Problem 1

1.

不能。因为石头剪刀布的可选择项很少，x 只能是石头、剪刀或布。故当 A 发送 $h(x)$ 给 B 后，B 只需要带入 $h(\text{石头})$ 、$h(\text{剪刀})$ 、$h(\text{布})$ ，与 A 发过来的信息进行对比，就可以轻松判断出 x 的内容，在这种情况下 $hash$ 函数显然是失效的。

2.

增加一个随机变量 m ，将协议修改成如下所示：

$A \rightarrow B$: $h(x+m), h(m)$

$B \rightarrow A$: y

$A \rightarrow B$: x, m

此时，B 将无法通过遍历 x 为石头、剪刀、布的情况得到 x 的内容，而在 A 给出 x、m 的值时候，B 可以验证 A 没有说谎，可以确定 m 没有更改。

Problem 2

1.

该协议很容易受到中间人攻击。假设在 A 和 B 之间有一个 C，攻击如下：

$A \rightarrow C: A, N_A, C$

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

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

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

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

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

此时 A 和 B 分别与不知道密钥的 C 建立了一个认证，但是 A 和 B 之间并没有建立认证。

2.

解决方案如下：

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

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

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

通过将己方名称与 $nonces$ 一起放在加密块内，使得 C 在不知道密钥的情况下无法修改加密的 A 和 B 字段，进而可以有效抵御中间人攻击。

Problem 4

因为用户的输入设备是完全被监视的，所以我们不能通过输入设备泄露任何的信息，但是因为给用户的显示（例如屏幕）是安全的，所以可以利用显示这一方面来展示密码信息。

可以设计这样一个方案：在屏幕上给出乱序字符，用户通过`↑`、`↓`、`←`、`→`键自己选择输入的密码的每一位字符，选中后输入回车。每选择一个字符并输入一次回车后，屏幕上的所有字符随机重排，用户通过`↑`、`↓`、`←`、`→`键继续选择字符。当全部密码输入结束后，连续按两次回车。

在上述方案中，攻击者不能够从键盘输入中获得任何关于密码的信息。相关的密码信息显示在屏幕上，但是因为给用户的显示是安全的，所以攻击者不能从这里获得信息，所以在上述方案上用户能够安全登录。

Problem 5

1.

1. 选取一个随机的9次多项式 p ，令 $p(0)=k$ 。
2. 对$i=1,2,\dots,30$，令$s(i)=f(i)$。
3. 将军决定 $\{s_1,s_2,\dots,s_{10}\}$，第一位上校决定 $\{s_{11},s_{12},\dots,s_{15}\}$，第二位上校决定 $\{s_{16},s_{17},\dots,s_{20}\}$，5个职员分别决定 $\{s_{21},s_{22}\}$、$\{s_{23},s_{24}\}$、$\{s_{25},s_{26}\}$、$\{s_{27},s_{28}\}$和 $\{s_{29},s_{30}\}$。

2.

依题意有，在该系统中$p=11$，$t=2$， $f(x)=y=(kx+b)\ mod\ 11$。

由Shamir secret sharing scheme可知，A、B、C、D 4个点中，除了 外国特工 ，另外3个人应该同时满足上式且唯一确定一组(k,b)，而唯一的外国特工将不满足这组(k,b)。

若由 A 和 B 确定 k 和 b:

将 A,B 代入得:

$$\begin{cases}(k+b)\ mod\ 11=4\\(3k+b)\ mod\ 11=7\end{cases}$$

解得:

$$\begin{cases}k=7\\b=8\end{cases}$$

故有$f(x)=y=(7x+8)\ mod\ 11$，将 C 和 D 代入 $f(x)$ ，发现 C 并不满足 $f(x)=(7x+8)\ mod\ 11$，即 C 是外国特工，$message=f(0)=8$。

Problem 6

1. $Peggy$ 选择3个随机整数 r_1,r_2,r_3，其中 $r_1r_2r_3=x\ mod\ n$。
2. $Peggy$ 计算 $x_i=r_i^2(i=1,2,3)$ 并将 x_1,x_2,x_3 发送给 $Victor$。
3. $Victor$ 检查是否满足 $x_1x_2x_3=s\ mod\ n$。
4. $Victor$ 选择 $i,j\in 1,2,3$ 并将 i,j 发送给 $Peggy$。
5. $Peggy$ 将 r_i,r_j 发送给 $Victor$。
6. $Victor$ 检查是否满足 $x_i=r_i^2\ mod\ n$、$x_j=r_j^2\ mod\ n$。

重复上述操作5次，即可保证有99%的概率任务 $Peggy$ 没有说谎。