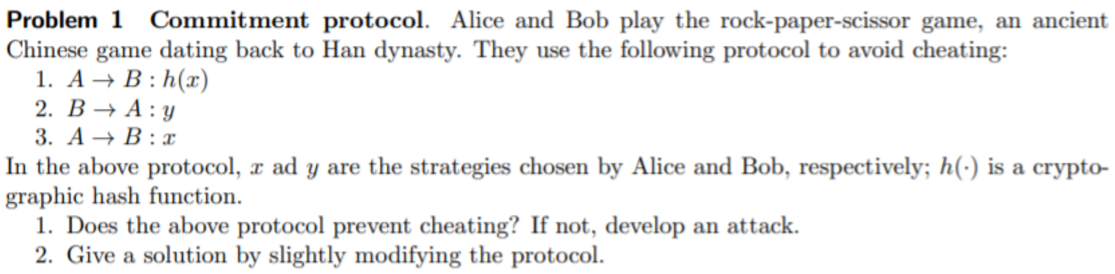
信息安全 作业2

> 姓名：唐瑞怡
>
> 学号：18340159
>
> 专业：计算机科学与技术

本次作业，选择第1、2、4、5、6题进行练习。

Problem 1



Problem 1 Commitment protocol. Alice and Bob play the rock-paper-scissor game, an ancient Chinese game dating back to Han dynasty. They use the following protocol to avoid cheating:

1. $A \rightarrow B : h(x)$
2. $B \rightarrow A : y$
3. $A \rightarrow B : x$

In the above protocol, x ad y are the strategies chosen by Alice and Bob, respectively; $h(\cdot)$ is a cryptographic hash function.

1. Does the above protocol prevent cheating? If not, develop an attack.
2. Give a solution by slightly modifying the protocol.

解：

1. 以上协议不可以防止作弊。

    原因如下：在石头剪刀布游戏中，A可选择的`x`很少，B可以通过简单地列举三种情况并得到它们的哈希值，与A发送的`h(x)`进行比较，哈希值相同的就是A对应选择的`x`。然后B再根据`x`作出相应的`y`即可赢得游戏。

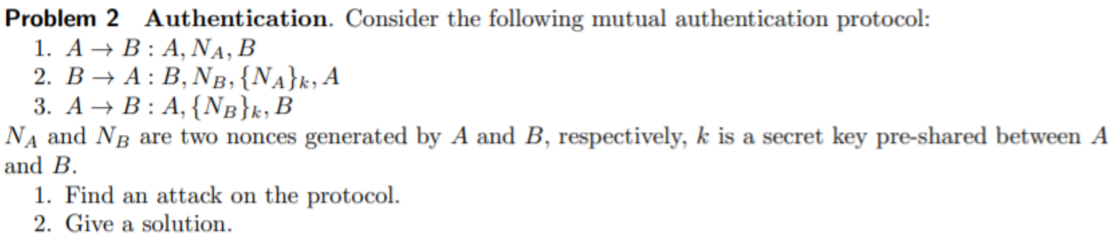
2. 解决方案：

    ```
    1.A->B:h(x+n)， h(n)
    2.B->A:y
    3.A->B:x,n
    ```

    即：A在哈希中引入自己选定的随机数`n`，并将`h(x,n)`和`h(n)`发送给B；然后B将y发送给A；最后A将`x`和`n`发送给B。

    这样，B可以通过`x`和`n`来验证`h(x+n)`和`h(n)`，从而验证A是否作弊。同时，由于A的随机数`n`是A随机选定的，B并不知道`n`的大小，所以B无法通过列举来推测出A选择的`x`，防止了B作弊。因此，双方可以公平进行游戏。

Problem 2



Problem 2 **Authentication**. Consider the following mutual authentication protocol:

1. $A \to B : A, N_A, B$
2. $B \to A : B, N_B, \{N_A\}_k, A$
3. $A \to B : A, \{N_B\}_k, B$

N_A and N_B are two nonces generated by A and B, respectively, k is a secret key pre-shared between A and B.

1. Find an attack on the protocol.
2. Give a solution.

解：

1. attacker C 可以进行“man-in-the-middle”中间人攻击，从而分别向A和B进行认证。

$$\begin{array}{l} 1.\ A \to C : A, N_A, C \\ 2.\ C \to B : A, N_A, B \\ 3.\ B \to C : B, N_B, \{N_A\}_k, A \\ 4.\ C \to A : C, N_B, \{N_A\}_k, A \\ 5.\ A \to C : A, \{N_B\}_k, C \\ 6.\ C \to B : A, \{N_B\}_k, B \end{array}$$

