Name: Ridwan Hoq
EID: rmh2376
CS Login: ridwan
Email: ridwanhoq@gmail.com

Lecture 53

1. Because then future messages might not be authentically signed if using an old signature from a previous message.
2. Public key encryption is expensive and messages can be arbitrarily long. However, a hash will always be a fixed length so it is usually cheaper to encrypt the hash.
3. It has all the desired properties: unforgeable, authentic, no repudiation, tamperproof, not reusable

Lecture 54

1. To establish trust between two parties. When two parties have never met/dealt with each other before, a third party can vouch for a party to establish trust.
2. X acts as the third party to establish trust.
3. To ensure Y and KY weren't tampered with
4. It could pretend that it was X which would be bad.

Lecture 55

1. The root of a chain of trust should be some unimpeachable authority
2. Validity interval determines how long this certificate should be trusted for
3. That means the certificate has been changed and isn't to be trusted

Lecture 56

1. RSA/AES
2. If you skip a step in a protocol then it is likely that the message cannot be properly read since the other party will not know you that you skipped a step in the protocol
3. Ciphers must commute since encrypting one within another cannot decrypt the other.
4. XOR msg 1 and 2 to get Kb. then XOR Kb, msg 1, and msg 3 to get Ka. Then XOR msg1 and Ka to get M.
5. XOR msg 1 and 2 to get Kb. then XOR Kb, msg 1, and msg 3 to get Ka.
6. XOR msg 1 and 2 to get Kb.
7. Because it only takes 1 vulnerability to compromise the strength of the cryptographic protocol.

Lecture 57

1. A protocol is important for the internet since it creates a structured way to communicate. Without protocols, communication would be disorganized and haphazard which would be very inefficient.
2. Cryptographic protocols are important in the context of the internet because many scenarios require that information be confidential such that third parties cannot read that information.
3. That A and B know eachother's secret keys.
4. A shares with B a secret Key K and each party is authenticated to the other
5. No it is satisfied because it is flawed.

6. The flaw is that there needs to be a way to ensure that those keys are already shared.

Lecture 58

1. Those steps could be eliminated
2. That means that information could be read by anyone which means it shouldn't be used at all to secure the information being transmitted by the protocol.

Lecture 59

1. Because often times an attack will seem like a normal execution of the protocol when there is really an attacker sending a message posing as an authorized party.
2. An attacker can save an old message and send it later to get a response which may give the attacker enough information to crack the protocol.
3. Yes an attacker may just attempt to introduce noise or just disrupt the flow of information.
4. An attacker will not have the exact procedure of encryption as long as it is not published online.
5. So that a protocol system can be carried out on a distributed system.

Lecture 60

1. No because the principals must know that the messages they are receiving are fresh.
2. asd

Lecture 61

1. By sending the same key with a new nonce.
2. Yes it is.
3. Require both A and B to authenticate with S.

Lecture 62

1. That A and B both have a secret key in which they can communicate with.
2. Otway-Rees guarantees that both directions of messages are fresh whereas Needham-Schroeder only guarantees one direction of message are fresh.
3. Don't send private keys.

Lecture 63

1. To ensure they actually work as advertised.
2. A belief logic is a formal system for reasoning about beliefs.
3. Beliefs are what assumptions are being made.

Lecture 64

1. A logic in which there are different states/modes
2. If A believes that A shares a K with B and that A sees a message encrypted with K then it knows that the message is from B.
3. If A gets a nonce back after sending it, it knows the message was fresh.
4. Essentially it is the transitive property. If A believes that B has jusridiction over X and that B believes X, then A believes X.
5. Idealization turns a sent message into its intended semantics.

Lecture 65

1. So that there is no assumption that information can be read by anyone.
2. To ensure protocols are working as intended.
3. By laying out all beliefs made by all actors it can highlight where exactly assumptions are being made.