**Lecture 53**

1. So the signature cannot be detached and applied to another message.
2. So the message can be encrypted, and the signature is only on that hash function.
3. Either key can be used for encryption or decryption and vise versa when sending a message. It allows for a symmetric key.

**Lecture 54**

1. It gives you trust that you are working with a non-corrupted or legitimate other party.
2. So that he can encrypt the original key with his signature, that Y can’t alter.
3. You need the hast of Y and Ky in order to compare the current state of Y and Ky, essentially verifying that the certificate is good.
4. If Z had the public key for X, then the entire certificate process is void. This policy requires that Z is a trustworthy party

**Lecture 55**

1. Y gets a certificate from both parties and in order to create a train of trust between both of them.

2. “validity interval” is used so that the certificate is only valid for a certain amount of time, not infinitely. It makes the two parties re-check the certificates often in case one goes corrupt.

3. If the hash and received values didn’t match then the party has become corrupted

**Lecture 56**

1. Encryptions and ciphers are protocols, commonly used online.

2. The package/message could be intercepted when it is sent to the first time

3. Ciphers must communicate in order to unlock the keys that the other party needs in order to communicate.

4. An attacker can extract M by xor’ing the 3 differint strings to obtain Kb, and then M

5. the attacker could extract Ka by xor’ing the first and second messages with eachother.

6. The attacker could extract Kb by xor’ing the the last two messages

7. They are difficult to design/get wrong because you have to use the right type of encryption and keys in order to maintain confidentiality.

**Lecture 57**

1. The internet is a dangerous place to be exchanging messages and protocols are needed for safety and verification.
2. Cryptographic protocols keep information confidential and use Keys to keep information private when being shared.
3. That they both have a public key that the other knows
4. To authenticate each party with the other
5. Yes, by sharing the following info with eachother authentication should be gained
6. Its flawed because they need to share public keys, but that would reveal the inner info

**Lecture 58**

1. Because they are potential weaknesses in the protocol and may take more time to complete
2. So that you know the secrecy level of the messages and so you know that lower level information can be passed through the protocol as well

**Lecture 59**

1. an attack on a crypto- graphic protocol can’t be easily determined because the attacker could be unknown or unseen.
2. potential dangers of a replay attack are that protocols are repeated many times, so if the attacker gains access once, the entire protocol is ruined.
3. Sure, sometimes all they do is inject information and gain nothing from it.
4. Its difficult to determine those, you have to assume the attacker has all possible information available.
5. Any party that is in the system doesn’t know the protocol is occurring until it receives a message, and won’t know anything about the current run of the protocol.

**Lecture 60**

1. No, Nonces are needed so the parties know the message is “fresh”

2. The sender is trying to convey authenticity and confidentiality with the message, and the receiver is entitled to believe both (it came from that sender secretly)

**Lecture 61**

1. S only knows that the message is coming from A because they share a secret key.
2. Yes/no depending on the strength of the encryption
3. Use secret keys for both AS and BS so they both know they are legitimate

**Lecture 62**

1. Otway rees guarantees that the correct A and B are communicating.
2. Only Otway Rees provides these because the previous protocol would allow A to be impersonated and B not to know
3. Use the public key on the outside of the formula and the private key on the inside, or use a third party to generate a key

**Lecture 63**

1. To make sure that the protocol is safe and reliable from danger/attacks

2. Belief logic is a formal system for reasoning about beliefs, any logic consists of a set of logical operators and rules of inference

3. A protocol is a program; Beliefs are whether you expect the program to work correctly

**Lecture 64**

1. Modal logic is using beliefs to formulate outcomes

2. inference rule means that by implying something, you can come to a conclusion from that inference: A believes (A+B share a key) and A shares a sees a message with that encryption, then that message came from B

3. nonce verification inference rule says that if A believes X is fresh and A believes B once said X, then A believes B believes X

4. Jurisdiction inference rule: If A believes B has jurisdiction over X and A believes B believes X, then A believes X

5. Idealization is a process of logical steps for a protocol, and is needed for knowing that a protocol is valid.

**Lecture 65**

1. BAN idealization assumes the plaintext is valid and exists.
2. Some idealized steps seem to refer to beliefs that will happen later in the protocol, because if the first steps are true then the later steps will happen based on that. If the first steps fail then there is no sense in continuing the protocol
3. One benefit of a BAN proof is that it exposes assumptions. The formulas highlight the areas where the protocol assumes keys are valid or the protocol is correct