Computer Networks Group
University of Göttingen, Germany

Homework #11

(Due on 12:00am, Thursday, Jan 27, 2011)

1. What are the security concerns network security is targeting at? What 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. Perform an RSA encryption and decryption with p=7 and q=11 with the word “Telematics”. (decryption may be hard without a math tool like Maple etc.)

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