问题1：假定口令长度为6个字符，可以使用字母和数字，区分大小写。在以下条件下，蛮力攻击平均所需要的时间分别为多少？检查一个口令需要1/10秒。检查一个口令需要1 微秒。

问题2 假定你只允许使用26个字符来构造长为n的口令。进一步假设你在区分大小写和不区分大小写的两个系统中使用了此口令，试给出猜测出大小写区分的口令所需要的最大尝试次数。

问题3： 口令是由用户输入并由计算机检查是否合法。因此， 在用户和计算机之间一定有通信的通道（包括远程的通信）。到目前为止，我们一直非常抽象地看待这个通道，假设他们存在并且足够安全。那么什么时候这种假设是合理的？什么时候这种假设是不合理的？

问题1：假定口令长度为6个字符，可以使用字母和数字，区分大小写。在以下条件下，蛮力攻击平均所需要的时间分别为多少？检查一个口令需要1/10秒。检查一个口令需要1 微秒。

答：(1)62 个字符 , 626个可能的密码。

(2)平均每次蛮力攻击时要检查一半的口令空间。

(3) 1/10 s: 626 ×1/2×1/10 s = 90 y。大约90年

1 us时: 626 ×1/2×10-6 s = 8 h。 大约8小时

问题2 假定你只允许使用26个字符来构造长为n的口令。进一步假设你在区分大小写和不区分大小写的两个系统中使用了此口令，试给出猜测出大小写区分的口令所需要的最大尝试次数。

答：(1)先在不区分大小写系统尝试：26n次；

(2)尝试该n位序列的大小写状态： 2n 次；

(3) 26*n*次+ 2*n* 次;

问题3： 口令由用户输入并由计算机检查。因此， 在用户和计算机之间一定有通信的通道(也包括远程的通信)。到目 前为止，我们一直非常抽象地看待这个通道， 假设他们存在并且足够安全。什么时候这种假 设是合理的？什么时候是不合理的？

答：无线通信、公共电话线路、Internet下是不合理的；本机下输入口令、设备间的加密通道下是合理的。