Computer Networks Group

University of Göttingen, Germany

Homework #11

(Due Thursday, Jan 22, 2015)

1. Name two differences between public and private key cryptography. Which two protocols utilising private key cryptography have been discussed in the lecture?

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

3. What are pro's and con's for public vs. private key crypographic systems in computer networks?

4. RSA public key cryptography: Let $p=3$ and $q=11$. Use appropriate values for e and d and encrypt the value '*3*'

5. What other tricks might attackers use to overcome authentication protection?

6. Please explain using the AP protocols presented in the lecture.

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