Computer and Network Security: Homework 2

Instructions

- Please answer 5 of the 6 problems. All questions are weighted equally.
- Please send your solution to $2160853158@qq.com$ by July. 10 midnight.

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.

Answer:

1. 这个协议不能阻止作弊。

原因:

因为Alice发出的x只能是rock,paper,scissor其中的一个,在第1步（$A \rightarrow B : h(x)$）,Bob收到h(x)后可以将rock,paper,scissor分别带入$h(\cdot)$， 再与 $h(x)$比较,哪一个相等就说明Alice出了对应的x。

攻击方案:

(1)在第1步（$A \rightarrow B : h(x)$）,Bob收到h(x)后可以将rock,paper,scissor分别带入$h(\cdot)$， 再与

$h(x)$比较,哪一个相等就说明Alice出了对应的x。

(2)Bob知道了Alice出的x，就可以选择能赢Alice的y。

2. 改进协议以防止作弊:

改进协议：

1. $A \rightarrow B : h(x||r)$
2. $B \rightarrow A : y$
3. $A \rightarrow B : x$

在改进的协议中，x仍然是Alice的策略，y是Bob的策略，r是Alice选择的一个随机数，$h(\cdot)$是一个加密哈希函数。

改进协议解析：

1. Alice选择她的策略x和一个随机数r，然后计算$h(x||r)$并将其发送给Bob。这里$||$表示字符串的连接操作。
2. Bob在接收到$h(x||r)$之后，选择他的策略y并将其发送给Alice。
3. Alice在接收到Bob的策略y之后，将她的策略x一同发送给Bob。

由于哈希函数的性质，Bob无法从$h(x||r)$中推测出x或r。Bob就无法得知Alice的x和r。从而这个协议实现了避免作弊。

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.

Answer:

1. Find an attack on the protocol.

假设有一个攻击者 C 试图冒充 B 来欺骗 A 、冒充 A 来欺骗 B 并且获得认证。以下是攻击步骤：

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

可以从上述攻击步骤中看出,C成功实现了冒充 B 来欺骗 A 、冒充 A 来欺骗 B 并且获得A和B的认证。

2. Give a solution.

为了防止这种攻击，我们需要确保 A 和 B 在通信过程中能够验证对方的身份。

改进后的协议如下：

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

在改进后的协议中：

- 第一步不变，A 发送它的标识符 A、随机数 N_A 和 B 的标识符 B 给 B。
- 第二步中，B 发送它的标识符 B、随机数 N_B，以及使用共享密钥 k 加密的 $\{N_A, B\}$ 给 A。这个加密消息确保 B 知道 N_A，并且是 B 发出的。
- 第三步中，A 发送它的标识符 A，以及使用共享密钥 k 加密的 $\{N_B, A\}$ 给 B。这个加密消息确保 A 知道 N_B，并且是 A 发出的。

通过这个改进，攻击者 C 无法仅通过拦截和重放消息来冒充 B，因为它无法生成正确的加密消息 $\{N_A, B\}_k$ 和 $\{N_B, A\}_k$。只有真正的 A 和 B 才能生成这些正确的加密消息，从而确保了通信的安全性。

Problem 3 Quotable signatures.

Alice sends Bob a signed email. Our goal is to design a signature scheme that will enable Bob to deduce a signature on a subset of the message. This will enable Bob to quote a signed paragraph from the email where the signature can be verified using only the quoted paragraph. Suppose the email M is a sequence of words $m_1, m_2, \cdots, m_n$. The signature works as follows: (1) Alice has a private key for a standard signature scheme such as RSA, (2) to sign the message M Alice views these n words as leaves of a binary tree, (3) she computes a Merkle hash tree from these leaves and obtains the root hash at the top of the tree, (4) she signs this root hash using the standard signature scheme to obtain a signature S. Alice then sends M along with this signature S to Bob.

