CS361 Questions: Week 10

These questions relate to Modules 12 and 13. Type your answers and submit them on Canvas.

Lecture 53

1. Why is it important for a digital signature to be non reusable?
2. Why is the hash of the message typically signed?
3. What assurance does R gain from the interchange on slide 4?

Lecture 54

1. What is the importance of certificate authorities?
2. In the example on slide 5, why does X sign the hash of the first message with its private key?
3. Why is it necessary to have a hash of Y and K_y?
4. What would happen if Z had a public key for X, but it was not trustworthy?

Lecture 55

1. What happens at the root of a chain of trust?
2. Why does an X.509 certificate include a "validity interval?"
3. What would it mean if the hash and the received value did not match?

Lecture 56

1. What are some protocols previously discussed?
2. What may happen if one step of a protocol is ignored?
3. Why must the ciphers commute in order to accomplish the task in slide 4?
4. Describe how an attacker can extract M from the protocol in slide 6.
5. Describle how an attacker can extract Ka from the protocol in slide 6.

6. Describle how an attacker can extract Kb from the protocol in slide 6.
7. Why are cryptographic protocols difficult to design and easy to get wrong?

Lecture 57

1. Explain the importance of protocols in the context of the internet.
2. Explain the importance of cryptographic protocols in the context of the internet.
3. What are the assumptions of the protocol in slide 6?
4. What are the goals of the protocol in slide 6?
5. Are the goals of the protocol in slide 6 satisfied? Explain.
6. How is the protocol in slide 6 flawed?

Lecture 58

1. Why is it important to know if a protocol includes unnecessary steps or messages?
2. Why is it important to know if a protocol encrypts items that could be sent in the clear?