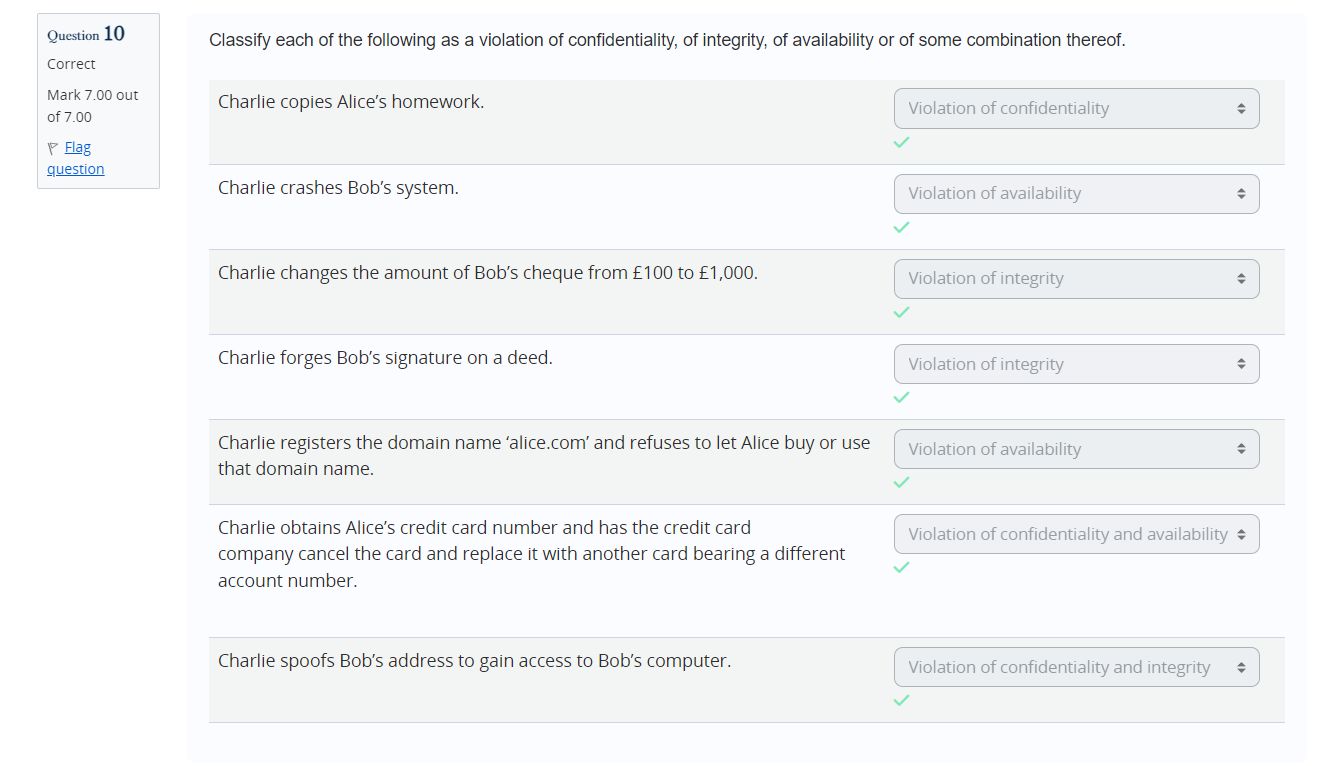
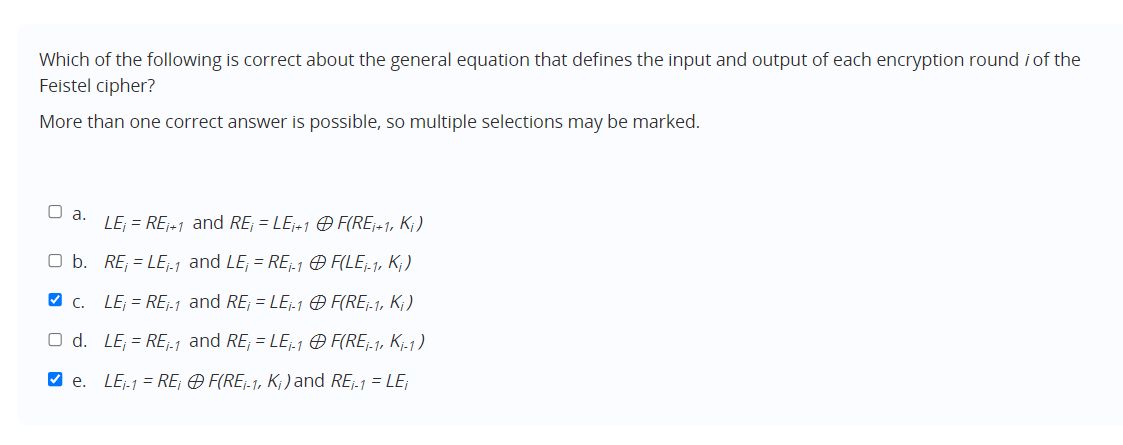
## Week 1