1. Bob wants to quote a paragraph from M, namely a consecutive set of words $m_i, m_{i+1}, \cdots, m_j$. Show that Bob can generate a signature on this paragraph that will convince a third party that the paragraph is from Alice. This signature will contain S plus at most $\lceil \log n \rceil$ additional hashes. Explain how Carol verifies the signature on this quoted paragraph, and why Alice's signature cannot be forged on a quotable paragraph, assuming that a proper hash function is used to construct the hash tree.
2. Bob now wants to quote a subset of t words that are not necessarily consecutive. Using the method from (1), what is the worst-case length of the resulting signature as a function of t and n ? In other words, what is the maximum number of hashes that Bob must provide so that a third party is convinced that these words came from Alice.

Answer:

1.

Bob想要引用邮件 M 中的一个段落，即连续的单词序列 $m_i, m_{i+1}, \cdots, m_j$。Bob需要生成一个签名，以便说服第三方该段落来自Alice，并且能够验证签名的有效性。这个签名包含签名 S 加上最多 $\lceil \log n \rceil$ 个额外的哈希值。

- **生成签名过程**：
    i. Bob确定段落的起始和结束位置 (i, j)。
    ii. Bob从Merkle哈希树中提取与该段落相关的哈希值：

        - Bob从根哈希开始，逐级向下移动到达叶子节点对应段落的哈希值。
        - 如果段落的长度超过一个叶子节点，则需要提供额外的哈希值以覆盖所有受影响的叶子节点。
    iii. Bob使用这些哈希值重新计算一个根哈希，作为段落的签名。
- **验证过程（由Carol执行）**：
    i. Carol获得邮件 M 和段落的签名。
    ii. Carol从邮件 M 中提取相同的段落，并使用与Bob相同的方式重建Merkle哈希树。
    iii. Carol使用Bob提供的签名根哈希以及从Merkle哈希树重建的根哈希进行比较。
    iv. 如果两个根哈希相同，则段落的签名验证成功，证明该段落确实来自于Alice。
- **安全性**：
    - Alice的签名 S 是根据整个邮件 M 的根哈希计算的，包含邮件中所有单词的完整性。即使Bob只引用了邮件中的一部分，由于Merkle哈希树的性质，只有与Bob引用段落相关的哈希值会影响到根哈希的计算，而不会影响到其他部分。因此，Alice的签名不能被伪造为引用段落之外的任何其他段落。

2.

Bob现在希望引用邮件 M 中的 t 个单词的任意子集，这些单词不一定是连续的。使用上述方法，最坏情况下，生成的签名长度如何取决于 t 和 n？

- 在最坏情况下，Bob需要提供涵盖 t 个单词所对应的所有叶子节点的哈希值。
- 为了覆盖这些叶子节点，Bob需要提供至多 $\lceil \log n \rceil$ 个额外的哈希值。

因此，最坏情况下，Bob需要提供的签名长度为 S 加上至多 $\lceil \log n \rceil$ 个额外哈希值，以确保第三方能够验证引用的子集确实来自Alice。

这种签名方案通过Merkle哈希树的结构，使得在不影响整体签名安全性的前提下，可以有效地验证引用邮件中任意段落或子集的完整性和来源。

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:

由于攻击者无法监视显示器但可以监视键盘或键盘输入，每次执行一次输入PIN时随机生成一个数字随机排列的虚拟键盘显示在屏幕上，而用户通过物理键盘输入替代数字。以下是具体的设计方案：

1. **显示随机排列的虚拟键盘**：
    - 终端显示一个随机排列的虚拟数字键盘，每次用户输入PIN时这个虚拟键盘的排列顺序都不一样。例如：

```
显示的虚拟键盘:
7 3 1
9 2 6
4 8 5
0
```

2. **用户输入对应的数字**：
    - 用户查看显示屏上的虚拟键盘，并根据实际PIN输入对应的数字。例如，如果用户的实际PIN是1234，而虚拟键盘如上所示，那么用户将按下物理键盘上的以下数字：
        - 1 对应虚拟键盘上的3
        - 2 对应虚拟键盘上的9
        - 3 对应虚拟键盘上的1
        - 4 对应虚拟键盘上的4
3. **终端还原用户的真实PIN**：
    - 终端接收到用户输入的数字后，根据当前显示的虚拟键盘排列顺序，还原用户的实际PIN，并进行验证。

这样，攻击者只能看到用户输入的转换后的PIN，而无法看到映射表，因此无法推测出用户的实际PIN。

并且映射表每次登录时都会随机生成，即使攻击者记录了用户的输入，也无法在下次登录时使用，因为映射表已经改变。

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.

