Exercise 1: Authentication Protocol One

Assume Alice and Bob have a shared strong password: p, and they create an encryption key $k = \text{HMAC}(H(p), t)$ for some secure hash fuction H and the current time t. Consider the following protocol:

$A \to B : A$
$B \to A : t$
$A \to B : \{s, n\}_k$ where $k = \text{HMAC}(H(p), t)$
$B \to A : \{n\}_s$

That is, Alice sends to Bob a secret key s and a random nonce n encrypted with k. Bob replies with n encrypted with s, and they use s as a session key afterwards.

- What are the long-term keys and short-term keys?
- Does this protocol acheive forward secrecy? Why or why not?
- Is this protocol vulnerable to a replay attack if Eve learns both s and $\{s, n\}_k$?

Exercise 2: Authentication Protocol Two

Assume that Alice (A) and Bob (B) both use public key cryptography. They each have a private key and share their corresponding public key with each other over an authentic channel. Let PK_A be Alice's public key and PK_B be Bob's public key.

Alice and Bob then use these keys to exchange a new symmetric key using the following protocol:

1. $A \to B : \{A, N_1\}_{\text{PK}_B}$
2. $B \to A : \{N_1, N_2\}_{\text{PK}_A}$
3. $A \to B : \{N_2\}_{\text{PK}_B}$

Both Alice and Bob then compute a shared symmetric key $K = N_1 \oplus N_2$. (Recall that $\oplus$ is the bitwise binary XOR operation.)

In step 1, Alice generates a random nonce N_1 and sends it to Bob along with Alice's identity, encrypted with Bob's public key. In step 2, Bob generates a random nonce N_2 and sends both N_1 and N_2 to Alice encrypted with her public key. Alice then sends N_2 back to Bob encrypted with his public key.

- What are the long-term keys and short-term keys?
- Does this protocol achieve perfect forward secrecy?
- This protocol is vulnerable to a mafia fraud attack, that is, if Eve can convince Alice to follow this protocol with her, then Eve can convince Bob that Eve is Alice. The first line of this attack is $A \to E : \{A, N_1\}_{\text{PK}_E}$. Write down the rest of the attack.

- Based on the attack that you describe, what is the shared symmetric key that Bob thinks he's exchanged with Alice?
- Amend the original protocol so that it is not vulnerable.

Exercise 3: Kerberos

- What is a ticket in Kerberos and what purpose does it serve?
- What information is carried on a ticket and why?
- What type of key is used to encrypt a ticket
- What is an authenticator in Kerberos and what purpose does it serve?
- What type of key is used to encrypt an authenticator