信息安全技术作业（三）

中山大学计算机学院　计算机科学与技术

19335174　施天予

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

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. 上述协议无法阻止 cheating。因为第一步 Bob 能获得 h(x)，而石头-剪刀-布游戏中只有三种策略, Bob 可以尝试每一种策略 x 得到 h(x)，并且与 Alice 发来的结果进行匹配, 从而得出 Alice 的策略，所以无法阻止 cheating。

2. Alice 可以在 h 的输入值中添加随机性（n 是一个随机数）

   1. $A \to B : h(x+n), h(n)$
   2. $B \to A : y$
   3. $A \to B : x, n$

这样 Bob 可以通过 x 和 n 来计算 h(x+n) 和 h(n)，从而验证 A 是否作弊。同时由于 Alice 的随机数 n 是 Alice 随机选定的，Bob 并不知道 n 的值，所以 Bob 无法通过枚举来推测出 Alice 选择的 x ，防止了 Bob 作弊。

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. 这个是 Man-in-the-middle attack。假设攻击者为 C，有如下攻击形式：

   1. $A \to C : A, N_A, B$
   2. $C \to B : C, N_A, B$

3. $B \to C : B, N_B, \{N_A\}_k, C$
4. $C \to A : B, N_B, \{N_A\}_k, A$
5. $A \to C : A, \{N_B\}_k, B$
6. $C \to B : C, \{N_B\}_k, B$

这样 C 就获得了 B 的认证。

2. 可以将 A 和 B 的身份信息进行加密用于验证：

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

之前的攻击是 C 将自己的 id 替换了 A 的 id 使得攻击成功，如果用含有随机数和 id 的密文来检验正确性，C 就无法成功攻击了。

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：

可以让显示器显示一个 0-9 的随机数字，用户通过 UP 和 DOWN 键进行增加和减小，按空格确认这个数字，PIN 的每一位数字都如此。最后 PIN 全部确定后按下回车完成输入，就可以保证用户输入的 PIN 是安全的。

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.

解：

1. 随机选择 10 个数作为系数，构造 9 次多项式：

$$f(x) = a_0 + a_1 x + ... + a_9 x^9$$

对于（10，30）的方案，可以随机生成 30 个整数输入 f 得到 30 个数对。给将军分配 10 个，2 个上校每人 5 个，5 个职员每人 2 个，这样有大于等于 10 个数对就能确定 f，可以发射导弹。

2. 由于任意两人可以确定加密信息，所以 Shamir secret 为一次多项式：

$$f(x) = (a_0 + a_1 x) \ mod \ 11$$

可以发现 (1, 4), (3, 7), (7, 2) 都满足 $f(x) = (8 + 7x) \ mod \ 11$，所以 C 是间谍，秘密信息 $a_0 = 8$

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 $r_1 r_2 r_3 = x \bmod n$.
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：

4. Victor 随机选取 $i, j \in \{1, 2, 3\}$ 发送给 Peggy.
5. Peggy 发送 r_i 和 r_j 给 Victor.
6. Victor 验证等式 $r_i^2 \equiv x_i \ mod \ n$ 和 $r_j^2 \equiv x_j \ mod \ n$.
7. 将上述步骤重复 5 次，每次重新选择 r1, r2, r3 ，其中 r1, r2, r3 = x mod n.

显然当 Peggy 撒谎但猜对概率是 $\frac{1}{3}$，重复 5 次的情况下均猜对的概率为 $(\frac{1}{3})^5 = \frac{1}{243} < 0.01$，所以 Victor 至少有 99% 的几率相信 Peggy 没有撒谎。