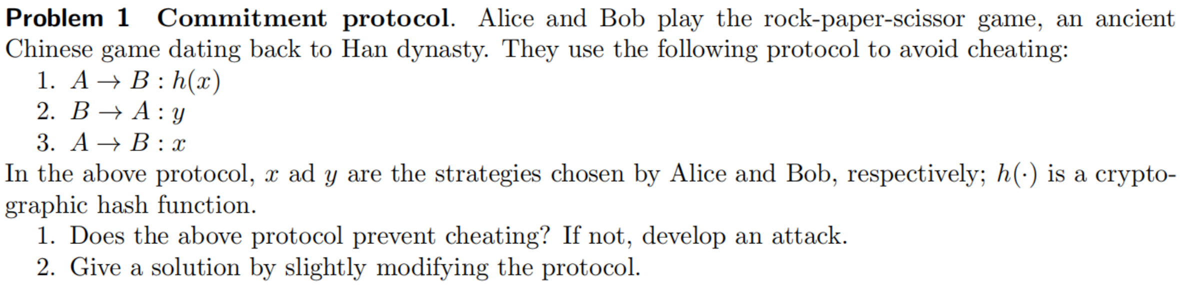
Computer and Network Security: Homework 2

18340013 陈琮昊



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.

Answer：

1.不能阻止欺骗，攻击的情况如下：

$A \to B : h(x)$ Alice写了一个动态的x并签名，把这份承诺发送给Bob。

$B \to A : y$ Bob向Alice透露了他的行动，但没有签署承诺。

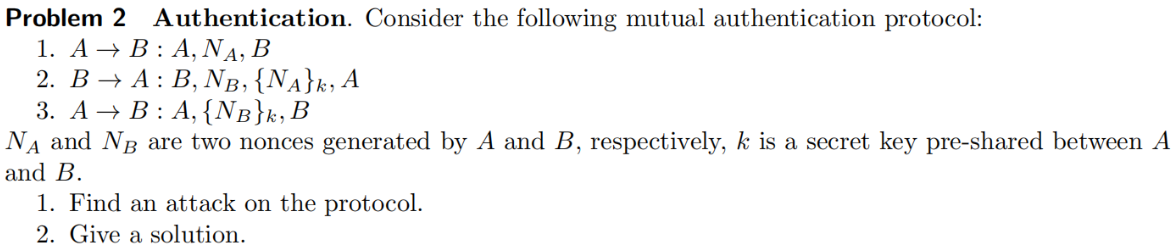
$A \to B : x$ Alice提供了一个钥匙给Bob，让他在这里披露她的承诺。

Bob在看到Alice的举动后，可以尝试改变自己的行动，因为他并没有签署他的承诺给Alice。

在这种情况下，Alice不能阻止Bob的欺骗。

2.修改协议如下：

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



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.

