**第七章 公钥密码体制**

一、术语解释

1、公钥密码体制：

2、陷门单向函数：

3、大数因子分解问题：

4、离散对数问题：

5、背包问题：