Cryptography in Networking, Exercises 7 (November 22, 2016)

1) Bob, Ted, Carol, and Alice want to agree on a common cryptographic key. They publicly choose a large prime \( p \) and a generator \( g \) of \( \mathbb{Z}_p^* \). They privately choose random numbers \( b, t, c, a \), respectively. Describe a protocol that allows them to compute a shared secret \( K = g^{bta} \pmod{p} \) in a way that is secure against passive attackers.

2) Consider the following protocol, where \( A \) and \( B \) authenticate each other with the help of a trusted server. \( A \) and \( B \) have secret keys \( K_{AS} \) and \( K_{BS} \), respectively, with the server.

\[
\begin{align*}
1. \ A & \rightarrow \ B: \ A \\
2. \ B & \rightarrow \ A: \ N_B \\
3. \ A & \rightarrow \ B: \ \{N_B\}^{K_{AS}} \ \\
4. \ B & \rightarrow \ S: \ \{A, \{N_B\}^{K_{AS}}\}^{K_{BS}} \\
5. \ S & \rightarrow \ B: \ \{N_B\}^{K_{BS}}
\end{align*}
\]

Develop an attack, where an intruder \( I \) makes \( B \) to accept the run in which \( I \) is masquerading as \( A \). In order to achieve this result, the intruder starts two runs with \( B \), in one of which \( I \) claims to be \( A \).

3) Consider the following key transport protocol which uses public key cryptography:

\[
\begin{align*}
1. \ A & \rightarrow \ B: \ E_B(A, K_{AB}, N_A) \\
2. \ B & \rightarrow \ A: \ E_A(K_{BA}, N_A, N_B) \\
3. \ A & \rightarrow \ B: \ N_B
\end{align*}
\]

Design an attack, where the adversary \( C \) induces \( A \) to commence the protocol with \( C \), and then starts a protocol run with \( B \) while masquerading as \( A \).

4) Consider the following key transport protocol:

\[
\begin{align*}
1. \ A & \rightarrow \ S: \ A, \{T_A, B, K_{AB}\}^{K_{AS}} \\
2. \ S & \rightarrow \ B: \ \{T_S, A, K_{AB}\}^{K_{BS}}
\end{align*}
\]

\( A \) generates the session key \( K_{AB} \) and sends it to \( B \) via the server \( S \). The protocol uses timestamps. However, there is an attack against the protocol. It assumes that the intruder \( I \) has recorded one earlier protocol run:

\[
\begin{align*}
1'. \ I_B & \rightarrow \ S: \ B, \{T_S, A, K_{AB}\}^{K_{BS}} \\
2'. \ S & \rightarrow \ I_A: \ \{T_S, B, K_{AB}\}^{K_{AS}} \\
1''. \ I_A & \rightarrow \ S: \ A, \{T_S, B, K_{AB}\}^{K_{AS}} \\
2''. \ S & \rightarrow \ B: \ \{T_S, A, K_{AB}\}^{K_{BS}}
\end{align*}
\]

Explain the attack. What has the intruder achieved? What is needed (extra ingredients in the protocol or extra assumptions) in order to prevent the attack?

5) Let us consider Shamir’s \((4, n)\)-threshold scheme with \( p = 23 \). Let us assume that \( x_i = i \) is assigned to \( P_i \) while shares of \( P_2, P_3, P_5 \) and \( P_6 \) are \( s_2 = 10, s_3 = 6, s_5 = 10, s_6 = 20 \). Compute the secret \( s \) and also the share of \( P_4 \).
6) Construct a secret sharing scheme for a group of $n$ people that contains a specific proper subset $A$ such that:

(i) any $k$ shares are sufficient for finding the secret;

(ii) $k - 1$ shares are sufficient if and only if they are all assigned to people in $A$;

(iii) no set of $k - 2$ shares is sufficient for finding the secret.