Answer：

1.攻击如下：

1.攻击者C发了一个消息给B，里面有nonce（N_A），这样B就会以为是A发来的消息。

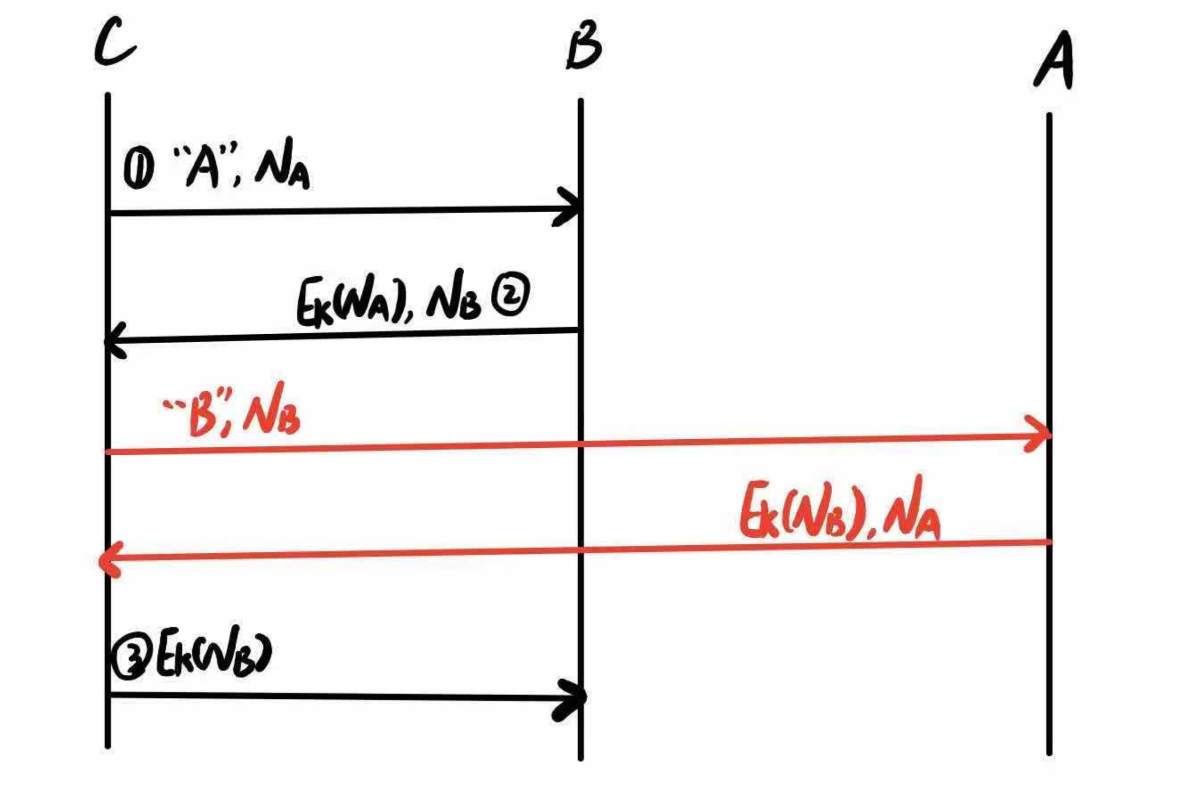
2.B发送给C加密后的$E_k(N_A)$和自己产生的nonce（N_B）。

3.这样的话，C就可以通过N_B联系A，宣称自己是B。

4.A会给C回应$E_k(N_B)$和自己的nonce（N_A）。

5.C将刚刚得到的$E_k(N_B)$发给B。

通过上述步骤，可以看到C和B完成了题目所给的`protocol`。即C完成了一次攻击。

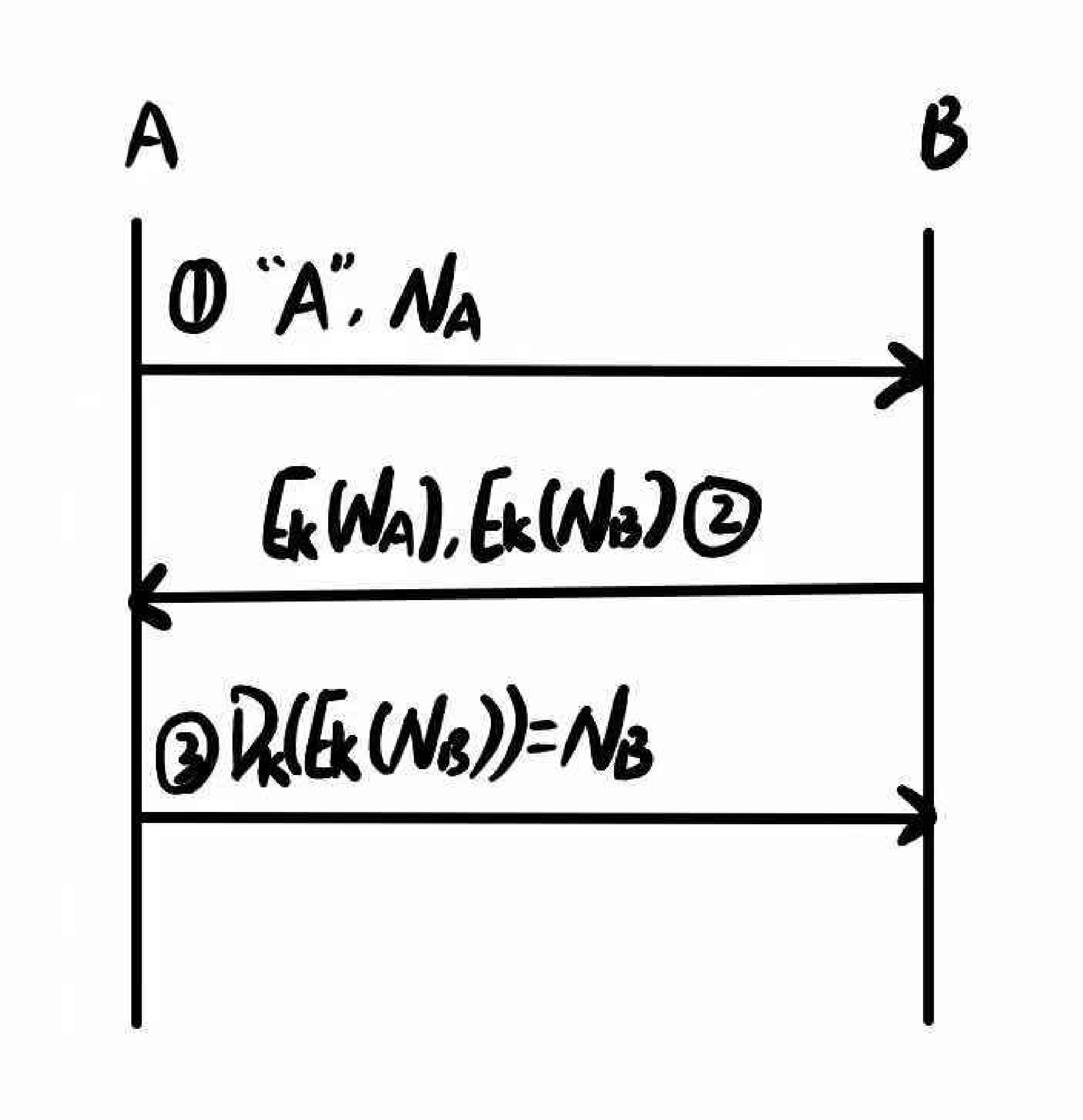


2.解决方案：

1.A发送自己产生的nonce(N_A)给B

2.B发送加密后的$E_k(N_A)$、$E_k(N_B)$给A

3.A通过共享密钥进行解码：$D_k(E_k(N_B)) = N_B$再发回给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.

Answer：

根据题意不能直接输入某个整数，因此我们可以让屏幕随机显示一个整数。用户通过按上下键（↑↓）来进行选择，选择好数字后，按`ENTER`键将该数字作为`PIN`。显然这是可行的，因为对手并不能监控屏幕。

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.

Answer:

1.设T为门槛，G,C,D分别为每个`general`，`colonel`，`desk clerks`的`shares`。根据题目里的4个要求有：

$$T \le G$$
$$T \le 2C$$
$$T \le 5D$$
$$T \le C + 3D$$

还有：

$$T = 10$$
$$G + 2C + 5D = 30$$

可以解得$G = 2C = 5D = 10$，即$G = 10, C = 5, D = 2$，此时也满足$10 = T \le C + 3D = 11$

