Computer and Network Security: Homework 2

18340052 何泽

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→B:h(x)
2. B→A:y
3. A→B:x

In the above protocol, x ad y are the strategies chosen by Alice and Bob, respectively; h(·) is a crypto- graphic hash function.

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

1. 上面的协议不能阻止欺骗，因为在第一步的时候B获得了h(x)之后，如果将h(x)与h(rock)、h(papar)与h(scissor)比较则可以获知A的策略，故不能阻止欺骗。
2. 若k是一个整数，$k \equiv 0\ mod\ 3$时k为rock，$k \equiv 1\ mod\ 3$时k为paper，$k \equiv 2\ mod\ 3$时k为scissor，第一步改为A→B:h(k)即可

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. 令C为攻击者，分别向A、B发送即可：

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

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

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

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

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

2. 生成一个k'即可：第一步不变，第二步改为：$B \rightarrow A: B, N_B, \{N_A, k'\}_k, A$，第三步改为：$A \rightarrow B: A, \{N_B\}_{k'}, B$

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.

- 首先在显示器上显示一个随机的顺序，用户按照这个顺序输入
- 其次，输入的数字也要改变：若用户想输入的数字为a，则先随机生成一个加盐值b，接下来用户输入(a+b)mod10

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. 首先随机定义一个最高项次数为9的f(x)，然后生成30个数对，将军保存10对，每名上校保存5对，每名职员保存2对，至少有10对才可以发射导弹。

2. 使用几何思想，而不用interpolation polynomial，各share可以看成平面上点的坐标，那么其余三个人在一条直线上，为了判断这个，使用三角形行列式公式计算面积，若结果为0则代表在一条直线上，那么另一个就是foreign agent。

   首先计算A，B，C：$det\begin{vmatrix}1 & 4 & 9\\3 & 7 & 1\\5 & 1 & 1\end{vmatrix} = 7+20+3-35-12-1 = -18 \equiv 4\ mod\ 11 \neq 0$

   故A，B，C不在一条直线上，则foreign agent是这三个中的一个，

   接着计算A，B，D：$det\begin{vmatrix}1 & 4 & 9\\3 & 7 & 1\\7 & 2 & 1\end{vmatrix} = 7+28+6-49-12-2 = -22 \equiv 0\ mod\ 11$

   结果为0，故A，B，D在一行，**故C为foreign agent**。

   接下来计算message：

$$\begin{cases} 4 = 1m + k \\ 7 = 3m + k \end{cases}$$ 可解得：$8 \equiv k \ (mod\ 11)$

故message为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 x2 = s mod 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 mod 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 mod n.

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

4. Victor随机选择一个大于等于1的数i和一个小于等于3的数j，将这两个数发给Peggy
5. Peggy将V_i ,V_j 发给Victor
6. Peggy检查$V_i^2 \equiv x_i \ mod\ n$ ， $V_j^2 \equiv x_j \ mod\ n$
7. 将上述步骤重复5次