**电子科技大学2023-2024学年第二学期期中考试卷**

**课程名称：密码学 考试形式：闭卷 使用教师：汪小芬**

**学院：\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 姓名：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_学号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. 填空题（每空2分，共20分）

1，密钥保密性。

2，代换-置换SP网络 和feistel网络

3，无条件安全。

4， OFB模式、CFB模式、CTR模式。

5， 48bit、 32bit、 0011

1. 选择题（每小题3分，共15分）

BDDD10101010

1. 计算题（每小题15分，共45分）

1，

（1）D(c)=(c−21)×15 mod 26

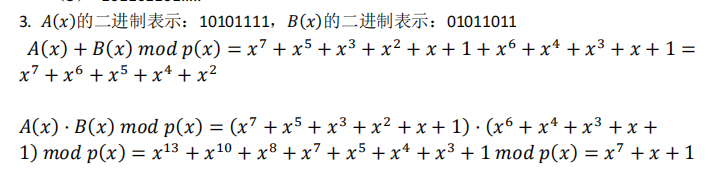
（2）yxvjsxk

（3）security

2,

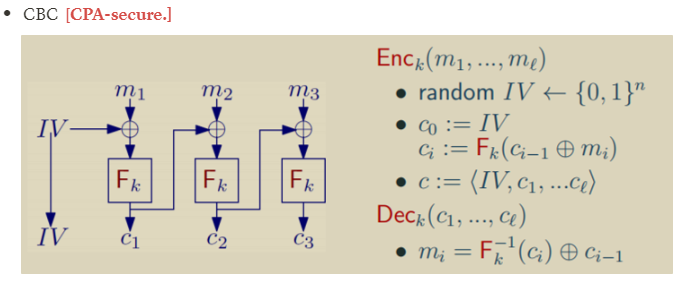
图片包含 文本

描述已自动生成



四，简答题（20分）

1，（答案合理就给分）

1) 

2).初始向量(IV)在CBC模式中起到了两个重要作用:

首先，它确保了每次加密操作的唯一性。由于CBC模式是基于前一个密文分组的加密结果来加密当前明文分组，如果每次加密过程使用相同的IV那么相同的明文将会生成相同的密文，这可能导致安全性问题。其次，它增加了密码的随机性。CBC模式要求IV必须是随机的，这样可以减少密码分析的可能性，并提高密码系统的安全性。

3).CBC模式中的填充是指在加密时对明文进行填充，以保证明文的长度是AES块大小的整数倍。填充的目的是为了满足加密算法对固定长度数据块的要求，使得明文可以被正确地分割成块并进行加密。在AES算法中，通常使用PKCS#7填充(也称为PKCS5padding)，即在需要填充的位置填充相应的字节，字节的值等于需要填充的字节数，

4).优点：由于引入了初始向量, 相同的明文块产生的密文块可能不同, 能够隐蔽明文的数据格式。

缺点：密文块ci中单个比特出错会影响后续至多两个密文块(ci和ci+1)的解密, 具有有限的错误传播特性。明文块mi发生改变将引起后面所有密文块发生改变。