1. 填空

1、

4.11. 试分析一下CBC、CFB、OFB运行模式的错误传播情况。

CBC的错误传播只影响当前分组和下一分组的解密

CFB的错误传播影响当前分组的对应bit解密和后续的⎣64/j ⎦或⎣64/j ⎦+1个分组的解密

OFB的错误传播只影响当前分组的对应比特解密，无错误传播

4. 14. Rijndael算法是建立在GF(28)有限域上的，且模多项式为*m*(*x*)=*x*8+*x*4+*x*3+*x*+1，试计算(*x*6+*x*2+*x*+1)×(*x*4+*x*+1) mod *m*(*x*)，该计算用x乘来表示时，试给出计算过程。

解：上述乘法即求’47’ ×’13’

’47’ ×’02’=*x*time(47)=’8E’ //×*x*

’47’ ×’04’=*x*time(8E)=’07’ //×*x*2

’47’ ×’08’=*x*time(07)=’0E’ //×*x*3

’47’ ×’10’=*x*time(0E)=’1C’ //×*x*4

而’13’=’01’+ ’02’+ ’10’

所以’47’ ×’13’=’47’ ×(’01’+ ’02’+ ’10’)= ’47’+ ’8E’+ ’1C’=’D5’

即(*x*6+*x*2+*x*+1)×(*x*4+*x*+1) mod *m*(*x*)= *x*7+ *x*6+ *x*4+*x*2+1

5.3 试证明：在Feistel结构密码中解密过程第1轮的输出等于加密过程最后一轮输入左右两半交换值

证明：假设加密过程的最后一轮输入左右两半分别表示为*LE*15，*RE*15，输出的左右两半分别表示为*LE*15，*RE*15，第16轮子密钥为*K*16

解密过程取密文作为同一算法的输入，由于加密最后一轮输出后又进行了左右交换，所以解密第1轮输入是*RE*16‖*LE*16

在加密过程中：

*LE*16＝*RE*15 ； *RE*16＝*LE*15⊕*F*(*RE*15, *K*16)

在解密过程中

*LD*1＝*RD*0=*LE*16＝*RE*15

*RD*1＝*LD*0⊕*F*(*RD*0, *K*16)＝*RE*16⊕*F*(*RE*15, *K*16)

＝[*LE*15⊕*F*(*RE*15, *K*16)] ⊕*F*(*RE*15, *K*16)＝*LE*15

证毕#