作业：AES实现

作者：王硕

Mail：[kyiwong97@gmail.com](mailto:kyiwong97@gmail.com)

Tel ：13026994661

环境：Python 3.7.4

AES128Encode：AES128加密

AES128Decode：AES128解密

图片题目来源：课本P119 5.3.6 AES举例例题

特别说明：课本中，中间参数错误，不过结果没有错。

AES明文按列输入，密文按列输出，在程序中，为了符合从左至右从上至下的习惯，选择了密文按行输出结果，具体结果可与课本P120结果对照。（按列输出可以实现，但是不符合习惯，故舍去）

在AES解密脚本中，实现了通用字节乘法运算(函数：Invchen)，其它模块与加密大致相同，不再作解释。