Homework #11

(Due on Thursday, Jan 24th , 2019)

1. What are the security concerns network security is targeting at? What are the main areas of protection does network security cover?

2. What are the two main types of cryptography?

3. What is a man-in-the-middle attack? Is public key cryptography safe against that type of attack?

4. What other tricks do attackers use to overcome authentication protection. Please explain using the AP protocols presented in the lecture.

5. What is the purpose of a nonce in an end-point authentication protocol?

6. What is the conceptual difference between a crypto-hash function and other hash functions?

7. Alice wants to send a big message (~ 1Gb) to Bob. Explain how she can authenticate herself. Is there a more efficient way to do it?

8. Alice wants to send a big message (~ 1Gb) to Bob. She wants to send the message in a confidential way. How can she do that? With the techniques explained during class, please explain how it would be possible to do it in a more efficient way.