CS361 Questions: Week 9

These questions relate to Modules 11. Type your answers and submit on Canvas.

Lecture 46

1. Which of the 4 steps in AES uses confusion and how is it done?
2. Which of the 4 steps in AES uses diffusion and how is it done?
3. Why does decryption in AES take longer than encryption?
4. Describe the use of blocks and rounds in AES.
5. Why would one want to increase the total number of Rounds in AES?

Lecture 47

1. What is a disadvantage in using ECB mode?
2. How can this flaw be fixed?
3. What are potential weaknesses of CBC?
4. How is key stream generation different from standard block encryption modes?

Lecture 48

1. For public key systems, what must be kept secret in order to ensure secrecy?
2. Why are one-way functions critical to public key systems?
3. How do public key systems largely solve the key distribution problem?
4. Simplify the following according to RSA rules: $\{\{\{P\}_K^{-1}\}_K\}_{K^{-1}}$.
5. Compare the efficiency of asymmetric algorithms and symmetric algorithms.

Lecture 49

1. If one generated new RSA keys and switched the public and private keys, would the algorithm still work? Why or why not?

2. Explain the role of prime numbers in RSA.
3. Is RSA breakable?
4. Why can no one intercepting $\{M\}_{K_a}$ read the message?
5. Why can't A be sure $\{M\}_{K_a}$ came from B?
6. Why is A sure $\{M\}_{K_b^{-1}}$ originated with B?
7. How can someone intercepting $\{M\}_{K_b^{-1}}$ read the message?
8. How can B ensure authentication as well as confidentiality when sending a message to A?

Lecture 50

1. Why is it necessary for a hash function to be easy to compute for any given data?
2. What is the key difference between strong and weak collision resistance of a hash function.
3. What is the difference between preimage resistance and second preimage resistance?
4. What are the implications of the birthday attack on a 128 bit hash value?
5. What are the implications of the birthday attack on a 160 bit hash value?
6. Why aren't cryptographic hash functions used for confidentiality?
7. What attribute of cryptographic hash functions ensures that message M is bound to $H(M)$, and therefore tamper-resistant?
8. Using RSA and a cryptographic hash function, how can B securely send a message to A and guarantee both confidentiality and integrity?

Lecture 51

1. For key exchange, if S wants to send key K to R, can S send the following message: $\{\{K\}_{KS^{-1}}\}_{K_R^{-1}}$? Why or why not?
2. In the third attempt at key exchange on slide 5, could S have done the encryptions in the other order? Why or why not?

3. Is $\{\{\{K\}_{KS^{-1}}\}_{K_R}\}_{K_S}$ equivalent to $\{\{K\}_{K_S^{-1}}\}_{K_R}$?
4. What are the requirements of key exchange and why?

Lecture 52

1. What would happen if g, p and $g^a \mathrm{mod} p$ were known by an eavesdropper listening in on a Diffie-Hellman exchange?
2. What would happen if a were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?
3. What would happen if b were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?