Name: Ali Khan
EID: aak849
CS Login: alikhan@cs.utexas.edu
Email: alikhan2010@live.com

CS361 Questions: Week 4
The questions marked with a dagger (†) require external research and may be more extensive and time consuming. You don't have to do them for the assignment but, but do them to increase your competency in the class.

Lecture 53
1. Why is it important for a digital signature to be non reusable?
So the signature cannot be detached and reused for another message
2. Why is it the hash of the message typically signed, rather than the message itself?
So the integrity of the message is protected in addition to separating the signature from the content itself
3. What assurance does R gain from the interchange on slide 4?
The message is sent securely from sender to receiver with proper authentication

Lecture 54
1. What is the importance of certificate authorities?
The necessity for someone to vouch for the accuracy of the binding
2. In the example on slide 5, why does X sign the hash of the first message with its private key?
To clearly articulate the correct trajectory and flow of the image
3. Why is it necessary to have a hash of Y and Ky?
The message certifies the binding of Y to Ky if there exists a hash
4. What would happen if Z had a public key for X, but it was not trustworthy?
There would be a lack of authorization for communication flow

Lecture 55
1. What happens at the root of a chain of trust?
Provides a basis of authority by which other transitive chain of authority of is created
2. Why does an X.509 certificate include a "validity interval"?
To provide start and end times for validity
3. What would it mean if the hash and the received value did not match?
Then there is no communication channel established

Lecture 56
1. What are some protocols previously discussed?
The protocol and policies as they relate to confidentiality
2. What may happen if one step of a protocol is ignored?
Then the entire process might be terminated preventing a breach in the system

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.
The two applications of Ka can "cancel out" leaving M+kb which b can easily decrypt with his own key kb
5. Describe how an attacker can extract Ka from the protocol in slide 6.
In the situation described above, b can easily decrypt with his own key kb
CS361 Questions: Week 4 2
6. Describe how an attacker can extract Kb from the protocol in slide 6.
See response above; same question
7. Why are cryptographic protocols difficult to design and easy to get wrong?
Because there are so many subtleties that can be overlooked

Lecture 57
1. Explain the importance of protocols in the context of the internet.
A protocol is a structured dialogue among two or more parties in a distributed context controlling the syntax, semantics, and synchronization of communication, and designed to accomplish a communication-related function
2. Explain the importance of cryptographic protocols in the context of the internet.
Using cryptographic mechanisms to accomplish some security levels function
3. What are the assumptions of the protocol in slide 6?
The assumption is that each party is authenticated with to other
4. What are the goals of the protocol in slide 6?
The goal is towards the end of confidentiality
5. Are the goals of the protocol in slide 6 satisfied? Explain.
Yes, it uses a sufficient amount of cryptography to achieve its ends
6. How is the protocol in slide 6 flawed?
Its flawed given its two way transitivity

Lecture 58
1. Why is it important to know if a protocol includes unnecessary steps or messages?
To optimize the protocol to ensure its quality and efficiency
2. Why is it important to know if a protocol encrypts items that could be sent in the clear?
So that we ensure that there is minimal traffic on a channel and that the protocol efficiently encrypts items

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?

Yes if the given preconditions are met

CS361 Questions: Week 4 3

2. For each step of the NS protocol, answer the two questions on slide 5.

The sender is trying to send if the given message is fresh and not a replay from an earlier exchange. The only assumption is that it has not been used in any earlier interchange, with probability

Lecture 61

1. As in slide 5, if A's key were later changed, after having Kas compromised, how could A still be impersonated?

If the key was compromised, anyone could impersonate A and establish communication with any other party

2. Is it fair to ask the question of a key being broken?

It is because a presumption of any cryptographic protocol that the encryption is strong

3. How might you address these flaws if you were the protocol designer?

To ensure that all encryption is strong

Lecture 62

1. What guarantees does Otway-Rees seem to provide to A and B?

It doesn't necessarily guarantee any safe passage

2. Are there guarantees that Needham-Schroeder provides that Otway-Rees does not or vice versa?

Needham-Schroeder it illustrates how difficult it is to build a secure cryptographic protocol

3. How could you fix the flawed protocol from slide 4?

C initiates a new run of the protocol with B

Lecture 63

1. Why is the verification of protocols important?

Protocols are crucial to the Internet

2. What is belief logic?

A belief logic is a formal system for reasoning beliefs. Any logic consists of a set of logical operators and rules of inference

3. A protocol is a program; where do you think beliefs come in?

You have to postulate some reasonable initial assumptions about the state knowledge/belief of the principals

Lecture 64

1. What is a modal logic?

They are operators describing a belief system

2. Explain the intuition behind the message meaning inference rule.

There are numerous rules of inference for manipulating the protocol to generate a set of beliefs

3. Explain the intuition behind the nonce verification inference rule.

4. Explain the intuition behind the jurisdiction inference rule.

To optimize the protocol to ensure its quality and efficiency

3. What is idealization and why is it needed?

One purpose of idealization is to omit parts of the message that do not contribute to the not contribute to the beliefs of the recipient. In BAN all plaintext is omitted since it can be forged

Lecture 65

1. Why do you think plaintext is omitted in a BAN idealization?

Use of a logic like BAN shows what is provable and also what must be assumed

2. Some idealized steps seem to refer to beliefs that will happen later in the protocol. Why would that be?

Using a ban effectively requires a lot of practice insight into the protocol

3. One benefit of a BAN proof is that it exposes assumptions. Explain that.

These are the point of the protocol. The proof exhibits