Problem 1. (Lamport’s protocol) Discuss the following properties of Lamport’s protocol:

a) Show that the one-way function is not required to be secret.

b) Which properties must a hash function fulfill to be usable as a one-way function in the protocol?

c) Propose a function that could be used as the one-way function, assuming that the discrete logarithm is hard to solve in $\mathbb{Z}_p^*$ for a usable $p$. Describe Lamport’s protocol for this special case.

d) How can an attacker get access to a one-time password using an active attack?

Problem 2. (Attacks on identification schemes) Alice and Bob want to use the following identification schemes. Amongst others they are using a hash function $h$, some symmetric encryption $E_k$ and some digital signatures $S_A$ and $S_B$.

a) Alice and Bob use the following fixed password identification scheme.

1) $A \rightarrow B : pwd$

2) $B$ verifies that $h(pwd)$ is equal to a stored version of the hashed password pwd.

Describe a replay attack for a fixed password identification. Can this replay attack be prevented by encrypting the password, i.e., Alice sends $E_k(pwd)$ to Bob?

b) The following challenge-response mutual authentication protocol is given.

1) $A \rightarrow B : r_A$

2) $A \leftarrow B : E_K(r_A, r_B)$

3) $A \rightarrow B : r_B$

Explain how an eavesdropper $E$ can authenticate to $A$ without knowing the symmetric key $K$ by a reflection attack. How can such a reflection attack be avoided? Propose an improved protocol, where $r_B$ is not revealed to an eavesdropper $E$.

c) The following challenge-response protocol based on digital signatures is given.

1) $A \rightarrow B : r_A$

2) $A \leftarrow B : r_B, S_B(r_B, r_A, A)$

3) $A \rightarrow B : r'_A, S_A(r'_A, r_B, B)$
Explain how an eavesdropper $E$ can authenticate to $B$ without signing any message with his own identity by an interleaving attack. How can this attack be avoided?

**Problem 3. (Kerberos with ticket granting server)** We introduce a ticket granting server for the simplified Kerberos protocol. To establish secure unilaterial authentication from $A$ (Alice) to $B$ (Bob) with a trusted authority server $T$ (Trent) and a ticket granting server $G$ (Grant), we use the following parameters:

- $k_{AT}$ is a shared key between $A$ and $T$.
- $k_{AG}$ is a session key for secure communication between $A$ and $G$.
- $TGT$ is a ticket granting ticket to authenticate $A$ to $G$.
- $k_{TG}$ is a shared key between $T$ and $G$.
- $a_{AG}$ is an authenticator between $A$ and $G$.
- $k_{AB}$ is a session key for secure communication between $A$ and $B$.
- $k_{BG}$ is a shared key between $G$ and $B$.
- $ST$ is a service ticket to authenticate $A$ to $B$.
- $a_{AB}$ is an authenticator between $A$ and $B$.
- Time stamps $t_i$ and validity periods $l_i$, for $i = 1, 2, ...$

The sequence of messages to be exchanged by the protocol is provided in the figure below.

![Diagram](diagram.png)

Formulate the corresponding protocol and describe it with the parameters as given above.

---

1Feel free to use textbooks, www, etc.