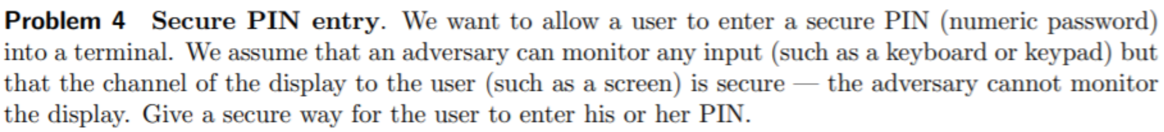
2. 解决方法：

在密钥加密信息中加入身份的信息，从而避免中间人攻击。

$$\begin{array}{l} 1. A \to B : A, N_A, B \\ 2. B \to A : B, N_B, \{N_A, B\}_k, A \\ 3. A \to B : A, \{N_B, A\}_k, B \end{array}$$

如果存在中间人攻击，则第三步A发送给B后，B通过k解密得到 N_B 和 A，B就会发现有中间人C的存在，因此中间人攻击不成立。

Problem 4



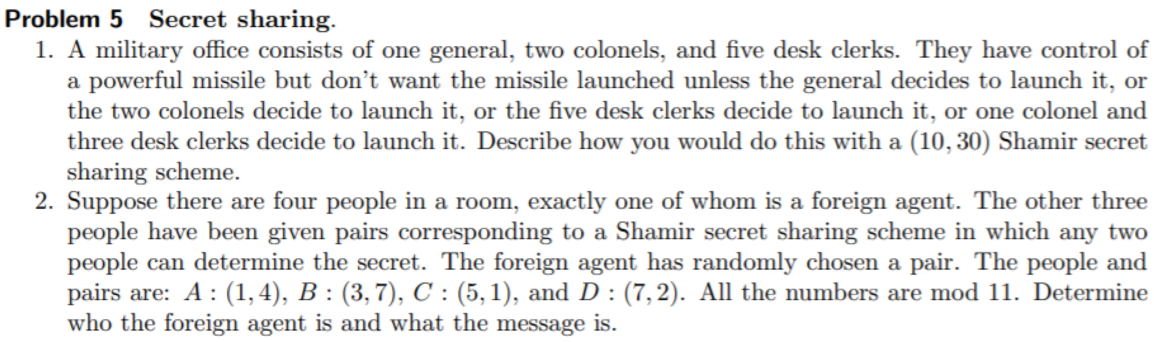
Problem 4 **Secure PIN entry**. We want to allow a user to enter a secure PIN (numeric password) into a terminal. We assume that an adversary can monitor any input (such as a keyboard or keypad) but that the channel of the display to the user (such as a screen) is secure — the adversary cannot monitor the display. Give a secure way for the user to enter his or her PIN.

解：可以通过以下方法来使得用户安全输入：

在显示屏显示一个随机的整数。用户通过使用键盘上的UP或DOWN键来增加或减少它（在0左右循环，即对9进行UP操作会回到0，对0进行DOWN操作会回到9），并按ENTER将该数字作为PIN的输入值，输入到系统中。

此时，adversary只会看到一系列UP和DOWN的操作，但由于其无法获得屏幕上显示的随机整数，所以adversary无法知道PIN，因此是安全的。

Problem 5



Problem 5 **Secret sharing.**

1. A military office consists of one general, two colonels, and five desk clerks. They have control of a powerful missile but don't want the missile launched unless the general decides to launch it, or the two colonels decide to launch it, or the five desk clerks decide to launch it, or one colonel and three desk clerks decide to launch it. Describe how you would do this with a $(10, 30)$ Shamir secret sharing scheme.
2. Suppose there are four people in a room, exactly one of whom is a foreign agent. The other three people have been given pairs corresponding to a Shamir secret sharing scheme in which any two people can determine the secret. The foreign agent has randomly chosen a pair. The people and pairs are: $A : (1, 4)$, $B : (3, 7)$, $C : (5, 1)$, and $D : (7, 2)$. All the numbers are mod 11. Determine who the foreign agent is and what the message is.

1、解：

- 构造一个9次多项式：

$$f(x) = S + a_1x_1 + a_2x_2 + ... + a_9x_9 \ mod\ p，S\text{为} \ secret，p\text{为小于}S\text{的素数}$$

- 碎片share $S_i = f(i)$，其中$i = 1$到30 。且得到**10**块碎片即可解得secret S。
- 根据题意，不妨设general可以得到$S_1 - S_{10}$；两个colonel分别可以得到$S_{11} - S_{15}$和$S_{16} - S_{20}$的碎片；五个desk clerk分别可以得到$S_{21} - S_{22}$，$S_{23} - S_{24}$，$S_{25} - S_{26}$，$S_{27} - S_{28}$，$S_{29} - S_{30}$的碎片。
- 由于获得10块碎片就可以解得secret S，则general有10块碎片，自己就可以解得 S。而两个colonel加起来一共也有10块碎片，也可以解得 S。同理，五个desk clerk加起来也有10块碎片，也可以解得 S。另外，1个colonel和3个desk clerk加起来一共有11块碎片，也可以得到 S。并且可知，该组合少一个colonel或者desk clerk都不可以得到10块碎片，因此无法得到 S。
- 综上所述，用$(10, 30)$的Shamir secret sharing scheme可以解决此问题。