我们需要一个秘密分享方案，使得在以下条件下可以发射导弹：

1. 将军决定发射。
2. 两名上校决定发射。
3. 五名书记员决定发射。
4. 一名上校和三名书记员决定发射。

为了实现这一点，我们可以使用 $(10, 30)$ 的 Shamir 秘密分享方案，如下：

1. **设置:**
    - 设秘密 S 控制导弹发射。
    - 使用一个 (k, n) 的 Shamir 秘密分享方案，其中 $k = 10$（重构秘密所需的最少份额数），$n = 30$（总份额数）。
2. **分配份额:**
    - 将军收到 10 份份额。
    - 每名上校收到 5 份份额。
    - 每名书记员收到 2 份份额。

这样分配份额可以确保在符合以下条件时才能发射导弹。我们来验证每个条件：

1. **将军决定发射:**
    - 将军有 10 份份额，满足阈值 $k = 10$。
2. **两名上校决定发射:**
    - 每名上校有 5 份份额。两名上校共有 $5 + 5 = 10$ 份额，满足阈值。
3. **五名书记员决定发射:**
    - 每名书记员有 2 份份额。五名书记员共有 $5 \times 2 = 10$ 份额，满足阈值。
4. **一名上校和三名书记员决定发射:**
    - 一名上校有 5 份份额，三名书记员有 $3 \times 2 = 6$ 份额。共有 $5 + 6 = 11$ 份额，超过阈值。

这种方案确保只有在符合指定条件时才能发射导弹。

2.

我们有四个人在房间里，其中一人是外籍代理人。其他三人已经获得了对应于 Shamir 秘密分享方案的配对，而外籍代理人随机选择了一对。配对如下：

- $A : (1, 4)$
- $B : (3, 7)$
- $C : (5, 1)$
- $D : (7, 2)$

所有数值都在 mod 11 下进行运算。

任何两个点在 Shamir 秘密分享方案中确定一条直线（1 次多项式），可以用来重构秘密。为了找出谁是外籍代理人，我们需要确定哪三对配对与相同的秘密一致，并检查哪一对不符合。

假设多项式为 $f(x) = ax + b$。对于每对配对 (x_i, y_i)，我们有：

$$y_i = ax_i + b$$

我们需要确定 a 和 b 满足三点的方程，并检查哪个不符合。

1. **从 A 和 B 的配对:**

$$\begin{cases} 4 = a \cdot 1 + b \\ 7 = a \cdot 3 + b \end{cases}$$

解这些方程:

$$4 = a + b \quad (1)$$

$$7 = 3a + b \quad (2)$$

从(2)减去(1):

$$3 = 2a \implies a = \frac{3}{2} \mod 11$$

由于 $\frac{3}{2} = 3 \cdot 2^{-1} \mod 11$，并且 $2^{-1} \equiv 6 \mod 11$（因为 $2 \cdot 6 = 12 \equiv 1 \mod 11$），因此:

$$a = 3 \cdot 6 = 18 \equiv 7 \mod 11$$

使用 $a = 7$ 在方程 (1) 中:

