Lecture 53

1. If the signature is non-reusable, an attacker cannot take the signature and use it to authenticate another object.
2. Public key encryption is expensive, but a hash is a short finite number. So signing the hash would be less expensive than signing the actual message.
3. It is tamperproof. Only R can remove the outer layer of encryption.

Lecture 54

1. Certificate authorities "vouch for" a person. They establish a web of trust.
2. X signs the hash of the first message to authenticate that it actually is the key for Y. X signs it with it's private key so that you can decrypt the message and figure out if it is actually the key for Y.
3. You have a hash of Y and K_y so you can verify Y and K_y.
4. Then you don't know if Y and K_y have been altered.

Lecture 55

1. The chain is rooted at some unimpeachable authority.
2. To check if the certificate is expired. If the certificate is expired, then you can't trust it.
3. It would mean that something has been altered. Therefore, it is not trustworthy.

Lecture 56

1. Public key encryption, RSA
2. The message you are sending may no longer be secure.
3. The other party does not have to key to unlock the "strongbox".
4. If the attacker is eavesdropping, they can store all three messages and can XOR combinations to extract M.
5. If the attacker is eavesdropping, they can store all three messages and can XOR combinations to extract K_a.
6. If the attacker is eavesdropping, they can store all three messages and can XOR combinations to extract K_b.
7. Like the protocol on slide 6, it may seem like it would work fine and be secure. However, it can be easy to discover the components if someone looks at all of the messages.

Lecture 57

1. A protocol is important in context of the internet because they are used so that information sent between two machines/objects are able to read each others messages.
2. Cryptographic protocols are important in context of the internet because people send private information that they want to be kept secure all the time. For example, a cryptographic protocol is necessary for a person who is signing into their Amazon account.
3. There is a public key system in place and that each has a reliable version of the others public key.
4. That B has received K from A and can extract it; that A is talking to B and B is talking to A.
5. Yes. The messages A and B send are only extractable by the other since they should be the only ones who have their own private key.
6. The message can be intercepted by someone else and then they could send B their own key.

Lecture 58

1. It would just be inefficient since those steps don't aren't necessary to send the message confidentially.
2. If the protocol is encrypting items that do not need to be sent confidentiality, it would take more time and not be as efficient.