑算法合理使用字加运算，构成进位加4级流水，在不显著增加硬件开销的情况下，采用P置换，加速了算法的雪崩效应，提高了运算效率。同时，SM3密码杂凑算法采用了适合32b微处理器和8b智能卡实现的基本运算，具有跨平台实现的高效性和广泛的适用性。

第二节作业

**1、对上述选择消息攻击（攻击二），三种填充方法是否可以防止？选择处理（截断）是否可以抵抗上面攻击？**

对于攻击二，前两种填充方式不能防止，第三种可以；选择处理可以抵抗上面攻击。

**2、试给出CFB运行模式的选择密文攻击。**

****