[redacted]

简答题

1.密码学的五个安全属性是什么？SM4、ZUC分别是保障什么安全属性的？

2.Shannon给出的通信保密模型的六要素是什么？

明文、密文、加密密钥空间、解密密钥空间、加密算法、解密算法。

DE=I

3.已知明文/密文的假设下，单表代换、置换(分组长度为m)，AES-128、RC4-128，穷举搜索密钥的复杂度各是多少？为什么？

26!

m!

2^128，因为这是最坏情况下搜尽所有密钥，总能找到正确的。

2^128

4.AES 和DES的迭代结构是什么？AES的轮函数中的哪几个操作主要是实现混淆、扩散？

混淆(非线性)：只有字节代换

扩散：列混合、行移位

5.分组密码的工作模式中，哪个只适合短消息，哪个是分组模式且适合长消息加密，哪种模式适合长消息加密且可以并行加密，哪总有传播错误且有限的传播错误，哪种有密文扩展。

CBC

CTR

CBC/CFB

ECB、CBC

6.以A5算法为例子，解释基于LFSR技术设计的安全伪随机数生成器，通常包含哪两个部分？

[redacted]

驱动部分、非线性部分

A5为例，用三个线性..作为驱动部分，有一个**函数，在里面选，何时进动，实现非线性。当前最低位作为输出。

7.IV初始值作为为随机数生成器的输入有何作用？IV选取通常满足什么条件。

只有密钥会导致，相同的消息会输出相同的密文，这在选择明文攻击下，可能会泄露明文。

m_1 → Oracle → …

m_2 …

作用就是，抗选择明文攻击

IV值满足的条件(在分组密码的工作模式时，仍需满足这些条件)

IV值不可预测/随机

IV值空间要大

(可选)有外界同步方式

8.简述hash的MD迭代结构和压缩函数的DM结构

- MD结构(描述下面几个点，或者画个图都行)
  - 填充
  - 分组
  - 链接遍历的传递，最后一块消息迭代完的是哈希值
- DM结构(描述下面几点，或者画个图都行）
  - 消息块作为密钥
  - 链接变量作为明文
  - 加密函数的输出要与链接变量进行异或

9.对于CBC-MAC（调用AES-256算法），穷举搜索密钥和伪造攻击的复杂度各是多少？为什么？

穷举搜索密钥 2^256

伪造 min{2^mac长度,2^密钥长度}=2^128

10.SM3是保障什么安全属性的？调用SM3的HMAC是保障什么安全属性的？简单说明她们在保障该属性时的区别？

SM3保障消息完整性

HMAC保障消息完整性、实体认证性

区别：有没有密钥，哈希函数防范 攻击者是被动攻击的时候，但是如果攻击者是主动攻击者(可以读写)，此时只能使用HMAC。

分析计算题

1.什么是加解密相似？证明DES的迭代结构是加解密相似的

加解密相似 < = > 加解密模块是完全一样的，仅密钥顺序不一样

推导一下就行了

2.计算列混合(课本有例题)

3.设计一个4级的LFSR，生成m序列

四级本原多项式→写出反馈函数

4.给出hash函数求碰撞的生日攻击过程及其复杂度

抄PPT

5.举例说明为什么使用认证加密模式才可以保障信息的机密性？

分组密码的工作模式/流密码只能防范选择明文攻击

但是，要使用认证加密模式，防止选择密文攻击(最强攻击者）

- 笔记
  - 机密需要 加密+消息鉴别保证
  - 加密防止选择明文攻击及其以下的攻击
  - 消息鉴别防范选择密文攻击，接收方如果发现C被篡改了，就不输出明文了