2、解：

- 由题意知：任意两个人就可以得到secret，所以构建1次多项式：

$$f(x) = a_0 + a_1x_1 \ mod(11)，a_0 \ is \ secret$$

- 根据Shamir secret sharing的定义和A、B、C、D的pair可以构造出如下多项式组：

$$\begin{aligned} f(1) =& a_0 + a_1 \ mod(11) = 4 & (1) \\ f(3) =& a_0 + 3a_1 \ mod(11) = 7 & (2) \\ f(5) =& a_0 + 5a_1 \ mod(11) = 1 & (3) \\ f(7) =& a_0 + 7a_1 \ mod(11) = 2 & (4) \end{aligned}$$

- 将上述同余方程组两两组合，求解：
  - (1)+(2)：

$$\begin{aligned} a_0 &\equiv 8 \ mod(11) \\ a_1 &\equiv 7 \ mod(11) \end{aligned}$$

  - (1)+(3):

$$\begin{aligned} a_0 &\equiv 2 \ mod(11) \\ a_1 &\equiv 2 \ mod(11) \end{aligned}$$

  - (1)+(4):

$$\begin{aligned} a_0 &\equiv 8 \ mod(11) \\ a_1 &\equiv 7 \ mod(11) \end{aligned}$$

  - (2)+(3):

$$\begin{aligned} a_0 &\equiv 5 \ mod(11) \\ a_1 &\equiv 8 \ mod(11) \end{aligned}$$

  - (2)+(4):

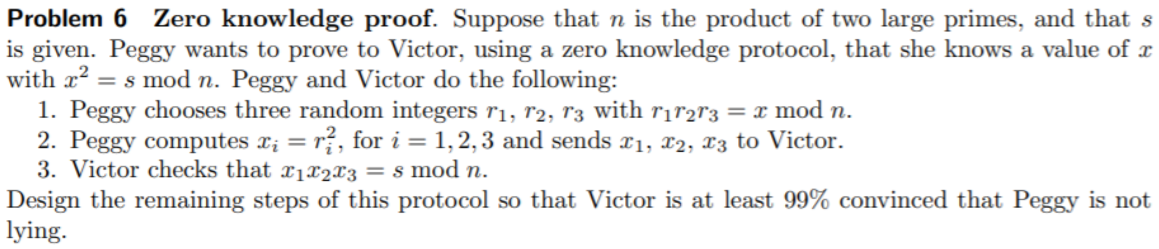
$$a_0 \equiv 8 \; mod(11)$$
$$a_1 \equiv 7 \; mod(11)$$

  - (3)+(4):

$$a_0 \equiv 4 \; mod(11)$$
$$a_1 \equiv 6 \; mod(11)$$

- 由上述各情况的解可知，(1)+(2), (2)+(4), (1)+(4)组合得到的解是相等的，因此可判断C是外国特工。并且可知message为8.

Problem 6



Problem 6 Zero knowledge proof. Suppose that n is the product of two large primes, and that s is given. Peggy wants to prove to Victor, using a zero knowledge protocol, that she knows a value of x with $x^2 = s \bmod n$. Peggy and Victor do the following:

1. Peggy chooses three random integers r_1, r_2, r_3 with $r_1 r_2 r_3 = x \bmod n$.
2. Peggy computes $x_i = r_i^2$, for $i = 1, 2, 3$ and sends x_1, x_2, x_3 to Victor.
3. Victor checks that $x_1 x_2 x_3 = s \bmod n$.

Design the remaining steps of this protocol so that Victor is at least 99% convinced that Peggy is not lying.

解：Remaining steps are:

4. Victor sends Peggy $i, j \in 1, 2, 3$.
5. Peggy sends Victor r_i and r_j.
6. Victor checks that $r_i^2 \equiv x_i \; mod \; n$ and $r_j^2 \equiv x_j \; mod \; n$

重复上述步骤5次以上（每次都用新的r_1, r_2, r_3），即可保证有99%以上的把握使得Victor相信Peggy没有撒谎。

原因：通过上述步骤，Peggy撒谎且没被发现的概率是$\frac{1}{3}$，并且5次之后，Peggy撒谎且没被发现的概率为$(\frac{1}{3})^5 < 0.01$，那么Peggy没撒谎的概率达到0.99以上，因此此协议可以保证有99%以上的把握使得Victor相信Peggy没有撒谎。