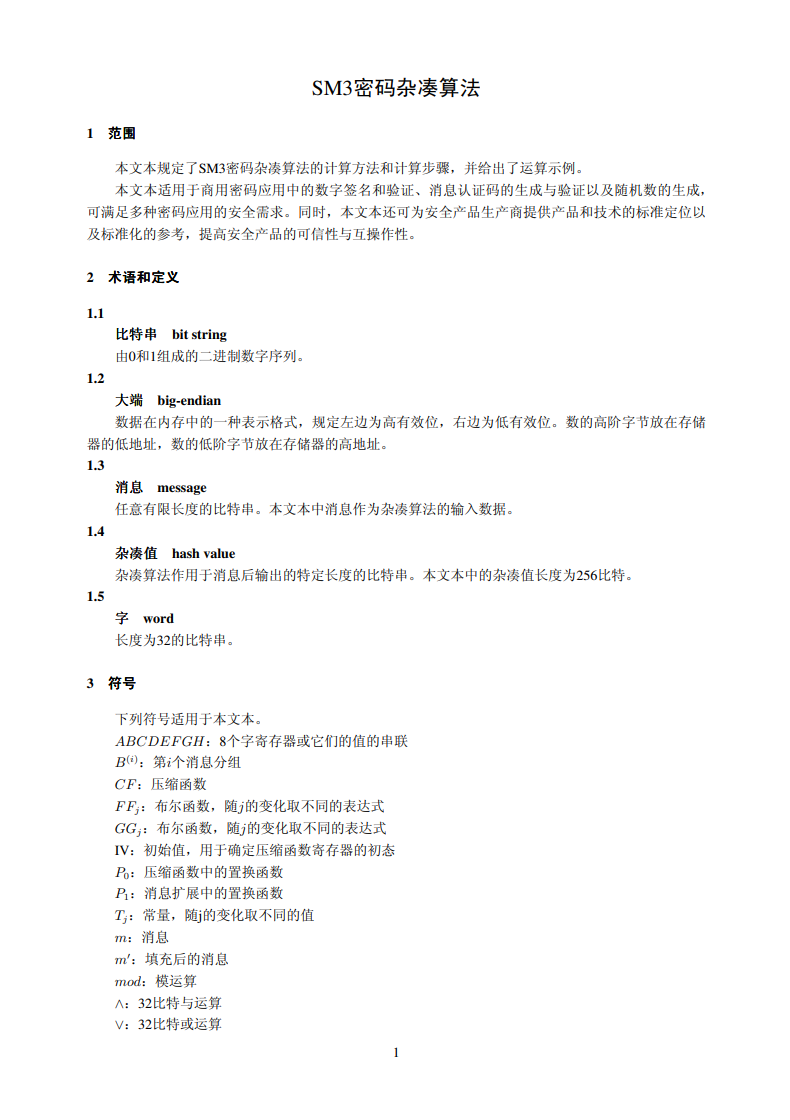
现代密码学作业——第六讲

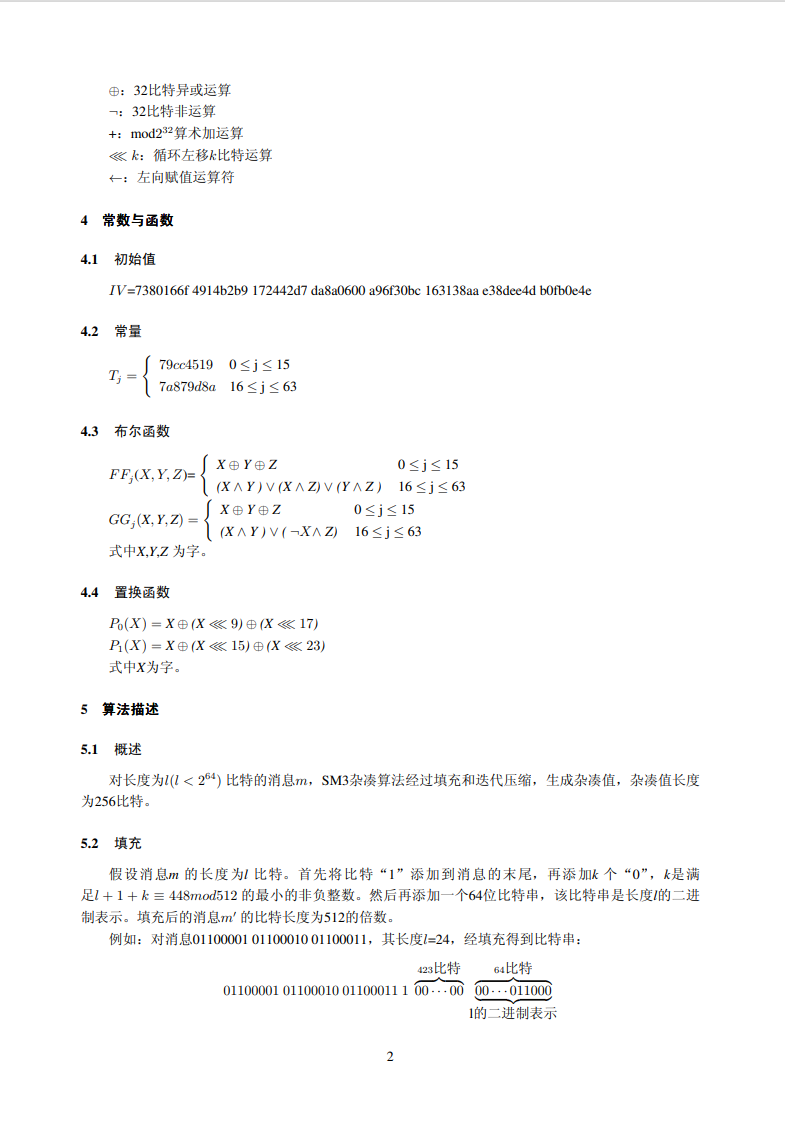
一、第一节

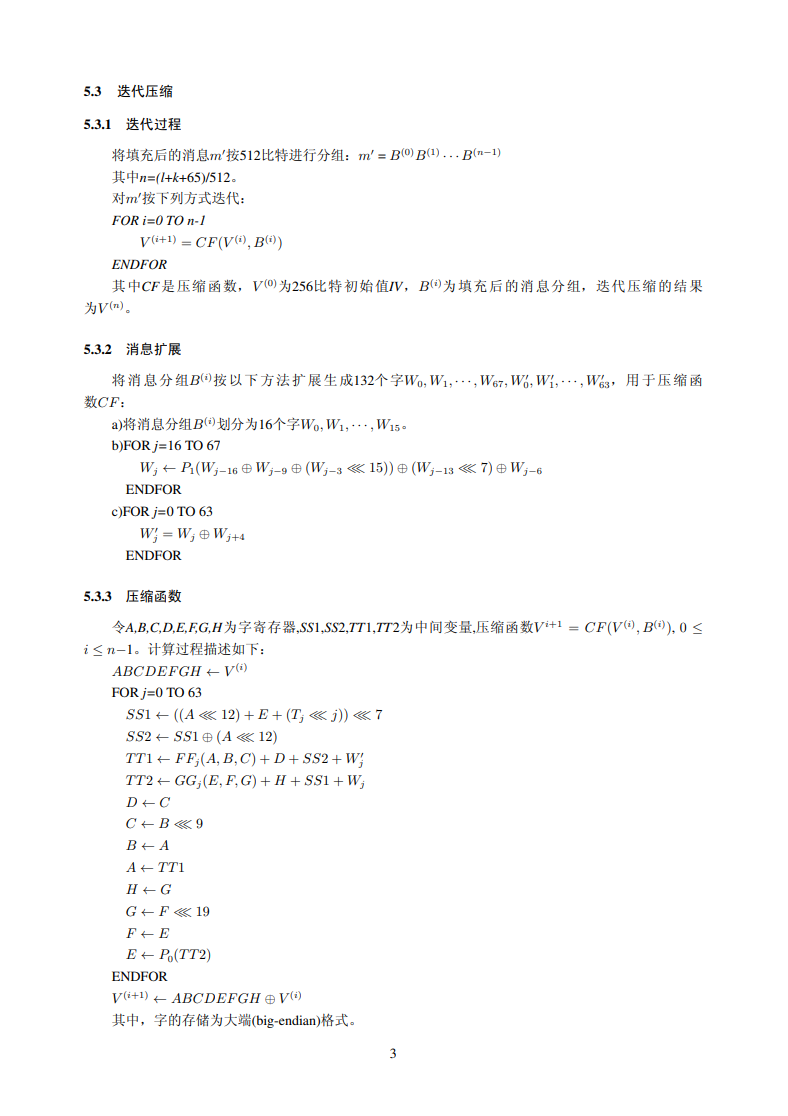
1、预留了64比特，用于填充消息的长度。

2、否则可以用中间相遇攻击求出二次原像，复杂度仅为O(2n/2)。

3、SM3杂凑算法。









一、第二节

1、第一、二种可以攻击成功，第三种和选择处理不行。

2、

①假设已知（C1||C2）j 为 IV 加密后的值

②构造一个 C2’=C2’⊕r

③将(C1||C2’)输入 oracle 得到(m1||m2’)

④推导出m1||m2=m1||m2’⊕r