现代密码学作业——第三讲

1、O(n2) 不是多项式的

2、

（1）

1. **def** super\_increasing\_knapsack(A, S):
2. **def** backtrack(curr\_set, curr\_sum, index):
3. **if** curr\_sum == S:
4. solutions.append(curr\_set)
5. **return**
6. **if** curr\_sum > S **or** index >= len(A):
7. **return**
8. **for** i **in** range(index, len(A)):
9. backtrack(curr\_set + [A[i]], curr\_sum + A[i], i + 1)
11. solutions = []
12. backtrack([], 0, 0)
13. **return** solutions

（2）O(n\*S)

3、

我国密码行业标准SM4的密钥长度为128位。

现代的个人电脑CPU的运算速度大约在几十GHz到几百GHz之间。为了进行估算，我们可以假设一个中等性能的个人电脑CPU每秒可以进行1010次操作。

穷尽搜索对于128位密钥，可能的密钥总数为2128。要计算最坏情况下获得密钥所需的时间，我们需要将可能的密钥总数除以每秒可以尝试的密钥数量：

所需时间= 2128/1010

这个数字是非常巨大的，因此目前通过穷尽搜索来破解128位密钥是不现实的。