UTEID: dpk326;
FIRSTNAME: David;
LASTNAME: Ko;
CSACCOUNT: davidko;
EMAIL: davidpeterko@gmail.com;

CS361 Questions: Week 4
These questions relate to Modules 12, 13 and 14. Type your answers and submit
them on Canvas by 5pm on Thursday, July 2.

Lecture 53
1. Why is it important for a digital signature to be non reusable?
	The attacker can jut reuse the digital signature and continue to try and verify different messages, or sign messages and pass them off as from the original signer.
2. Why is it the hash of the message typically signed, rather than the message
itself?
	The hash is typically signed because then the attacker has to decrypt 2 things, to dehash and then break the verification
3. What assurance does R gain from the interchange on slide 4?
	It gives the notion that R is coming form the real sender.

Lecture 54
1. What is the importance of certificate authorities?
	They make sure the certificate is authenticate and from the correct source.
2. In the example on slide 5, why does X sign the hash of the first message
with its private key?
	To encrypt the data, and it allows the reciever Y to decrypt with its public key
3. Why is it necessary to have a hash of Y and Ky?
	To make sure that the K itself is also safe
4. What would happen if Z had a public key for X, but it was not trustworthy?
	It wouldnt work because the private key is needed not public

Lecture 55
1. What happens at the root of a chain of trust?
	It is rooted at some unimpeachable authroity
2. Why does an X.509 certificate include a “validity interval”?
	To check when the validity expires
3. What would it mean if the hash and the received value did not match?
	Then the message was not hashed with the right function

Lecture 56

1. What are some protocols previously discussed?
   Hash, encryption/decryption, sign and verify
2. What may happen if one step of a protocol is ignored?
   Then the outcome becomes skewed and gives someting incorrect since a step was not done correctly or ignored
3. Why must the ciphers commute in order to accomplish the task in slide 4?
   To send some content with confidentiality in the context of a hostile or utrustworthy environment.
4. Describe how an attacker can extract M from the protocol in slide 6.
   By grabbing both keys to both lockboxes
5. Describle how an attacker can extract Ka from the protocol in slide 6.
   You can reverse XOR
6. Describle how an attacker can extract Kb from the protocol in slide 6.
   You can reverse XOR
7. Why are cryptographic protocols difficult to design and easy to get wrong?
   They must not be able to reverse the protocol, or be able to use a previous key to get the message (since its deterministics like the one time pad)

Lecture 57

1. Explain the importance of protocols in the context of the internet.
   Protocols are on the internet ot ensure security and authenticity of websites and etc.
2. Explain the importance of cryptographic protocols in the context of the internet.
   TO be able to send information or passwords across the internet without being seen or stolen
3. What are the assumptions of the protocol in slide 6?
   That both A and B have the keys they both need.
4. What are the goals of the protocol in slide 6?
   A shares with B a secret key K and each party is authenticated to each other
5. Are the goals of the protocol in slide 6 satisfied? Explain.
   A must have a key, and B must haev a key.
6. How is the protocol in slide 6 flawed?
   Someone could take the key, or the key itself could be stolen

Lecture 58

1. Why is it important to know if a protocol includes unnecessary steps or
messages?

Because those steps could be the reason why the protocol fails
2. Why is it important to know if a protocol encrypts items that could be sent
in the clear?
So that other people listening on cannot see what the item is, which is the purpose.

Lecture 59
1. Why might it be difficult to answer what constitutes an attack on a cryptographic
protocol?
There are so many possibilities for attacks that you cant generalize them
2. Describe potential dangers of a replay attack.
You can do the transaction btu the money could be fake
3. Are there attacks where an attacker gains no secret information? Explain.
Yes, there could be attackw here its purpose is to disrupt or destroy and not even take information
4. What restrictions are imposed on the attacker?
They can acess all the methods of communication and corrupt it
5. Why is it important that protocols are asynchronous?
One being affect doesnt affect the others

Lecture 60
1. Would the Needham-Schroeder protocol work without nonces?
Yes
2. For each step of the NS protocol, answer the two questions on slide 5.
A. tell S who the sender and the reciever and the message id is
B. tell A the shared key for B
C. tell B the shared key for both
D. tell A th emessage is just made
E. tell B is the message is complete

Lecture 61
1. As in slide 5, if A's key were later changed, after having Kas compromised,
how could A still be impersonated?
B would think that A send the message and uses the old keys because S neer told B that the key no longer is valid
2. Is it fair to ask the question of a key being broken?
Yes
3. How might you address these flaws if you were the protocol designer?
Add a protocol step to ensure A and B both know when the key

ends with validation

Lecture 62
1. What guarantees does Otway-Rees seem to provide to A and B?
	Sessions
2. Are there guarantees that Needham-Schroeder provides that Otway-Rees
does not or vice versa?
	B is always aware if a message is a rely with high probability
3. How could you fix the flawed protocol from slide 4?
	Encrypt K before sending it

Lecture 63
1. Why is the verification of protocols important?
	We want ot make sure that they do what they are intended (and keep the chain trusted)
2. What is a belief logic?
	Reasoning about what principals within the protocol should be able to infer from messages they have
3. A protocol is a program; where do you think beliefs come in?
	The protocol is based ont he beliefe system/logic of the people who designed it

Lecture 64
1. What is a modal logic?
	how to represent a belief
2. Explain the intuition behind the message meaning inference rule.
	If A believes something, then when it sees something, A believes what B said (X)
3. Explain the intuition behind the nonce verification inference rule.
	If A believes X is freh and A believs B once said X then both and A and B believe X
4. Explain the intuition behind the jurisdiction inference rule.
	If A believes B, it has jurisdiction over X and A believes B which believes X then A believes X
5. What is idealization and why is it needed?
	converting to modal logic, whihc is how you abstractly verify protocols

Lecture 65
1. Why do you think plaintext is omitted in a BAN idealization?
	You should never sent PT as it can be caught by whoever is listneing in
2. Some idealized steps seem to refer to beliefs that will happen later in the
protocol. Why would that be?

It acts as a certification method to check that it meet at all points

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

It allows you to break down the steps and see where and when you make assumption you dont make at the beginning