CS361 Questions: Week 11

These questions relate to Modules 14. Type your answers and submit them on Canvas.

Lecture 59

1. Why might it be difficult to answer what constitutes an attack on a cryptographic protocol?
2. Describe potential dangers of a replay attack.
3. Are there attacks where an attacker gains no secret information? Explain.
4. What restrictions are imposed on the attacker?
5. Why is it important that protocols are asynchronous?

Lecture 60

1. Would the Needham-Schroeder protocol work without nonces?
2. For each step of the NS protocol, answer the two questions on slide 5.

Lecture 61

1. As in slide 5, if A's key were later changed, after having Kas compromised, how could A still be impersonated?
2. Is it fair to ask the question of a key being broken?
3. How might you address these flaws if you were the protocol designer?

Lecture 62

1. What guarantees does Otway-Rees seem to provide to A and B?
2. Are there guarantees that Needham-Schroeder provides that Otway-Rees does not or vice versa?
3. How could you fix the flawed protocol from slide 4?

Lecture 63

1. Why is the verification of protocols important?
2. What is a belief logic?
3. A protocol is a program; where do you think beliefs come in?

Lecture 64

1. What is a modal logic?
2. Explain the intuition behind the message meaning inference rule.
3. Explain the intuition behind the nonce verification inference rule.
4. Explain the intuition behind the jurisdiction inference rule.
5. What is idealization and why is it needed?

Lecture 65

1. Why do you think plaintext is omitted in a BAN idealization?
2. Some idealized steps seem to refer to beliefs that will happen later in the protocol. Why would that be?
3. One benefit of a BAN proof is that it exposes assumptions. Explain that.