$$4 = 7 + b \implies b = 4 - 7 \equiv -3 \equiv 8 \mod 11$$

2. **验证 C:**

$$1 = 7 \cdot 5 + 8 \mod 11$$

$$1 = 35 + 8 \equiv 43 \equiv 10 \mod 11 \quad (\text{不满足})$$

因此，C 不符合这个解。

3. **检查 D 与 A 和 B:**

$$2 = 7 \cdot 7 + 8 \mod 11$$

$$2 = 49 + 8 \equiv 57 \equiv 2 \mod 11 \quad \text{(满足)}$$

因此，A, B 和 D 的配对是一致的。外籍代理人必须是 C，因为其不符合多项式解。

结论

外籍代理人是 C。从一致的配对 A, B, D 重构的消息（秘密）对应的多项式系数为 $a = 7$ 和 $b = 8$，可以通过代入多项式 $f(x) = 7x + 8$ 验证该秘密。

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 $x^2 = s \mod n$. Peggy and Victor do the following:

1. Peggy chooses three random integers r_1, r_2, r_3 with $r_1 r_2 r_3 = x \mod n$.
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 $x_1 x_2 x_3 = s \mod n$.

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

Answer:

为了设计一个零知识协议，使得Victor至少有99%的概率相信Peggy确实知道一个满足$x^2 \equiv s \pmod{n}$的x，可以借鉴Fiat-Shamir启发式方法并针对这个具体问题进行调整。以下是协议的具体设计：

协议步骤

1. **Peggy的承诺**：
    - Peggy选择三个随机整数r_1, r_2, r_3，使得$r_1 r_2 r_3 \equiv x \pmod{n}$。
    - Peggy计算$x_i = r_i^2 \pmod{n}$，其中$i = 1, 2, 3$。
    - Peggy将(x_1, x_2, x_3)发送给Victor。
2. **Victor的挑战**：
    - Victor发送一个随机挑战$c \in \{1, 2, 3\}$给Peggy。
3. **Peggy的响应**：

- 根据挑战c，Peggy做如下响应：
    - 如果$c = 1$，Peggy发送$(r_1, r_2 \cdot r_3)$给Victor。
    - 如果$c = 2$，Peggy发送$(r_2, r_1 \cdot r_3)$给Victor。
    - 如果$c = 3$，Peggy发送$(r_3, r_1 \cdot r_2)$给Victor。

4. **Victor的验证**：
    - Victor收到Peggy的响应后，进行以下检查：
        - 如果$c = 1$，Victor检查：

$$r_1^2 \equiv x_1 \pmod{n}$$

$$(r_2 \cdot r_3)^2 \equiv x_2 \cdot x_3 \pmod{n}$$

        - 如果$c = 2$，Victor检查：

$$r_2^2 \equiv x_2 \pmod{n}$$

$$(r_1 \cdot r_3)^2 \equiv x_1 \cdot x_3 \pmod{n}$$

        - 如果$c = 3$，Victor检查：

$$r_3^2 \equiv x_3 \pmod{n}$$

$$(r_1 \cdot r_2)^2 \equiv x_1 \cdot x_2 \pmod{n}$$

确保Victor的高置信度

为了使Victor有至少99%的概率相信Peggy没有撒谎，需要多次重复上述协议。每轮协议中，Victor有$\frac{2}{3}$的概率发现Peggy在撒谎，因为有3种挑战，而她需要正确应答每个挑战。

为了确保99%的置信度，我们需要重复协议多次。设重复的轮数为k。Peggy能够欺骗通过所有轮次的概率为：

$$\left(\frac{1}{3}\right)^k$$

希望这个概率小于0.01（1%）：

$$\left(\frac{1}{3}\right)^k < 0.01$$

取对数：

$$k \log\left(\frac{1}{3}\right) < \log(0.01)$$

$$k \log\left(\frac{1}{3}\right) < -2$$

$$k > \frac{-2}{\log\left(\frac{1}{3}\right)}$$

使用$\log\left(\frac{1}{3}\right) \approx -0.477$：

$$k > \frac{-2}{-0.477} \approx 4.2$$

因此，Peggy和Victor应该至少重复协议5次（因为k必须是整数），以确保Victor有至少99%的置信度相信Peggy知道x，使得$x^2 \equiv s \pmod{n}$。