**密码学第五次作业参考答案**

1.【工作模式基础知识】请填写下表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | ECB | CBC | CFB | OFB | CTR |
| 加密递推式 |  |  |  | （OFB模式应同CFB一样具有移位寄存器LSB，但教材P146未定义该模块） |  |
| 解密递推式 |  |  |  |  |  |
| 初始向量（时变值，计数器等）（Y/N） | N | Y | Y | Y | Y |
| 加密并行性（Y/N） | Y | N | N | (可并行执行，建议填Y) | Y |
| 解密并行性（Y/N） | Y | Y | Y | Y | Y |
| 需要分组密码解密模块（Y/N） | Y | Y | N | N | N |
| 含有反馈（Y/N） | N | Y | Y | Y | (不同教材存在争议，密码学教材主张Y) |

2.【错误恢复能力】

（1）错误传播：错误传播是指第个密文分组的错误会被第组及其后的所有明文分组继承。对于ECB，CBC，CFB，OFB，CTR五种工作模式，假设第组明文加密得到的密文产生了1bit错误，后续密文是否有影响？基于此密文的解密结果，相比于明文如何？请逐个说明。

ECB：后续密文无影响，该组密文解密得到的明文完全错误。

CBC：后续所有密文被打乱，该组密文解密得到的明文完全错误。

CFB：后续所有密文被打乱，该组密文解密得到的明文有1bit错误。

OFB：后续密文无影响，该组密文解密得到的明文有1bit错误。

CTR：后续密文无影响，该组密文解密得到的明文有1bit错误。

（2）传输错误：传输错误是指密文从发送方传递到接收方时由于信道质量不佳等原因所造成的接收方收到的密文与发出时的结果不同。对于ECB，CBC，CFB，OFB，CTR五种工作模式，假设第组密文传输时产生了1bit错误，基于此密文的解密结果，相比于明文如何？请逐个说明。

ECB：该组密文解密得到的明文完全错误。

CBC：该组密文解密得到的明文完全错误，下一组密文解密得到的明文有1bit错误。

CFB：该组密文解密得到的明文有1bit错误，后续组密文解密得到的明文完全错误。

OFB：该组密文解密得到的明文有1bit错误。

CTR：该组密文解密得到的明文有1bit错误。

（3）从错误处理角度，CTR较OFB在哪里具有优势？

OFB串联的加密模块部分不能出错，否则会导致密文无法正确解密，对该部分的校对耗费了更多资源。

3.【工作模式的填充】对于分组密码工作模式，常见的填充方式有ANSI X9.23，ISO 10126， PKCS 7等。

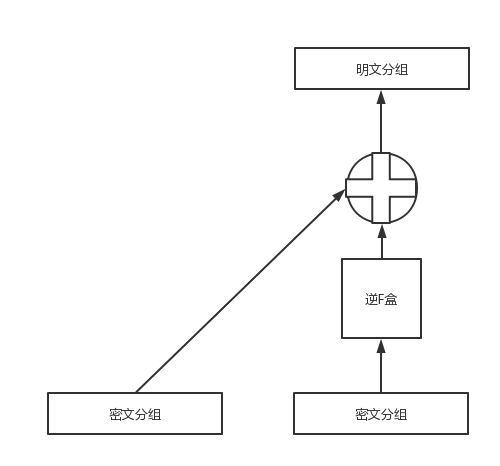
请简述PKCS 7的填充方式，并回答：如果原始明文长度恰是分组大小的整数倍，为什么需要再填充一个分组？

相比于PKCS5，PKCS7可以指定分组大小，其填充方式为：当数据长度不足数据块长度时，缺几位补几个几，如缺少2字节就补充2个0x02。若明文长度为分组整数倍，PKCS7要求再填充一个分组，其最主要的原因在于区分填充数据与原始明文数据，如此条件下明文分组的最后一字节为0x01就可能产生歧义。

4.【CBC Padding攻击】【选做】TLS问世前，实际应用中最主流的CBC工作模式采用常用的PKCS 7填充方法无法抵抗适应性选择密文（CCA2）攻击。假设解密程序对攻击者输入的任何密文会进行如下响应——若该密文解密后满足PKCS7填充规则，不做任何回应，我们记为；若该密文解密后不满足PKCS7填充规则，返回一个Error，我们记为。则对于任意的密文分组，都可以在一个较小的开销内求得其对应的明文分组。我们以AES-128-CBC中间的一个密文分组为例：

（1）选取字节随机串作为（选填或），与拼接后记为并查询Oracle，穷举该随机串的第字节（从第0字节起，下同）直到（选填或），该穷举的迭代次数为次。

（2）根据概率基础知识，我们知道这时明文分组最有可能的情况是第字节为。通过（选填异或或逆盒）运算，可以求出的第字节解密（经过逆盒）后的结果，我们记为。

（3）将与异或，修改所构造的随机串的第字节，此时两分组拼接结果记为。同（1）相同，穷举该随机串的第字节直到（选填或），该穷举的迭代次数为次，这时明文分组最有可能的情况是第字节为。同（2）相同，可以求出的第字节解密（经过逆盒）后的结果。

（4）以此类推，获得。将该字节序列（选填正序或倒序）拼接后与密文串异或，可以求得明文分组。

**注意：**

以上作业请使用**pdf**文档格式提交，于**2023年4月14日（星期五）23:59**之前在OJ系统上提交，并将作业命名为“**学号\_姓名\_密码学第五次作业**”。如“21371234\_张三\_密码学第五次作业”。