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.

1、否，B可以通过分别算 h(rock)，h(paper)，h(scissor) 与 h(x) 比对来得知 X

2、 $A \rightarrow B : h(Nonce \| x)$

$B \rightarrow A : y$

$A \rightarrow B : Nonce, x$

A无法修改x，因为很难找到另一个Nonce使 $h(Nonce' \| x') = h(Nonce \| x)$

B难以通过枚举来获得x，因为Nonce可能性很多

Problem 2 Authentication. Consider the following mutual authentication protocol:

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

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.

1、$C \rightarrow B : A, N_C, B$

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

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

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

$C \rightarrow B : A, \{N_B\}_k, B$　　C以A的身份与B验证成功

2、$A \rightarrow B : A, N_A, B$

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

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

此时中间人攻击不成立。因为C想利用一人来替其解码（2，3步）需证明自己有加码能力（1，2步）。

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.

机器先给出一个随机数到屏幕上，user可看到，adversary看不到。user调整随机数使其成为PIN，这样adversary只知道调整是什么，不知道PIN是什么。

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.

设G，C，D是general，colonel，desk clerk的份额

$$\begin{cases} 30 = G + 2C + 5D \\ 10 \le G \\ 10 \le 2C \\ 10 \le 5D \\ 10 \le C + 3D \end{cases}$$

$$\therefore \begin{cases} G = 10 \\ C = 5 \\ D = 2 \end{cases}$$

∴ 份额分别10，5，2，达到门限10发射.

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.

$$\begin{vmatrix} 1 & 4 & 1 \\ 3 & 7 & 1 \\ 7 & 2 & 1 \end{vmatrix} \equiv 5 + 16 - 43 \equiv -22 \equiv 0 \bmod 11$$

∴ C是 foreign agent

$\because \{ 1a + b \equiv 4 \bmod 11$ $\quad \therefore 2b \equiv 5 \bmod 11$

$3a+b\equiv 7 \bmod 11 \quad \therefore b\equiv 8 \bmod 11$

$\therefore$ message 是 8

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 $r_1r_2r_3 = x \bmod n$.
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 $x_1x_2x_3 = s \bmod n$.

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

Victor 随机向 Peggy 要 r_1, r_2, r_3 的一位，Peggy 回答.
如果 Peggy 不知道 x，可以随机找到 r_i, r_j，算出 x_i, x_j，然后用 $x_1x_2x_3\equiv s \bmod n$ 算出第三个 x_k。这样 Peggy 答出的概率是 $\frac{2}{3}$
上述 1.2.3 和补充的全部过程做 12 次
$(\frac{2}{3})^{12} \approx 0.008 < 0.01$
可知 若 Peggy 不知，它只有不到 1% 的概率全回答.
$\therefore$ 有 99% 以上的确信.

$$\frac{x}{(\frac{2}{3})^n(1-x)+x}$$

$$\frac{x}{(\frac{2}{3})^n+(1-(\frac{2}{3})^n)\cdot x} = \frac{1}{\frac{1}{x}(\frac{2}{3})\ \ 1-(\frac{2}{3})^n}$$