班级：_____ 学号：_____ 班内序号：_____ 姓名：_____

密 封 线

《现代密码学》

2017-2018 学年第一学期期中考试试题

一、简答题（每题 5 分）

1） 给出对称保密体制的定义？

六要素

2）hash 函数需要满足的安全目标是什么？

pre-image

second pre-image

collision

3）给出消息认证体制的定义？

M S V K

4）举例说明混淆和扩散的定义和它们的作用。

Wide
Hide

m+k = c 1个

am+b = c 2个

5）什么是 Feistel 结构、SPN 结构、MD 加强结构？

DES AES Merkle-Damgard

6）分组密码迭代的轮函数、hash 函数中压缩函数哪个必须是单向函数、哪个必须可逆，哪个可以单向也可以可逆？

hash 单向

SPN 可逆

Feistel 单向 or 可逆

7）保密系统满足的安全性假设是什么？

CCA - IND

不能获得任何信息

8）消息认证系统满足的安全性假设是什么？

ACM 一抗 EF

9）分组密码的工作模式的作用是什么？为什么分组密码和流密码中都需要保证（IV,k）不重复使用？ 长消息加密 改变

10）假设通信双方使用 CFB 模式(加密算法为 AES)加解密，设传送的每个单元 j=128 比特，攻击者在信道截获密文(IV,C*),|c*|=128 比特，试描述攻击者如何恢复目标明文 m*。

计算分析题（每题10分）

1) 计算0x87乘以0x03模 $m(x)=x^8+x^4+x^3+x+1$ 的值。

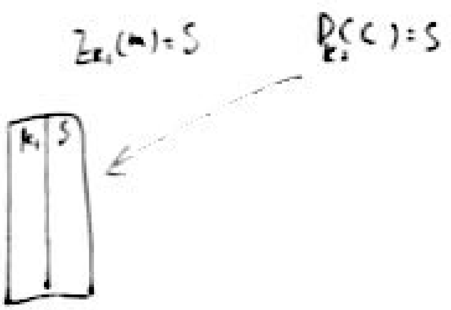
$(0x87 \otimes 0x02) \oplus (0x87 \otimes 0x01)$

2) 设计一个5级线性反馈移位寄存器，使其输出m序列？

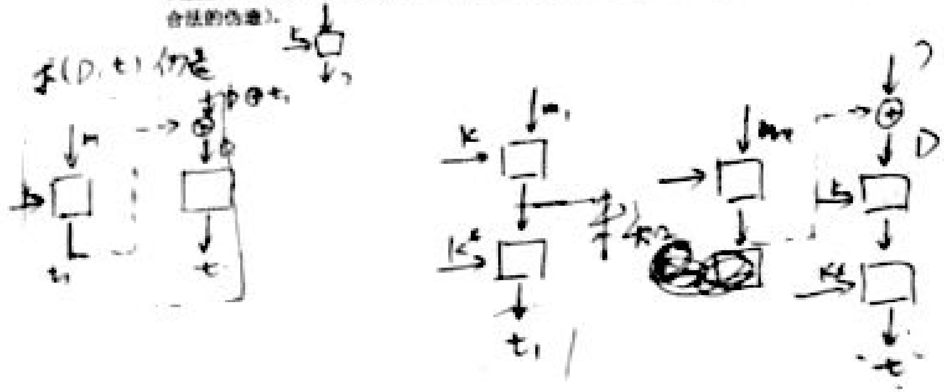
5级本原多项式

3) 给出2DES的中间相遇攻击过程及复杂度。

$E_{k_1}(m)=S$　　$D_{k_2}(C)=S$



4) 分析选择消息攻击如何伪造raw CBC-MAC的下述攻击（攻击者选定消息D，通过第一次挑战时的消息m1，得到响应t1，第二次挑战消息m1||D⊕t1，得到响应t，则(D,t)为合法的伪造）。



5) 令MD结构的hash函数的压缩函数定义为 $H_i=E(m_i,H_{i-1})\oplus m_i$，该体制是否安全？不安全写出具体攻击。

设定 $m_1||m_2$ 得 $h(m_1||m_2)=H_2$

$H_1=E(m_1, IV)\oplus m_1$　　$H_2=E(m_2, H_1)\oplus m_2$