作业三

1. 请指出 CFB、OFB、CTR 各自构成的密钥序列产生器。

答:

CFB 模式：CFB 使用前一个加密块的输出作为下一块的输入，经过加密后与明文进行异或操作。具体来说:

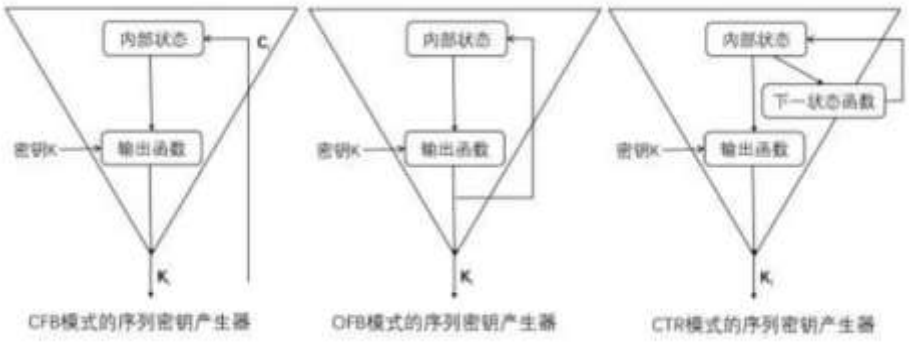
- 将初始化向量作为初始块输入到加密算法。
- 加密后的输出与明文进行异或得到密文，同时加密输出也作为下一个块的输入。

OFB 模式：OFB 密钥序列产生器是基于加密算法的输出直接生成的。与 CFB 的反馈机制不同，OFB 只依赖加密的输出而不是明文。具体来说:

- 将初始向量经过加密算法生成一个加密输出。
- 将此输出与明文异或得到密文。
- 下一轮的加密输入是上一次加密的输出，而不是明文。

CTR 模式：密钥序列产生器基于一个计数器生成。计数器通常是一个递增的数值，每次加密时，计数器的值与密钥一起加密生成伪随机序列。具体来说:

- 初始向量与一个计数器结合，输入加密算法中。
- 加密算法产生的输出与明文进行异或操作，得到密文。
- 计数器递增，用于生成下一个密钥序列。



2. 将 CFB 模式与 OFB 模式进行对比，指出其异同。

答:

相同点：CFB 模式和 OFB 模式针对密文位被删除或增加时都造成后续解密失败，要求同步。

不同点：

CFB 模式:

（1）自同步序列密码;

（2）错误传播：如果一个密文位在传输过程中被修改，则之后的 d 位密文的解密都会错误，且接受者无法确定修改的位置，但随后又能进行正确解密了;

（3）因为每个明文位影响随后的密文，明文的统计特性大大消弱，因此，比 OFB 模式更好地抗击明文冗余攻击;

（4）不可以从明文中间开始加密;

（5）适合应用通信线路好的应有环境。

OFB 模式:

（1）同步序列密码;

（2）错误传播：如果一个密文位在传输过程中被修改,不影响其它密文位的解密，同时，容易确定修改的位置;

（3）可以预先计算出密钥流，当信息到达时就可直接异或产生密文；

（4）可以从明文中间开始加密；

（5）适合应用通信线路差的应用环境。

3. 将 OFB 模式与 CTR 模式进行对比，指出其异同。

答:

相同点：OFB 模式和 CTR 模式都是同步序列密码。

不同点：CTR 基本具备所有 OFB 的特点，但不同有如下:

（1）CTR 可以以任何次序处理分组，也就是支持并行计算；

（2）在 OFB 模式中，如果对密钥流的一个分组进行加密后其结果恰巧和之前加密分组是相同的，那么这一分组之后的密钥流就变成同一值的不断反复，而 CTR 模式不存在这个问题。