信息安全技术作业

李钰 19335112

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. 显然上述协议无法阻止 cheating。因为为了验证 Alice 没有修改 *x* 即验证 *h*(*x*) , Bob 必须知道 *h* 。而石头-剪刀-布游戏中总共只有三种策略, *Bob* 可以尝试枚举每一种策略 *x* 并得到 *h*(*x*)，进而与 Alice 发来的结果进行匹配, 从而得出 Alice 的策略，再来决定自己的策略, 所以必定能赢。
2. Alice 在 *h* 的输入值中添加随机性来防止暴力枚举, 例如 Alice 可以在第一步中发送 *h*(*x*+*r*)而非 *h*(*x*) ，其中 *r* 为随机生成的整数，第三步中 Alice 再将 *x* 与 *r* 一起发送给 Bob，这样就可以使得 Bob 无法枚举破解。

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. 我们构造以下攻击：假设攻击者为R，并且它可以截获A，B间通信的信息，则有如下攻击形式

$$
\begin{gathered}
A \to R : A, N_A, B \\
R \to B : R, N_A, B \\
B \to R : B, N_B, \{N_A\}_K, R \\
R \to A : B, N_B, \{N_A\}_K, A \\
A \to R : A, \{N_B\}k, B \\
R \to B : R, \{N_B\}k, B
\end{gathered}
$$

   至此，R 获得了 B 的认证，与 B 建立了通信。

2. 解决以上攻击的方法可以为：

   A 与 *B* 将公开信息进行加密用于验证，即：

$$
\begin{gathered}
A \to B : A, \{N_A\}k, B \\
B \to A : B, NB, \{N_A, B\}k, A \\
A \to B : A, \{N_B, A\}k, B
\end{gathered}
$$

   之前的攻击是 *R* 将自己的 *ID* 替换了 *A* 的 *ID* 使得攻击成功，那么，我们就是用含有*nounce* 和 *ID* 的密文来确定 *ID* 的正确性，这样 *R* 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：因为 PIN 均由数字组成且显示器是安全的，所以可以在显示器上每隔若干，显示一个 0 - 9 的数字，当这个数字是被设置的密码时则按下空格继续输入下一个数字。当密码输入完成时按回车结束即可，这样就可以保证用户输入 PIN 时是安全的。

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. 由 *Shamir* 密钥共享原理，我们随机选择 10 个数作为系数, 即可构造出如下的多项式：

$$f(x) = a_0 + a_1x + \ldots + a_9x_9$$

对于 (10, 30) 的临界点方案，我们随机生成 30 个整数输入到 *f*() 中得到 30 个点。根据题意, 将其中 10 个点分配给将军, 给两个上校每个人各分配 5 个点, 5 人各分配 2 个点，则可知只要有大于等于十个点时就可以确定 *f* ，显然题目要求的情况均可满足。

2. 由于任意两人可以确定加密信息, 因此，*Shamir Screct* 的多项式必定为一次多项式，即可写为:

$$y = (a_0 + a_1x)mod11$$

根据数据分析可以发现 $(1, 4), (3, 7), (7, 2)$都满足 $y = 8x + 7(mod11)$，故 *C* 应为间谍，并且秘密信息可以知道为 $a_0 = 8(mod11)$ 。

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.

解：我们可以设计如下剩余步骤使得满足题目要求：

4. Victor 随机选取一个 *m* ∈ {1, 2, 3} 和一个 *n* ∈ {1, 2, 3} 发送给 Peggy;

5. 之后 Peggy 再发送 r_m 和 r_n 给 Victor;

6. Victor 验证等式 $x_m = r_m^2$和$x_n = r_n^2$ 是否正确;

7. 将上述步骤重复 5 次，每次重新选择r_1, r_2, r_3，并使得$r_1, r_2, r_3 = x(modn)$.

接下来说明如上步骤是可行的：

显然当 Peggy 不知道正确答案时，他随机猜测一个正确的概率是 $\frac{1}{3}$，而在重复 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。