对称密钥加密

C1.1. 使用相同的密钥和相同的算法对消息进行两次加密，但密文不同。可能是什么原因？

C1.2. Enigma 密码机如何缓解单表替换密码容易遭受频率分析的问题？

C1.3. AES 是分组密码。能否把它当作流密码使用，逐位加密消息而无需填充？

C1.4. 为什么 ECB 模式不安全？

C1.5. 使用 ECB 模式，学生发现如果使用高分辨率的 BMP 文件，加密的结果看起来也像噪音。请解释一下。

C1.6. 59 字节的消息使用 AES 和 CBC 模式加密。填充方案为 PKCS#7。请描述填充数据是什么。如果这条消息有 64 字节怎么办？

C1.7. Alice 使用计数器（CTR）模式加密消息，并且将其发送给鲍勃。马洛里截获了密文。虽然她不知道整个消息，但她知道第 17 个字节明文的值为 1；她想将值更改为其他值（其余消息不应更改）。马洛里不知道加密密钥，所以她只能修改密文。(1) 她怎么能这么做呢？(2) 如果马洛里愿意将值从 1 更改为 9，她怎样才能成功实现这一点吗？

C1.8. 要检测密文是否被他人篡改，应使用什么加密模式？

C1.9. 需要加密数据包的有效载荷，同时保护整个数据包（包括头部）的完整性。应使用什么加密模式？

C1.10. Alice 使用 OFB 模式加密发给 Bob 的电子邮件，却始终重复使用同一个 IV。Charlie 得到其中一封邮件的明文和密文。他能否解密 Alice 的另一封加密邮件？请说明理由和方法。

C1.11. Alice 使用 OFB 模式加密她发送给 Bob 的电子邮件，但她总是使用相同的 IV 来代替随机生成的 IV 加密她的电子邮件。查理以某种方式获得了以下数据：

- 第一个密文块的前 8 位：`0x11010101`
- 第一个明文块的前 8 位：`0x01111001`
- 第二个密文块的前 8 位：`0x10100100`

- 第二个明文块的前 8 位：`0x11001010`

查理还获得了爱丽丝新加密的消息的副本，前 8 个前两个块的位是 `0x01010010` 和分别为 `0x01101001`。请导出前两个块的前 8 位明文。

C1.12. 加密机利用 CBC 模式对数据进行加密。给定明文，它可以生成密文。四号用于不同消息的是执行加密的时间。时间是纪元时间，即秒数自 1970 年 1 月 1 日 00:00:00 GMT 起过去。爱丽丝使用了加密机器在时间 T（鲍勃知道时间 T）加密一个秘密数字。鲍勃也知道爱丽丝的密文 G。而且，他知道爱丽丝的秘密数字是 A、B 或 C。他怎样才能算出 Alice 的数字到底是多少？秘密号码是？请描述鲍勃应该做什么（假设所有数字正好是 128 位，这是密码的块大小）。

C1.13. 这个问题类似于问题 C1.12.，除了加密机使用的加密模式是 OFB 模式。鲍勃能找到爱丽丝的秘密号码吗？

C1.14. Alice 使用 AES 的 CBC 模式与 Bob 通信，并为每条消息随机生成一个新的 IV。她知道 IV 可以明文发送，否则 Bob 无法解密。然而，Alice 决定先把 IV 作为第一个明文分组放到消息开头，再加密这条组合消息。她认为这样不会有害，甚至可能更安全。你同意吗？这种做法安全吗？

C1.15. Alice 使用 AES 加密消息并把密文发给 Bob。传输过程中，第三个密文分组的第 2 位发生翻转。分别采用 CBC、CFB、OFB 或 CTR 模式时，Bob 还能正确恢复哪些明文？

C1.16. Alice 使用 AES 加密消息并把密文发给 Bob。计算第三个分组时发生故障，导致该分组 AES 输出的第 2 位损坏，其余计算不受影响。分别采用 CBC、CFB、OFB 或 CTR 模式时，Bob 还能正确恢复哪些明文？

C1.17. 加密机使用 CBC 模式和固定的秘密密钥 K 加密消息 P。Bob 知道密文 C 和加密使用的 IV。加密机提供填充检查功能：输入 IV 和密文后，它会解密并告知填充是否有效，但不会返回明文。请说明如何利用该功能解密 C。只需详细说明如何恢复第二个明文分组的最后三个字节（P 共 10 个分组）。

C1.18.（愚人节恶作剧题☺☺☺）：请描述一种先用 DES 加密消息，再用 AES 解密的方法。