现代密码学

第六讲作业

第一节作业

1 SHA-256处理的消息最大长度为$2^{64}-1$比特，为什么？

2 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

3 （选作）调研国标GM/T 0004-2012

4 （选作）调研区块链中Merkle tree的作用，是否可以直接将所有交易信息输入某hash算法，hash值放在区块中？为什么？

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？

2 试给出CFB运行模式的选择密文攻击？