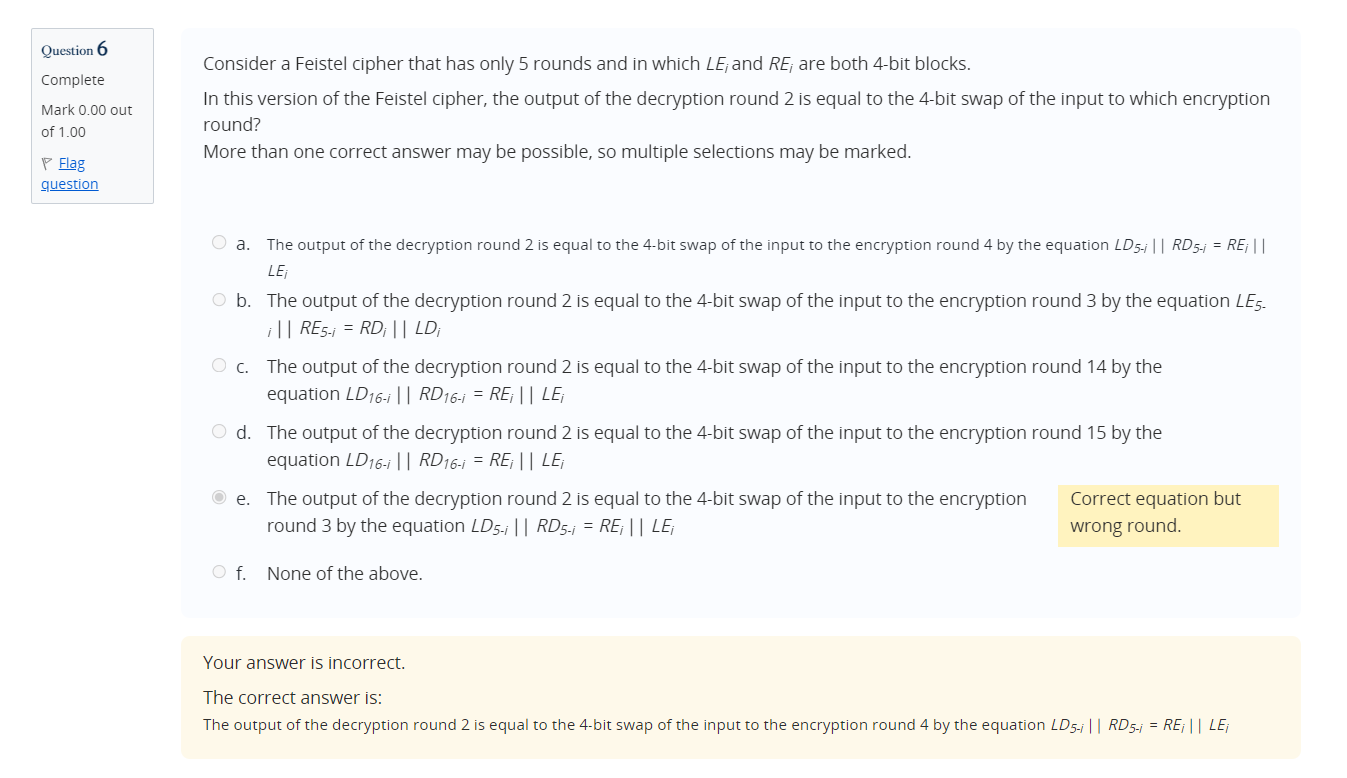


1. 违反保密性，因为本应该是私人的作业被C看到了
2. 违反可用性，系统崩溃因此无法使用
3. 违反完整性，数据被篡改，不再是原来是数据因此不再完整
4. 违反完整性，伪造签名，因为不是本人亲自签署，因此该契约不再完整（完整的契约应该是双方本人签署）
5. 违反可用性，Alice 被拒绝访问与她的名字相匹配的域名，这可能被视为阻止她使用潜在的个人或品牌相关资源。
6. 违反保密性和可用性，信用卡号码被得知（因此违反保密性），同时信用卡被注销，违反可用性
7. 违反保密性和完整性，Bobs的个人电脑被通过欺骗地址的方式侵入，因此违反保密性，同时，可能C会进行损害性行为因此违反完整性。

## Week 4



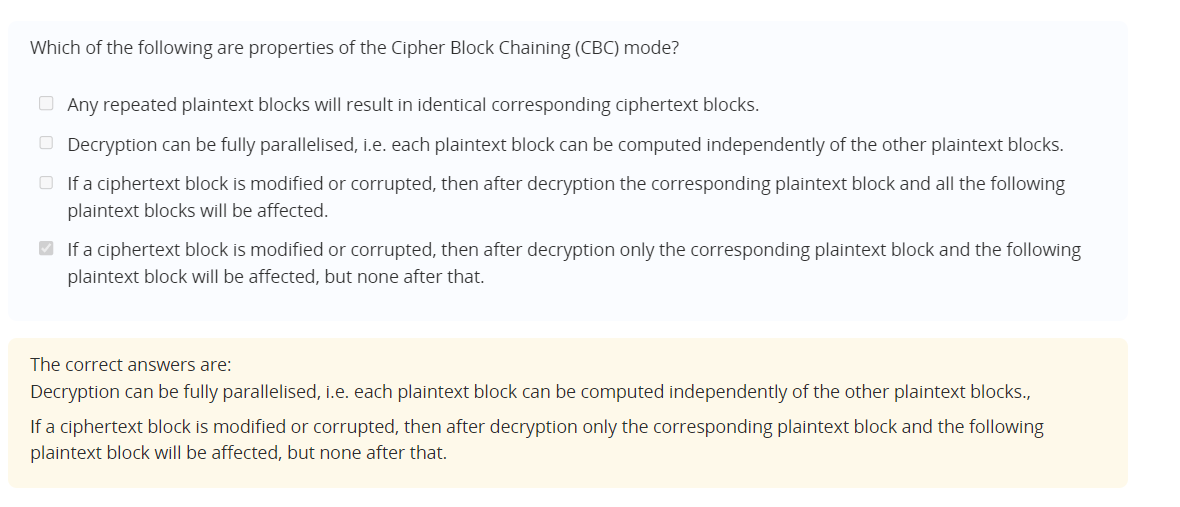
E也是对的，原因在tutorial 4的sheet上有



这里答案应该是A

解题思路如下





如下图所示，和加密不同，我们并不需要一个一个加密已获得帮助下一个明文块加密的密文块。解密的时候，我们实际上已经拥有了所有的密文块，而解密只是需要当前的密文块和前一个密文块XOR而已，所以理论上我们可以有无数个thread同时解密，他们所需要做的只是读取他们所需的两个密文块而已。而这也是为什么如果密文块出现问题，他只影响两个block，因为只会影响它本身（无法正确解密原来的内容）以及下一个密文块（因为需要XOR），但是在之后的密文块并不需要用到有问题的密文块，而有问题的密文块的下一块密文块也只是因为XOR的结果有问题所以无法正确解密，而不是密文块本身的内容有问题，所以不影响和下下个密文块XOR。

