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 Nov. 30 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. $A \to B : h(x)$
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.

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.

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.

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.

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.

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.