CSE543/Fall 2018 - Crypto Protocols

Due: Friday, September 7, 2018, 11:59pm — Prof. Trent Jaeger

This homework is worth 30 points toward the Projects Category. Please read the instructions and questions carefully. Be sure to follow the cryptographic notation on Slide 21 of the `applied-cryptography.pdf` Slide Deck (lectures of September 4 and 6). Please submit your answers in PDF form to the dropbox provided via Canvas.

1. (*5pts*) Suppose Alice and Bob have obtained each other's public keys securely. Please write a key agreement protocol that enables Alice and Bob to agree on a session key over an insecure communication channel that fresh and authenticated to be only available to Alice and Bob.

2. (*5pts*) Suppose Alice and Bob each share a symmetric key obtained securely. Please write a key agreement protocol that enables Alice and Bob to agree on a session key over an insecure communication channel that fresh and authenticated to be only available to Alice and Bob.

3. (*5pts*) Suppose Alice and Bob have obtained each other's public keys securely. Suppose Alice wants to send Bob a message m in a manner that protects the secrecy m over an insecure communication channel and enables Bob to validate the integrity and freshness of message m. Write the cryptographic message(s) sufficient to achieve that goal.

4. (*5pts*) Suppose Alice and Bob have agreed on a symmetric key securely. Suppose Alice wants to send Bob a message m in a manner that protects the secrecy m over an insecure communication channel and enables Bob to validate the integrity and freshness of message m. Write the cryptographic message(s) sufficient to achieve that goal.

5. (*7pts*) Suppose that Alice and Bob want to setup a fantasy football league with a twist. In this case, Alice and Bob may pick any players they want - even ones that the other chooses - but, to do that Alice and Bob must keep their player sets secret until after each week. How can Alice and Bob use cryptography in an efficient way to create a message containing their team for the week that the other can verify after the week concludes?

6. (*3pts*) How does the Needham-Schroeder symmetric-key protocol enable validation of integrity of each of the items in the second message in the protocol?