故每个`general`为10个`shares`，每个`colonel`为5个`shares`，每个`desk clerks`为2个`shares`。

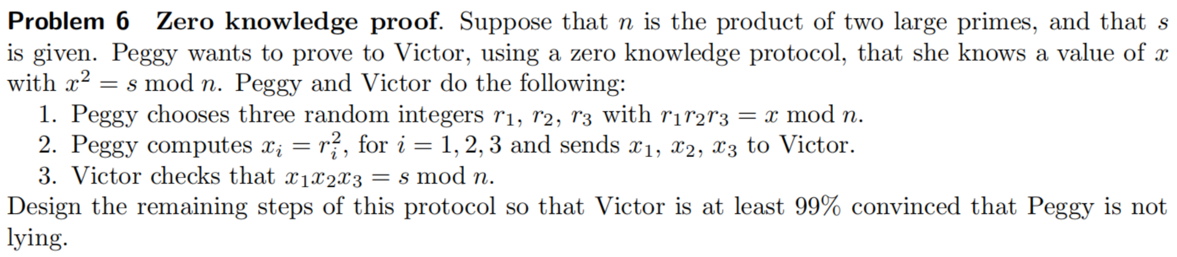
2.根据题意，可以简单的理解为：如果某三者的`pairs`共线，那么另一个就是`foreign agent`。但是所给`pairs`是$mod11$之后的结果，无法直接判断是否共线。因此通过模运算将`pair`的第二个元素调整为由$A \rightarrow D$单调递增且最接近（因为由$A \rightarrow D$第一个元素是单调递增且间隔相等）。根据这一想法将C由$(5,1)$调整为$(5,12)$，将D由$(7,2)$调整为$(7,13)$。这时$A(1,4), B(3,7), C(5,12), D(7,13)$。根据题意假定$A$、$B$决定一条直线，那么会发现$D$在该直线而$C$不在，同理，进行多次检验后发现只有$A$、$B$、$D$能在一条直线上，因此$C$是`foreign agent`。

根据题意，设$y = ax + b$，选择A和B二者的数据代进去得到：

$$4 = a + b①$$
$$7 = 3a + b②$$

① $\times\ 3 -$ ②得：$2b \equiv 5(mod11)$，故$b \equiv 8(mod11)$

所以`secret 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 $r_1 r_2 r_3 = x \bmod n$.
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.

Answer:

Victor将1，2，3中的任意两个数发给Peggy，不妨设这两个数为$i, j(i, j \in${1,2,3})。然后Peggy发送给Victor对应的r_i, r_j，Victor验证$r_i^2 \equiv x_i, r_j^2 \equiv x_j$。重复这样的过程5次（每次都更新$r_1, r_2, r_3$）。显然Peggy说谎的概率为$(\frac{1}{3})^5 < 1\%$。这样便达到了题目的要求。