

Homework #11

(Due on 12:00am, Thursday, Jan 28th, 2015)

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 save against that type of attack?
4. What other tricks does 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?