现代密码学

第三讲

作业

1 求冒泡排序法的计算复杂度, 该算法是否为多项式的?

2 超递增背包问题:

设A=(a_1,a_2,…,a_n)是由n个不同的正整数构成的n元组，且 $a_j > \sum_{i=1}^{j-1} a_i \quad j = 2,\cdots,n$

S是另一已知的正整数。

求A的子集A’，使 $\sum_{a_i \in A'} a_i = S$.

(1) 给出该问题的求解算法;

(2) 求算法的计算复杂度.

作业

3 调研我国密码行业标准SM4的密钥长度，以及目前个人电脑的计算性能，从穷尽搜索的角度（已知明密文对），最坏情况下需要多久才能获得密钥。