1.

Computer and Network Security

Homework 2

20337025 崔璨明

Problem 1

上述协议不能完全防止作弊。以下是一种攻击方法：

Alice 在第一步发送 h(x) 给 Bob 之后，她可以等待 Bob 发送 y 给她之前，选择一个不利于她的策略 x'。然后，当 Bob 发送 y 给 Alice 时，Alice 可以计算出 x' 的哈希值 h(x')，而不是之前选择的 x 的哈希值 h(x)。这样，Alice 就可以在第三步发送 x' 给 Bob，让自己取得胜利。

以下是稍微修改协议的解决方案：

1. A → B: h(x, r)
2. B → A: y, r
3. A → B: x, r

其中，r 是一个随机数，用于增加协议的安全性。通过在第一步和第二步引入随机数 r，可以防止 Alice 利用之前的策略计算哈希值并在第三步中发送不利于她的策略。这样，Bob 在收到 x 和 r 后可以验证哈希值是否与 h(x, r) 匹配，以确保 Alice 没有作弊。

Problem 2

1、设C为攻击者，分别向A、B发送：

$C \rightarrow B : A, N_C, B$

$B \rightarrow C : B, N_B, \{N_C\}_k, A$

$C \rightarrow A : B, N_B, A$

$A \rightarrow C : A, N_A, \{N_B\}_k, B$

$C \rightarrow B : A, \{N_B\}_k, B$

2、修改为（生成一个k'）：

1. $A \rightarrow B : A, N_A, B$
2. $B \rightarrow A : B, N_B, \{N_A, k`\}_k, A$
3. $A \rightarrow B : A, \{N_B\}_{k`}, B$

Problem 4

为了确保用户输入 PIN 的安全性，可以采用以下步骤：

1. 终端随机化键盘布局：终端在每次启动时随机化键盘布局，将字符位置进行随机排列。这样，攻击者无法仅仅根据按键位置推断出用户输入的字符。
2. 使用虚假按键：终端在屏幕上显示一组虚假按键，与实际键盘布局无关。例如，屏幕上显示的数字键盘可能与实际的物理数字键盘布局不同。这样，即使攻击者能够监视输入，也无法确定用户实际按下的是哪个键。

3. 随机化按键显示：终端在屏幕上显示的虚假按键位置随机变化。每次用户输入一个数字，虚假按键的位置就会重新随机排列。这样，攻击者无法根据屏幕上的按键位置与用户按键的对应关系来推断出 PIN。
4. 随机化输入反馈：终端在接收到用户的每个按键输入后，不立即在屏幕上显示相应的字符。相反，终端可以在输入之后的短暂时间内显示一个随机字符或星号来模糊输入。这样，即使攻击者能够观察到屏幕上的内容，也无法准确地确定用户输入的是哪个字符。

Problem 5

1、随机定义一个最高项次数为9的多项式f(x)，然后生成30个数对，将军保存10对，每名上校保存5对，每名职员保存2对。这样，至少有10对，即当碎片密钥数量大于或者等于10时，才可以发射导弹。

2、任意两人都可以确定秘密，则Shamir Screct的多项式为一次多项式，即:
$y = (a_0 + a_1 x) mod 11$ 容易得到对(1,4)、(3,7)、(7,2)都有y=8x+7(mod11)，所以C为间谍，且message为 $a_0 = 8 (mod 11)$ 。

Problem 6

剩余步骤：

4、Victor随机选择数i（i>=1）和一个数j（j<=3），将这两个数发送给Peggy

5、然后Peggy将Vi ,Vj 发送给Victor

6、Peggy检查$V_i^2 == x_i \ mod \ n, V_j^2 == x_j \ mod \ n$

7、重复5次上述步骤

若Peggy不知道正确答案，她随机猜测，正确的概率是$\frac{1}{3}$，而5次都猜对的概率为
$\frac{1}{3}^5 = \frac{1}{243} < 0.01$,所以 Victor 至少有99%可以相信 Peggy 没有撒谎。