

代码2-10 明文加密问题求解

In [27]:

```
1 import numpy as np # 导入numpy工具包
2 X = np.array([ # 创建ndarray类对象X (对应一个3*3的加密矩阵)
3     [1, -1, 2],
4     [-2, 3, -3],
5     [2, -2, 1]
6 ])
7 X_inv = np.linalg.inv(X) # 调用np.linalg.inv函数计算X的逆矩阵并将逆矩阵保存到X_inv
8 A = np.array([ # 创建ndarray类对象A (对应一个5*3的明文矩阵)
9     [73, 32, 108],
10    [105, 107, 101],
11    [32, 80, 121],
12    [116, 104, 111],
13    [110, 33, 0]
14 ])
15 )
16 B = A@X # 通过A@X矩阵乘积计算得到密文矩阵B
17 print('密文矩阵: \n', B)
18 C = B@X_inv # 通过B@X_inv计算还原明文矩阵
19 print('还原的明文矩阵: \n', np.around(C, 0)) # 通过np.around函数将C中元素四舍五入只保留整数部分
20
```

密文矩阵:

```
[[ 225 -193  158]
 [  93   14  -10]
 [ 114  -34  -55]
 [ 130  -26   31]
 [  44  -11  121]]
```

还原的明文矩阵:

```
[[ 73.  32. 108.]
 [105. 107. 101.]
 [ 32.  80. 121.]
 [116. 104. 111.]
 [110.  33.   0.]]
```