Algorithms of Information Security

Exercises for *Cryptographic Protocols*

1. Lamport's one-time password scheme. Let the initial value be $w = 0$. Create a sequence of $t = 10$ values (excluding the initial value), i.e., $H(w), H^2(w) \ldots, H^t(w)$ where the function H is define by

   $$H(w) = w + 3.$$

   Describe two iterations of the Lamport's one-time password scheme.

   Hint: Follow the pseudocode from the 5th lecture.

2. Guillou-Quisquater identification protocol. Let the primes be $p = 569, q = 739$ and assume that $v = 54955, t = 1$ and let the redundant identity of Alice be $J_A = 34579$. Describe the communication between Alice and Bob, if she chooses $r = 65446$ and he selects the challenge $e = 38980$.

   Hint: Follow the pseudocode from the 6th lecture.

3. Schnorr identification protocol. Let the primes be $p = 48731, q = 443$ and assume that $\alpha = 6, t = 8$ and let Alice's private key be $a = 357$. Describe the communication between Alice and Bob, if she chooses $r = 274$ and he selects the challenge $e = 129$.

   Hint: Follow the pseudocode from the 6th lecture.

4. Shamir's Secret Sharing. Let t be 3 and n be 5 and the modulus p be 17. Alice, Bob and Charles were given the following $(x, f(x))$: $(1, 8), (3, 10), (5, 11)$. Calculate the corresponding Lagrange interpolation polynomial and determine the secret.

   [Results: $f(x) = 2x^2 + 10x + 13 \mod 17$ and the secret is equal to 13.]

5. Optional Exercise: Implement Basic Kerberos authentication protocol (simplified).

   Hint: Follow the pseudocode from the 7th lecture.